

Impact of Spoofing of Navigation Systems on Maritime Situational Awareness

Andrej Androjna, Marko Perkovič

The development of contemporary navigation and positioning systems have significantly improved reliability and speeds in maritime navigation. At the same time, the vulnerabilities of these systems to cyber threats represent a remarkable issue to the safety of navigation. Therefore, the maritime community has raised the question of cybersecurity of navigation systems in recent years. This paper aims to analyse the vulnerabilities of the Global Navigation Satellite System (GNSS), Electronic Chart Display Information System (ECDIS) and Automatic Identification System (AIS). The concepts of these systems were developed at a time when cybersecurity issues have not been among the top priorities. Open broadcasts, the absence of or limited existence of data encryption and authentication can be considered as their primary security weaknesses. Therefore, these systems are vulnerable to cyber-attacks. The GPS as the data source of a ship's position can relatively easily be jammed and/or spoofed, increasing the vulnerabilities of ECDIS and AIS. A systematic literature review was conducted for this article, supplemented


KEY WORDS

- ~ Cybersecurity
- ~ Jamming
- ~ Spoofing
- ~ Safety of navigation
- ~ Shipboard navigation systems

University of Ljubljana, Faculty of Maritime Studies and Transport, Portorož, Slovenia

e-mail: andrej.androjna@fpp.uni-lj.si

doi: 10.7225/toms.v10.n02.w08

This work is licensed under 

Received on: 11.06.2021 / Revised on: 14.08.2021 / Accepted on: 22.08.2021 / Published online: 23.09.2021

by a SWOT analysis of the AIS service and particular case studies of recent cyber-attacks on these systems. The analysis of selected case studies confirmed that these systems could easily be spoofed and become a subject of data manipulation with significant consequences for the safety of navigation. The paper provides conclusions and recommendations highlighting the necessity for the users to be aware of the vulnerabilities of modern navigation systems.

1. INTRODUCTION

Maritime cybersecurity represents one of the most important segments of maritime security policy in general. Today's maritime industry is highly dependent on digitalisation. Modern digital systems are used in many segments of the maritime sector, including port authorities, national maritime administrations, maritime traffic management systems, shipping companies, and vessel monitoring and management systems.

The trend towards digitisation and integration of systems is largely present in the maritime sector. Most of the ship navigation, communication and control systems are integrated and use the Internet for successful operation (Middleton, 2014; Chybowski et al., 2019; Dobryakova et al., 2018). Modern information technologies, together with digitalisation and integration trends, have significantly accelerated and improved the processes of management, safety and control in the maritime sector. However, it is important to emphasise that these technologies are vulnerable to cyber-attacks. The number of these attacks shows a trend of significant growth. Cyber-attacks in the maritime industry have increased by 900% between 2017 and 2019 (Marine Insight, 2020).

As the International Maritime Organization (IMO) gives great importance to maritime security issues, it has adopted resolution MSC.428 (98) "Marine Cyber Risk Management in

Security Management System (SMS)" (IMO, 2017) and "Guidelines on Cyber Risk Management (MSC-FAL 1/Circ.3) (IMO, 2017a)." The adoption of these documents enabled the revision of the provisions of the International Safety Management Code (ISM). The ISM contains cyber risks and recommendations to protect ships and ship systems from cyber-attacks (IMO, 2018). The new provisions of the ISM Code entered into force on 1 January 2021.

Based on the IMO's suggestion, the International Electrotechnical Commission (IEC) has developed the standard 63.154 to ensure the technical aspects to increase cyber resilience. This standard contains general requirements, test methods and required test results with the aim of increasing the level of cybersecurity of maritime navigation and communication systems (IEC, 2019).

At the regional level, the cybersecurity efforts of the European Union (EU) should be highlighted. The EU has taken significant steps to raise the level of cybersecurity in a number of sectors, including the maritime sector. In the maritime sector, the "EU Maritime Security Strategy" (EU, 2014), "2018 Revised Action Plan" (EU, 2018) and "Progress Reports" (EU, 2016; EU, 2017b; EU, 2020) are worth mentioning. The EU Maritime Security Strategy is the EU's umbrella document for maritime cybersecurity issues, while the Action Plan defines measures and Progress Reports shows the implementation of these measures in the maritime sector on an annual basis.

States and professional associations in the maritime sector are also involved in addressing the cybersecurity issue. States develop national cyber and information security strategies (Danish Maritime Cybersecurity Unit, 2018), while professional associations conduct research and situation assessments to define the risk of cyber threats in the maritime sector (BIMCO, 2020).

Thus, it can be said that a regulatory framework, technical and operational mechanisms, and implementation tools have been developed at global, regional and national levels. This framework identifies problems, analyses risks, monitors trends and defines measures to reduce the risks of cyber threats in the maritime sector. It is important to stress that analyses and trends show that significant steps have not yet been taken to increase the level of cybersecurity on ships, i.e. their essential navigation and communication devices are vulnerable to cyber-attacks.

There is no single classification of the types of cyber threats. Jones et al. state that the general and broad spectrum of these threats to the maritime sector includes business disruption, financial loss, damage to reputation, damage to goods and the environment, incident response costs, and fines or legal issues (Jones et al., 2012). Caponi and Belmont specify such threats, which may include manipulation of passenger lists, illegal shipments, breach of sensitive cargo shipments, intentional engine failures, vessel shutdowns, or other manipulation of

onboard control systems (Caponi & Belmont, 2015). Over the past decade, cyberattacks have been recorded against almost all segments of the maritime sector. Ships, shore-based offices, seaports, terminals and supply chains are exposed to cyber threats (Androjna & Twrđy, 2020). It should also be noted that the IMO being affected by a cyber-attack at the end of last year was no exception (Knowler, 2020).

This paper analyses cyber threats to ship navigation and communication systems. These systems have significant weaknesses in terms of their exposure to cyber threats. According to BIMCO research, positioning systems, navigation systems, propulsion control systems, and surveillance systems are vulnerable to cyber threats (BIMCO, 2017).

Problems related to cyber threats to onboard navigation systems can be observed at two levels. One level of the problem represents the connection of the Shipboard Integrated Navigational System (INS) to the Internet. In the research conducted by Svilicic et al. (Svilicic, 2019) and Hareide et al. (Hareide, 2018), a higher level of cyber-attack threat was observed when the INS is connected to the Internet, i.e. when it is operating in online mode. The second level of the problem is related to the technical characteristics of the INS device. At the time of their commissioning, security was not the imperative as it is today (Kessler, 2020). Therefore, some of today's navigational devices can be relatively easily disrupted with relatively simple, inexpensive, and easily accessible devices.

Recent cyber-attacks on ships show that GPS, ECDIS and AIS are particularly vulnerable to these attacks. In this paper, we analyse the vulnerabilities of these systems. In general, these systems may be exposed to cyber threats related to jamming and spoofing.

Jamming is an intentional or unintentional interference (Kjerstad, 2016) of a radio frequency signal. Unintentional disruptions can be the result of various reasons, such as adverse weather conditions or equipment malfunctions, but they do not fall into the group of cyber threats because they are not caused intentionally. From a cyber-security perspective, particular attention is paid to intentional jamming, which is an intentional transmission of signals. GNSS is vulnerable to jamming. Cases of GNSS jamming are recorded in different parts of the world. From the point of view of navigation safety, it is essential to note that navigation systems sound an alarm when they detect jammers (Androjna et al., 2020). Spoofing is a more sophisticated method of cyber-attacks (Kjerstad, 2016) of intentionally creating false signals that can cause GNSS, ECDIS and AIS malfunctions. In most cases, spoofing is more difficult to detect than jamming. Jamming and spoofing of navigation systems can lead to data manipulation and modification, insertion of malicious content and fake data, hijacking, availability disruption, bandwidth usurpation.

The article consists of four sections. Section 2 describes the methodology. Section 3 provides a literature review on the main features of GNSS, ECDIS and AIS and their vulnerabilities to spoofing, examples and analysis of significant spoofing events. Section 4 discusses the results and provides some recommendations and conclusions.

2. METHODS

A literature review on spoofing of navigation systems on maritime situational awareness was conducted. It was followed by a comprehensive, explicit, reproducible, and idiosyncratic implicit method of data collection and structured following documented guidelines (Tranfield, Denyer & Smart, 2003; Grant & Booth, 2009; Milner, 2014). This method consists of ten steps congregated into three phases. The first phase focused on defining a review question to guide the search: "What are the effects of AIS spoofing in the maritime domain?" The second phase identified the appropriate time frame for documents to be included from relevant research databases such as Scopus, Web of Science, Science Direct, Google Scholar and open sources. "Spoofing" and "jamming" were identified as search keywords to be reviewed. After refining the selection to identify relevant documents, over 49 documents (21 articles, 18 peer-reviewed journal articles, and 10 reports from specialised agencies) were included, covering the mentioned area in the period from 2019 to 2020. In the third phase, we report our findings from the literature review.

The specific aspect of AIS / GPS spoofing is reinforced by the SWOT analysis in section 3.1.3 and by the case study analysis in section 3.3 from the Faculty of Maritime Studies and Transport, University of Ljubljana, regarding a particular AIS spoofing event near Elba Island in late 2019 (Androjna et al., 2021). As part of the research, AIS data were first obtained through cooperation with the Slovenian Maritime Administration, which is stored at MARES regional data exchange programme. Additional AIS day data were subsequently obtained from the Italian Coastguard. With these archive data, the strength of signals received at the AIS BS on the island of Elba was analysed, and a navigation scenario of the affected area created using the application AIS Network Data Client, played in two different VTS applications Navi-Harbor (Wärtsilä) and Pelagus (Elman). The spoofing data AIS analysis was then displayed on ECDIS and RADAR applications via the ship tracking simulator Navi Trainer Pro (Wärtsilä). Finally, a traffic density map (TDM) was created by using the European Marine Observation and Data Network (EMODnet) method (EMSA, 2019) and ship positioning data from terrestrial and S-AIS data sources, maritime infrastructure, and the SafeSeaNet Ecosystem Graphical Interface (SEG) application.

3. RESULTS

This chapter analyses the GNSS, ECDIS and AIS challenges connected with cyber threats to maritime navigation. It presents findings on their vulnerabilities, which will predominantly come from their technical performances. A basic description of these systems, basic technical and operational requirements, and liabilities to spoofing will be provided. The analysis of selected cyber-attacks to these systems confirmed their liability to cyber threats that may lead to a decrease in the level of safety of navigation and result in particular economic and even significant geopolitical consequences.

3.1. Vulnerabilities of GNSS, ECDIS and AIS to cyber threats

3.1.1. Vulnerabilities of GNSS

GNSS is designed to provide a continuous positioning service that measures time and speed for an unlimited number of users (Kjerstad, 2016). The best-known system in operational use is the US GPS (GPS/Navstar), which was developed as a military system with the option for civilian users.

The term GNSS refers to space-based systems such as the US GPS, Russian Global Navigation Satellite System (GLONASS), European Galileo System, Chinese BeiDou, Indian Navigation Indian Constellation (NavIC), Japanese Quasi-Zenith Satellite System (QZSS) (Androjna et al., 2020), and satellite navigation systems developed in future. The term GNSS is often colloquially replaced by the term GPS as it is widely used worldwide.

According to the International Convention for Safety of Life at Sea (SOLAS) Regulation V/19.2.1.6, all ships, irrespective of size, shall have a receiver for a GNSS or a terrestrial radio navigation system or other means suitable for use at all times throughout the intended voyage to establish and update the ship's position by automatic means (IMO, 2020). Due to SOLAS requirements, simplicity of use and high reliability, GNSS receivers now have an extensive application on ships and are a significant source of position fixing and timing.

GNSS is vulnerable to jamming, spoofing, meaconing (INTERTANKO, 2019) and blocking. GNSS jamming is the deliberate transmission of signals on frequencies used by GNSS to prevent receivers from locking onto authentic GNSS Signals (Androjna et al., 2020). Jamming can be done with relatively simple, inexpensive, and commercially available radio transmitters that send signals on almost the same frequency as the satellites (Kjerstad, 2016). It is important to note that there is unintended jamming due to space weather conditions. Cases of GNSS jamming have been reported in different parts of the

world, usually in some crisis areas and during military activities such as electronic warfare exercises (Kjerstad, 2016).

Unlike jamming, GNSS spoofing is a more demanding and sophisticated method of cyber-attack that requires sophisticated equipment and a higher level of technical knowledge for its implementation (Kjerstad, 2016). GNSS spoofing broadcasts a false GNSS signal or a rebroadcast of accurate signals acquired at a different location or time (INTERTANKO, 2019). Spoofing can result in false position indication or timing. In GNSS spoofing, the transmission of a false signal is synchronised with an actual signal. Since the false signal is stronger than the real one, the GNSS receiver follows this false signal. Technically, GNSS spoofing is easier to implement by rebroadcasting than by broadcasting a false signal (INTERTANKO, 2019). A significant problem associated with GNSS jamming and spoofing is that GNSS is linked to onboard navigation and communication systems and is the only source of position and time for these systems. This means that the position and time error of the GNSS receiver is transferred to other connected equipment, which can cause an additional problem in the safe conduct of maritime navigation.

3.1.2. Vulnerabilities of ECDIS

ECDIS is an advanced navigation information system (Weinrit, 2009) that provides a continuous display of vessel position using the official Electronic Navigational Charts (ENC). ECDIS allows the display of all information required for safe navigation and must support a full range of navigational functions. As an information system, ECDIS goes far beyond the pictorial display of nautical charts on a computer screen (Hecht et al., 2017). The legal requirements for ECDIS are defined in the SOLAS Convention. Regulation V/19.2.10 of the SOLAS Convention requires ECDIS to be carried on certain types of SOLAS ships engaged on international voyages (IMO, 2020). In addition, ECDIS must be certified in accordance with SOLAS Regulation V/18 and IMO Resolutions A.817(19), MSC.64(67), MSC.86(70), and MSC.232(82), comply with the IMO performance standards and type approved by the Administration. This means that ECDIS must have type approval and test procedures developed by IEC 61.174 and IEC 62.288 standards and based on the IMO and International Hydrographic Organization (IHO) requirements before installation on the ship (Hecht et al., 2017). According to SOLAS requirements, ENC, which is used in ECDIS, must be official (issued by the national hydrographic office), up-to-date and compliant with the relevant IHO standards and specifications.

In order to comply with the IMO requirements for a permanent indication of vessel's position and other navigation functions, ECDIS should be linked to the appropriate sensors. These sensors can be divided into mandatory and optional.

According to the IMO Resolution MSC.232(82), mandatory ECDIS sensors are a continuous position source (GNSS), a gyrocompass (or a heading transmission device), and a speed and distance measuring device (Thornton, 2016). All other sensors are optional. In practice, ECDIS is usually connected with various sensors, such as backup mandatory sensors, echo sounder, AIS, anemometer, radar (including ARPA).

In principle, there are three groups of ECDIS vulnerabilities. These are vulnerabilities of ENC data, then vulnerabilities of the mandatory and optional ECDIS sensors, and vulnerabilities of ECDIS as a computer-based system. ECDIS displays the official ENCs in human-readable System Electronic Navigational Chart (SENC) format. With the goal of preventing data manipulation and unauthorised use of the official ENCs and their updates, IHO Standard S-63 (IHO Data Protection Scheme) was developed. This standard provides a method to protect ENC data based on an encryption algorithm that provides piracy protection, selective access and authentication of ENC data (IHO, 2020). The application of this standard allows the end-users (vessels) to have authorised access to the official, up-to-date and protected ENC data while providing ENC manufacturers with protection against unauthorised access, modification, or manipulation of the data. The application of the Data protection scheme eliminates or significantly reduces the vulnerabilities of ENC data and enables its secure transfer via USB or the Internet from the manufacturer to the end-user. ECDIS mandatory and optional sensors of particular interest in cybersecurity are the vulnerabilities of the GNSS and AIS. In the event of a cyber-attack on the GNSS and/or AIS, these sensors will provide inaccurate information to ECDIS. The third group of vulnerabilities relates to ECDIS as a computer-based system. According to BIMCO, a malware attack on ECDIS installed onboard a newbuilding paperless bulk carrier is a reported case of a malware attack. ECDIS failure was not identified as a cyber-issue by the responsible crew members. This incident, in which ECDIS was infected with a virus, caused a significant delay to a voyage and high delay-related and repair costs (BIMCO, 2020a). ECDIS vulnerabilities, especially in paperless vessels, can lead to severe consequences ranging from navigational safety to marine pollution or geopolitical threats.

3.1.3. Vulnerabilities of AIS

The AIS is a communication system that enables automatic and continuous data exchange between ship and shore. The system was developed in collaboration among the IMO, International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA), International Telecommunication Union (ITU) and International Electrotechnical Commission (IEC) (IALA, 2016). According to SOLAS regulation V/19.2.4, all ships of 300 GT and more engaged in international voyages and

cargo ships of 500 GT and more not engaged in international voyages and passenger ships, irrespective of their size, shall be equipped with AIS (IMO, 2020). The European Union and national authorities have also developed obligations related to AIS for certain types of non-SOLAS vessels (i.e. fishing and recreational vessels) (Kjerstad, 2016). The international, regional, and national requirements and the ease and practicality of use greatly expand the range of users of AIS.

At the beginning of its development, the AIS was designed as a device to exchange identification information between ship and shore. The broader applications became apparent very quickly so that today the use of AIS is significantly expanded compared to the past, ranging from use for vessel collision avoidance, identification purposes, the safety of navigation, maritime security, traffic monitoring, prediction and analysis, search and rescue, monitoring of fishing activities, ecological concerns and scientific purposes (Natale et al., 2015; Eriksen et al., 2018; Ramin et al., 2020; Sciancalepore et al., 2021).

The AIS transceivers consist of a VHF transmitter, two VHF Time Division Multiple Access (TDMA) receivers, a VHF Digital Selective Calling (DSC) receiver, a positioning module (GNSS) and other sensors connected via standard marine electronic communication links (Caprolu et al., 2020). From a technical

point of view, the AIS transmits and receives standardised messages on two dedicated VHF channels 87B and 88B (AIS 1 and AIS 2) using the self-organised TDMA protocol (SOTDMA), where the unit of time (one minute) is divided into time slots of equal length of 26.7 ms, allowing a nominal AIS capability of 2,250 messages per minute and per one dedicated AIS channel (IALA, 2016). The basic requirement for using the SOTDMA protocol is the synchronisation of the time slots of AIS stations, which is achieved by a highly accurate standard time reference provided by the GNSS (ITU, 2014). The AIS messages are standardised by type and content and divided into four groups with corresponding nominal reporting intervals depending on the type of AIS stations, message group, navigational status, speed, and course change (IALA, 2016). The existing AIS protocol provides standardised, simple, accurate and fast data exchange between different types of mobile (shipborne) AIS stations (AIS Class A and AIS Class B, AIS SART, MOB-AIS, EPIRB-AIS and AIS and SAR aircraft) and fixed AIS stations (AIS Base Stations, AIS repeaters, and AIS Aids to Navigation - AtoNs). The AIS service has numerous advantages and, of course, disadvantages.

Based on these facts, the SWOT analysis (Piercy & Giles, 1989) of the AIS service is described in Table 1.

Table 1.

SWOT analysis of AIS service.

Strengths	Weaknesses
<ol style="list-style-type: none"> 1. Anti - collision aids to navigation. 2. Enhanced MSA. 3. SAR aid. 4. Safety aids to navigation – AtoN. 5. Marine environmental pollution monitoring and control. 	<ol style="list-style-type: none"> 1. Possible errors in navigation data may cause a CPA alarm to be raised. 2. Malicious attack on AIS service may generate unrealistic MSA. 3. Possible generation of false distress signals for MOB. 4. Generation of one or more fake buoys at critical locations. 5. Malicious attack on the AIS service with ship spoofing.
Opportunities	Threats
<ol style="list-style-type: none"> 1. If navigational data is appropriately used, the risk of collision can be reduced. 2. AIS provides increased MSA that enables effective response to emergencies such as search and rescue (SAR). It may help to identify trends or improvements in the provision of services to enhance the safety of navigation. 3. If SAR data are not corrupted in some way, the cost of operating SAR can be reduced, helping rescuers locate survivors. 4. AIS can increase the safety of navigation in a particular sea area. 5. S-AIS can detect ship oil spills in the open sea. 	<ol style="list-style-type: none"> 1. Potential spoofing can mislead the OOW in making a collision decision. 2. Potential spoofing of ships may mislead national authorities regarding maritime surveillance. 3. Potential AIS SART spoofing can trigger SART alerts to mislead victims into navigating to hostile and attacker-controlled sea areas. 4. AtoN spoofing can mislead the OOW in navigation, resulting in incorrect manoeuvres at critical locations with heavy shipping traffic or in coastal navigation (e.g., shoals). 5. Potential ship spoofing by attackers can falsify information to blame another ship for oil spills.

From the SWOT analyses, the advantages of AIS service can easily become disadvantages if the service is exposed to a malicious attack. Opportunities can lead to increased Maritime Situational Awareness, the safety of navigation, environmental protection, and efficiency of SAR operations. At the same time, since AIS service is a nonsecure and open broadcasting system, it can be exposed to external threats such as spoofing.

All types of AIS stations are vulnerable to spoofing, hijacking and availability disruption based on software or radiofrequency threats (Balduzzi et al., 2014). Vulnerabilities of AIS arise primarily from its technical performance as AIS is an open broadcasting system with no security features. The data sent by the transponders are not encrypted and do not have authentication, integrity checking, and confidentiality features (Goudossis & Katsikas, 2018; Caprolu et al., 2020). Therefore, there are risks for malicious transmissions and data manipulations (IALA, 2016).

So far, some methods have been proposed to mitigate AIS risks of spoofing. The proposal of a protected AIS software that uses the technique of public-key cryptography provides an authentication and message integrity service (Kessler, 2020). Another proposal is the secure AIS application protocol based

on encryption and authentication of transmission using a certification mechanism applicable in AIS class A and B stations (Aziz et al., 2020). This proposal has been further extended by introducing Auth-AIS, which allows the authentication of AIS messages (Sciancalepore et al., 2021). The maritime certificate-less identity-based public-key cryptography method provides on-demand authentication, message integrity, and confidentiality of AIS data (Goudossis & Katsikas, 2018; Goudossis & Katsikas, 2020). All these proposals are based on cryptographic methods that enable the encryption of AIS messages. They are also backwards compatible and allow interoperability with existing AIS devices that do not use the modified software or hardware (Androjna et al., 2021).

3.2. Selected case studies of GNSS spoofing

The last few years have been remarkable in many ways. Although the coronavirus pandemic disrupted worldwide operations, some global trends, such as our increasing reliance on GNSS, have continued unabated (Buesnel, 2020). In recent years, there have been several disruptive incidents that have caused a stir in the shipping industry, as shown in Table 2.

Table 2.

An overview of some GNSS spoofing events that affected maritime traffic between the years 2018 and 2020.

Location and Date	Spoofing Incidents Description
Ten global locations connected to one of the superpower states, 2016-2019	9,883 suspected spoofing incidents.
Point Reyes in northern California, 2019	Ships thousands of miles at sea mysteriously reported GPS positions in ring patterns off the coast of San Francisco.
Eastern Mediterranean and the Red Sea, 2019	Signal interference, loss of erratic AIS/GPS signals.
Strait of Hormuz, 07/2019	A British oil tanker, Stena Impero, was seized by Iranian forces after the ship was spoofed into changing course into Iranian waters.
Ningbo (China) - Nampo (Democratic People's Republic of Korea), 07-11/2019	The M/V Fu Xing 12 manipulated its identity by employing two AIS on board and using four different ship names to disguise its operations in delivering illegal coal and other resources.
Port of Shanghai, 2018-2019	Fake signals caused ships to appear to be moving in ring patterns at short intervals.
Ponce De Leon Inlet, Florida, 2020	Four visual AtoNs appeared on the map based on fake AIS messages.
Elba Island, 03/12/2019	Deliberate spoofing of the vast number of artificial AIS targets temporarily affected the navigation of ships.
Galapagos, 07/2020	One of the world's largest fleets of fishing nations misreported its location (approximately 10,000 km from its observed location) to conceal illegal fishing activities in the exclusive economic zone (EEZ) around the Galápagos Islands.

From Table 2, it can be concluded that the original purpose of AIS spoofing to this day is to conceal illegal fishing and other illegal activities at sea, including ship spoofing and AIS hijacking. There was also an example of AtoNs spoofing at Ponce De Le-on Inlet. In recent years, we have seen GNSS spoofing as part of defence development in a civilian scenario. The AIS spoofing has been deliberately used for electronic warfare and to disguise military activities such as the situation in the Eastern Mediterranean and Red Sea (Androjna et al., 2021). Another example in 2017 is the incident at Gelendzhik Airport, where at least 20 ships near the Black Sea Novorossiysk Commercial Sea Port reported that their AIS tracks falsely indicated their position as Gelendzhik Airport, about 32 km inland. Many ships were involved, and all of the ships' tracking systems placed them in the same nonsensical position. This led to the speculation that it could be attributed to one of the tests of satellite spoofing

technology by one of the space superpower states, whether as part of their electronic warfare arsenal or simply an anti-drone measure to protect very important persons (Androjna et al., 2020).

A practical example of geopolitical and geo-economic competition is the July 2019 detention of a British oil tanker, *Stena Impero*, which was seized by Iranian forces after her GPS used in the AIS message was tricked (spoofed) into changing her course to Iranian waters, as seen in Figure 1. As a result, the ship, cargo, and crew had become more than pawns in a geopolitical war (Bockmann, 2019). This incident could have been avoided if navigators were aware of the possibility of AIS spoofing and the potential impact on the MSA. They should never rely on a single source of information and should double-check data provided by AIS.

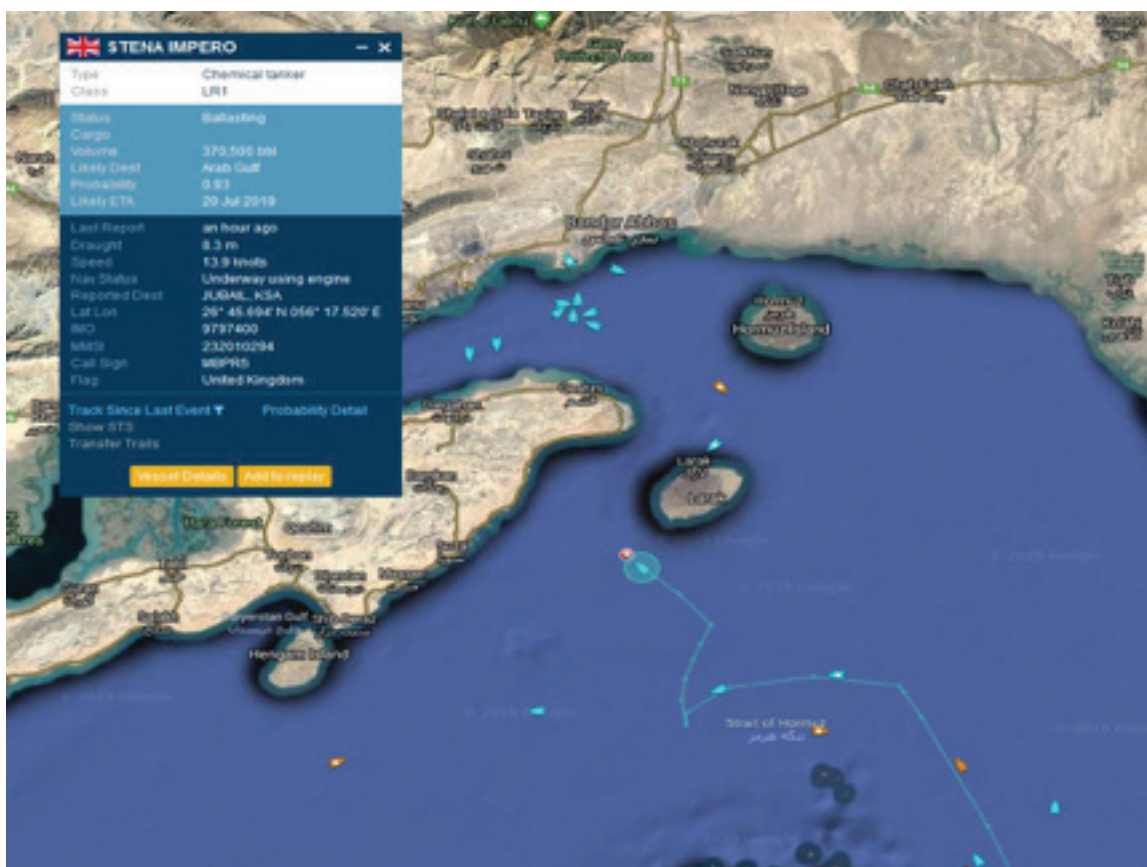


Figure 1. *Stena Impero* veered off course (Source: ClipperData, 2019).

At the same time, a mysterious new electronic device has emerged in China that spoofs AIS signals in ways experts have never seen before. There have been reports of several spoofing incidents discovered in over 20 coastal areas and ports that have been ongoing for months. Unlike “traditional” spoofing, GNSS signals were grouped into large circles, later referred to as “crop circles”, with the signals moving to the same position, resulting in a confusing traffic situation for ship pilots (Inside GNSS, 2019). Bergman (2019) observed that the locations of the “spoofing circles” were oil terminals. The timing of the spoofing, imposition of the US sanctions on the purchase of Iranian oil, and observations by others that Iranian oil was entering China suggest that some spoofing was being used to conceal these transactions.

Another example of spoofing was observed in July 2020 when one of the world’s top fishing fleets was accused of misreporting its location to conceal illegal fishing activities in the EEZ around the Galápagos Islands. The ships reported via AIS a location in New Zealand that was about 10,000 km from their observed location. In fact, they may have penetrated deep into the Galápagos EEZ, where illegal fishing has occurred, as shown in Figure 2 (Buesnel, 2020; HawkEye360, 2020). This kind of disappearance is just one of many ways criminals use location spoofing of a GNSS dependent system to support their nefarious activities.

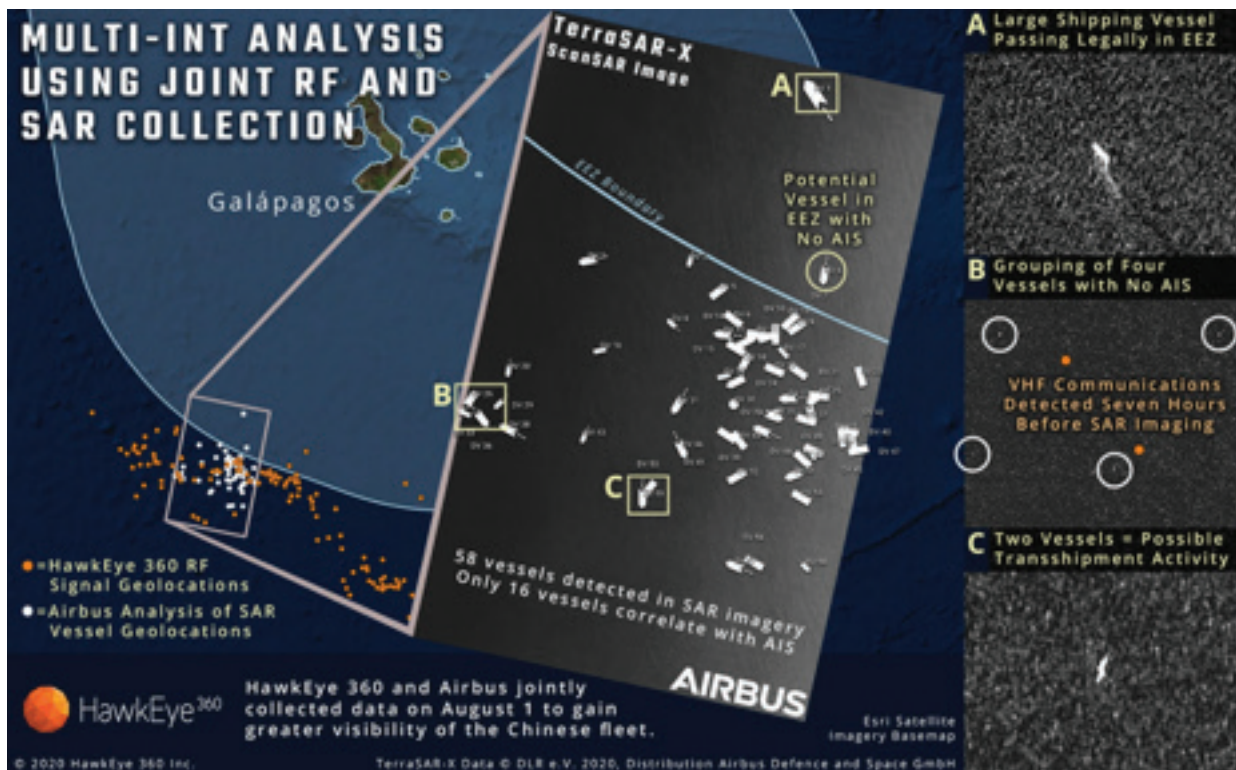


Figure 2. Vessels disappearance from AIS tracking, the Galápagos Islands (Source: HawkEye360, 2020).

3.3. AIS spoofing event near Elba Island – case study

In December 2019, a ship-spoofing situation occurred at an Italian AIS base station near Elba Island, which the European Maritime Safety Agency noticed. During the first Italian Coast Guard investigation, 870 different ships were displayed at two different times (13:13 and 13:28) with a duration of 3 min in the

first transmission and 2 min in the second. All tracks appeared in an area of 28 × 21 nautical miles between the islands of Elba and Corsica with different routes and speeds, which made it impossible to monitor the maritime traffic in this area and affected the real ship transmissions.

At the Faculty of Maritime Studies and Transport, University of Ljubljana, we thoroughly investigated the situation to support

EMSA's analysis and found 3,742 fake vessels (861 false tracks with MMSI 24480XXXX), which together generated 5,133 messages. Using the European Marine Observation and Data Network method, a traffic density map was created using vessel's position

data collected from terrestrial and satellite AIS data sources, maritime infrastructure and the SafeSeaNet Ecosystem Graphical Interface application. As shown in Figure 3, vessel density was up to 45 vessels/km² (Androjna et al., 2020).

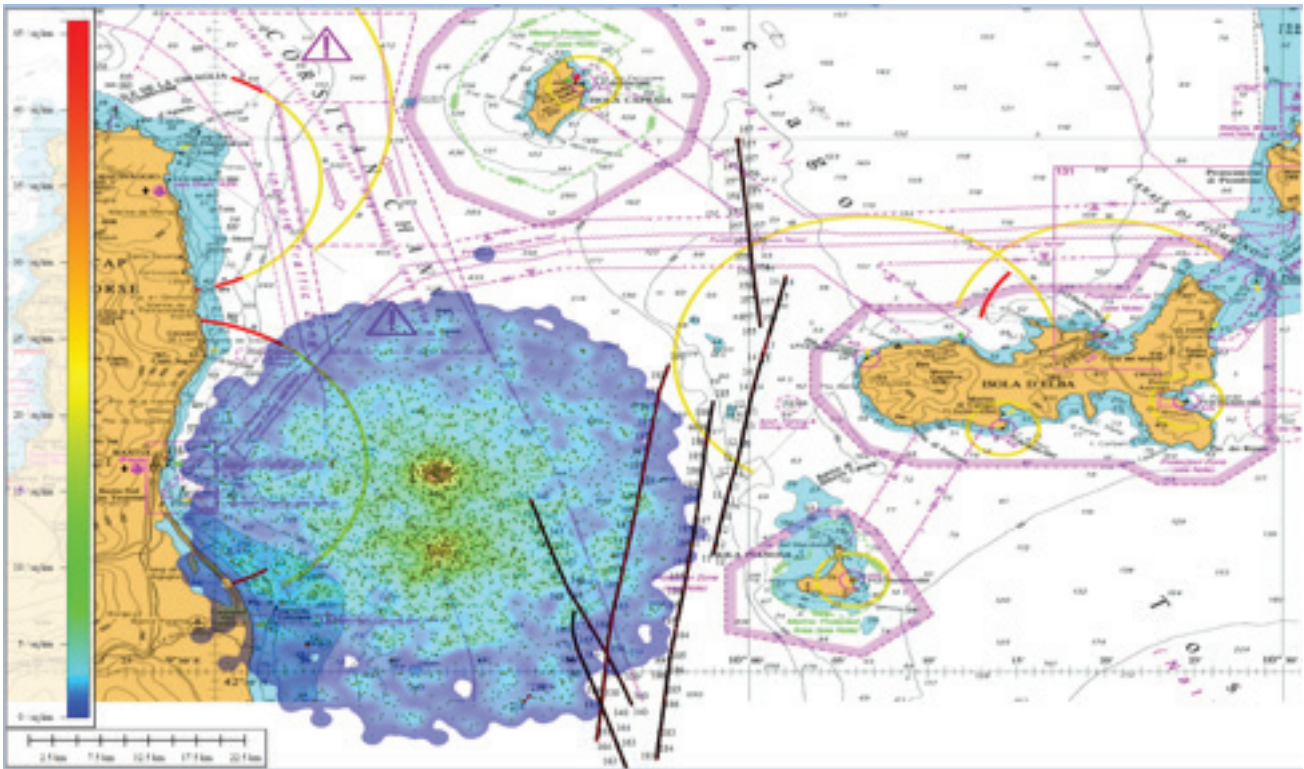


Figure 3.

AIS spoofing—shipping density near Island of Elba (Screenshot of Global Mapper, Admiralty Raster Chart background) (Source: Androjna et al., 2020, 2021).

AIS data was initially obtained by working with the Slovenian Maritime Administration, Italian Coastguard, MarineTraffic and VesselFinder. The archive data were again streamed using AIS Network Data Client application and fed into two different VTS applications Navi-Harbor (Wärtsilä) and Pelagus (Elman). The spoofing data AIS in the affected area is displayed in ECDIS and RADAR applications via the vessel tracking handling simulator Navi-Trainer Pro (Wärtsilä). A traffic density map was then constructed using vessel positioning data from the terrestrial and S-AIS data sources, maritime infrastructure, and the SafeSeaNet Ecosystem Graphical Interface application. We found that seven ships were in a spoofing cloud and that the broadcast system was congested. Thousands of AIS received streams (95% signal processing load) caused significant MSA degradation, as shown in Figure 4 (Androjna et al., 2021). They were identified as Dutch flag naval units, artificially generated, with different identification codes, positions, routes and speeds.

There were 3 AIS bursts, and “all” vessels were identified as passenger ships (AIS Type 60) 90 meters long and 24 meters wide, with no draft or destination information. Possible candidates for this AIS spoofing event include vessels with MMSI 999999999, which is quite common around AIS and often associated with naval vessels, MMSI 312320000, an individual fishery that assumed the identity of vessel scrapped in 2016, and MMSI 367309390. The obtained data indicate that a spoofing algorithm was run with automatically incrementing MMSI numbers. In our case study, it was not possible to determine the reasons for spoofing and the location of the sender that generated the false signals (Androjna et al., 2021).

The simulation of the spoofing event shows a potential impact on navigation safety. Ships in a spoofing cloud were on a collision course with more than a dozen other spoofed fake M/Vs, as shown in Figure 5.

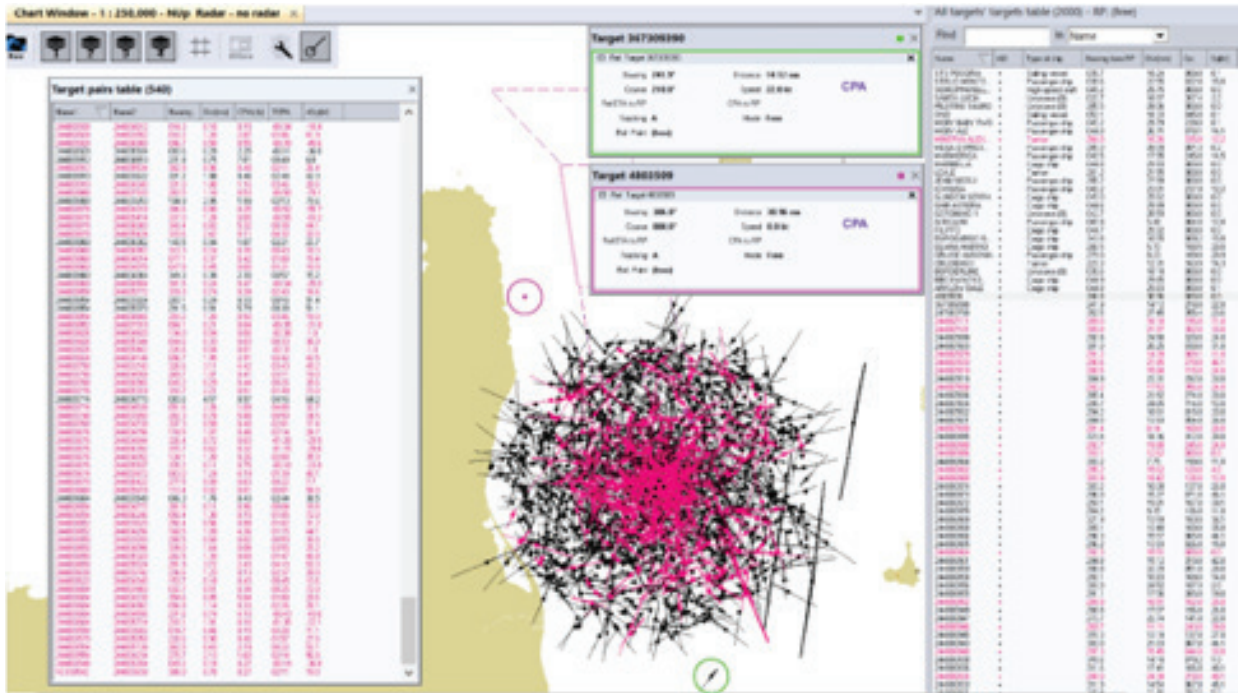


Figure 4. VTS system overload tested by Navi-Harbor (Wärtsilä) application.

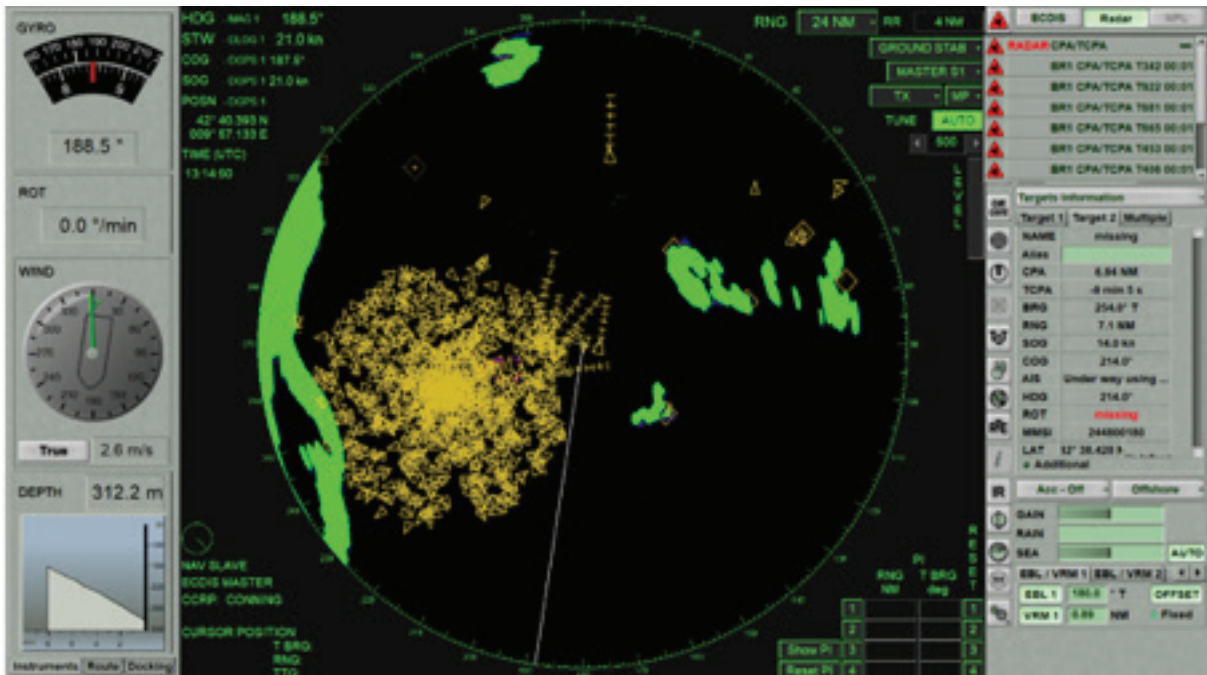


Figure 5. Collision course with the number of ships (Screenshot of Navi-RADAR 4000 ECDIS MFD, Navi-Trainer Professional 5000 Simulator, Wärtsilä) (Source: Androjna et al., 2021).

Consequently, a relatively large number of collision alerts appear, which may lead to an inappropriate OOW decision. In this situation, an experienced OOW will use a “raw” radar image without the AIS data support and enhance the sharp visual lookout. Fortunately, AIS spoofing event occurred during the day and in a favourable navigation area. Had it occurred at night and in a dense traffic sea area hazardous to navigation, navigation safety could have had severe consequences. Therefore, OOWs need to be aware of AIS spoofing and the potential impact on MSA.

4. CONCLUSIONS/DISCUSSION

In this article, the importance of cybersecurity is presented. GNSS spoofing has been an issue in defence for many years and is now beginning to affect shipping. As more devices and autonomous systems rely on GNSS, even more systems may be vulnerable to spoofing attacks. The maritime industry and shipping are not immune to such cyber-attacks. There will be many new cyber vulnerabilities in the future through which systems can be attacked if they are not adequately protected. Our analysis has shown that spoofing events like the one originating near the Island of Elba can affect ship security. Such a large number of ships appearing on ECDIS screen is primarily a technical problem that clearly creates a false scenario. In this mass of data, a vessel can be overlooked, so it is essential to use other means of safe navigation at the same time. If both AIS and GNSS, on which accurate positioning is based, are subject to spoofing, it may be unsafe to rely solely on ECDIS and its additional overlays. GNSS signals are essential for safe and efficient navigation. They are an integral part of maritime navigation, and their degradation threatens safety at sea.

Given the impact of digital technologies on maintaining seaworthiness, a robust defence against jamming and spoofing is required, i.e. a global cybersecurity framework. The maritime industry must stay ahead of the curve, so manufacturers must ensure the reliability, resilience, and function of multisensor systems for security and liability reasons. Confidentiality, authentication and message integrity of AIS data should remain preserved based on cryptographic data techniques and methods. Unfortunately, the cryptographic methods proposed by the scientific community have not been applied in practice. Therefore, AIS existing protocol is still unencrypted and vulnerable to cyber threats. This paper identifies the GNSS, ECDIS and AIS vulnerabilities that impact maritime security and recommends that the maritime community implement a robust cybersecurity system and use encrypted signals to protect against spoofing and other maritime cyber threats.

CONFLICT OF INTEREST: The authors declare no conflict of interest.

REFERENCES

- Androjna, A. et al., 2020. Assessing Cyber Challenges of Maritime Navigation. *Journal of Marine Science and Engineering*, 8(10), p.776. Available at: <http://dx.doi.org/10.3390/jmse8100776>.
- Androjna, A. & Twrdy, E., 2020. Cyber Threats to Maritime Critical Infrastructure. In: ČALETA, Denis (ur.), POWERS, James F. (ur.). *Cyber terrorism and extremism as threat to critical infrastructure protection*. E-ed. Ljubljana: Ministry of Defense, Republic of Slovenia; Institute for Corporate Security Studies; Tampa: Joint Special Operations University. Available at: https://dk.mors.si/Reader/Cyber_Terrorism_and_Extremism.html.
- Androjna, A. et al., 2021. AIS Data Vulnerability Indicated by a Spoofing Case-Study. *Applied Sciences*. 2021, 11, 5015. Available at: <https://doi.org/10.3390/app11115015>.
- Aziz, A. et al., 2020. SecureAIS - Securing Pairwise Vessels Communications. 2020 IEEE Conference on Communications and Network Security (CNS). Available at: <http://dx.doi.org/10.1109/cns48642.2020.9162320>.
- Balduzzi, M., Pasta, A. & Wilhoit, K., 2014. A security evaluation of AIS automated identification system. *Proceedings of the 30th Annual Computer Security Applications Conference*. Available at: <http://dx.doi.org/10.1145/2664243.2664257>.
- Bergman, B., 2019. Systematic GPS Manipulation Occurring at Chinese Oil Terminals and Government Installations. Available at: <https://skytruth.org/2019/12/systematic-gps-manipulation-occurring-at-chinese-oil-terminals-and-government-installations/>, accessed on: 10 May 2021.
- BIMCO, 2017. IHS-BIMCO-Survey-Findings—Story in Numbers. Available at: <https://cybersail.org/wp-content/uploads/2017/02/IHS-BIMCO-Survey-Findings.pdf>, accessed on: 25 April 2021.
- BIMCO, 2020. Safety at Sea and BIMCO cybersecurity white paper—IHS Markit 2020 Cyber Security Survey. Available at: https://ihsmarkit.com/info/0819/cyber-security-survey.html?utm_medium=website&utm_source=sas-news-article-1&utm_campaign=cyber-security-whitepaper, accessed on: 24 April 2021.
- BIMCO, 2020a. The Guidelines on Cyber Security Onboard Ships, Version 4. Available at: <https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships>, accessed on: 18 May 2021
- Bockmann, M., 2019. Seized UK Tanker Likely “Spoofed” by Iran. Available online: <https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-iran>, accessed on: 22 May 2021.
- Buesnel, G., 2020. Thousands of GMDSS jamming and spoofing incidents reported in 2020. Available at: <https://www.linkedin.com/pulse/thousands-gnss-jamming-spoofing-incidents-reported-2020-guy-buesnel/>, accessed on: 1 February 2021.
- Caponi, S.L. and Belmont, K.B., 2015. Maritime Cybersecurity: A Growing Threat Goes Unanswered. *Intellectual Property & Technology Law Journal*, 27(1), p.16.
- Caprolu, M. et al., 2020. Vessels Cybersecurity: Issues, Challenges, and the Road Ahead. *IEEE Communications Magazine*, 58(6), pp.90–96. Available at: <http://dx.doi.org/10.1109/mcom.001.1900632>.
- Chybowski, L., Gawdzińska, K. & Laskowski, R., 2019. Assessing the Unreliability of Systems during the Early Operation Period of a Ship—A Case Study. *Journal of Marine Science and Engineering*, 7(7), p. 213. Available at: <http://dx.doi.org/10.3390/jmse7070213>.
- ClipperData. ClipperData July 19, 2019 - the vessel took an abrupt turn north.

- Danish Maritime Cybersecurity Unit, 2018. Cyber and Information Security Strategy for the Maritime Sector 2019–2022. Available at: <https://www.dma.dk/Documents/Publikationer/Cyber%20and%20Information%20Security%20Strategy%20for%20the%20Maritime%20Sector.pdf>, accessed on: 24 April 2021.
- Dobryakova, L.A., Lemieszewski, L.S. & Ochinnikov, E.F., 2018. GNSS Spoofing Detection Using Static or Rotating Single-Antenna of a Static or Moving Victim. *IEEE Access*, 6, pp.79074–79081. Available at: <http://dx.doi.org/10.1109/access.2018.2879718>.
- EMSA, 2019. Traffic Density Mapping Service - Methodology. Ref. Ares (2019)4005069 - 24/06/2019. Available at: <http://www.emsa.europa.eu/related-projects/tdms.html>, accessed on: 28 April 2021.
- Eriksen, T., Greidanus, H. & Delaney, C., 2018. Metrics and provider-based results for completeness and temporal resolution of satellite-based AIS services. *Marine Policy*, 93, pp.80–92. Available at: <http://dx.doi.org/10.1016/j.marpol.2018.03.028>.
- EU, 2014. Council of the EU. European Union Maritime Security Strategy. 11205/14, Brussels. 24 June 2014. Available at: <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011205%202014%20INIT>, accessed on: 24 April 2021.
- EU, 2016. European Commission; High Representative. On the implementation of the EU Maritime Security Strategy Action Plan. Joint Staff Working Document SWD(2016)217 Final. Available at: https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/swd-2016-217_en.pdf, accessed on: 24 April 2020.
- EU, 2017. European Commission; High Representative. Second report on the implementation of the EU Maritime Security Strategy Action Plan. Joint Staff Working Document SWD(2017)238 Final. Available at: https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/swd-2017-238_en.pdf, accessed on: 24 April 2021.
- EU, 2018. Council of the EU. Revised European Union Maritime Security Strategy (EUMSS) Action Plan. Annex to 10494/18, Brussels. 26 June 2018. Available at: <https://data.consilium.europa.eu/doc/document/ST-10494-2018-INIT/en/pdf>, accessed on: 24 April 2021.
- EU, 2020. European Commission; High Representative. Report on the implementation of the revised EU maritime security strategy action plan. In Joint Staff Working Document; European Commission: Brussels, Belgium, 2020; in draft.
- Goudosis, A. & Katsikas, S., 2020. Secure AIS with Identity-Based Authentication and Encryption. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 14(2), pp.287–298. Available at: <http://dx.doi.org/10.12716/1001.14.02.03>.
- Goudossis, A. & Katsikas, S.K., 2018. Towards a secure automatic identification system (AIS). *Journal of Marine Science and Technology*, 24(2), pp.410–423. Available at: <http://dx.doi.org/10.1007/s00773-018-0561-3>.
- Hareide, O.S. et al., 2018. Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. *Journal of Navigation*, 71(5), pp.1025–1039. Available at: <http://dx.doi.org/10.1017/s0373463318000164>.
- HawkEye360, 2020. Chinese Fishing Fleet Encroaches on the Galapagos Islands: HawkEye360 Monitors the Fleet for Suspicious Behavior and Potential Illegal Fishing. Available at: <https://www.he360.com/insight/potential-illegal-fishing-seen-from-space/>, accessed on: 30 May 2021.
- Hecht, H., Berking, B., Jonas, M. & Woster, M., 2017. *The Electronic Chart Fundamentals, functions, data and other essentials, A Textbook for ECDIS Use and Training 4th Edition*, The Netherlands, Geomares Publishing.
- IALA, 2016. IALA Guideline - An overview of AIS, Edition 2.0. Available at: https://www.navcen.uscg.gov/pdf/IALA_Guideline_1082_An_Overview_of_AIS.pdf, accessed on 14 May 2021.
- IEC, 2019. International Electrotechnical Commission. *Maritime Navigation and Radiocommunication Equipment and Systems-Cybersecurity-General Requirements, Methods of Testing and Required Test. Results*; IEC 63154 ED1; IEC, Geneva, Switzerland.
- IHO, 2020. IHO Data Protection Scheme, Edition 1.2.1, Monaco.
- IMO, 2017. IMO Resolution MSC.428 (98). Available at: [http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428\(98\).pdf](http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428(98).pdf), accessed on 24 April 2021.
- IMO, 2017a. Guidelines on Cyber Risk Management. Maritime Safety Committee: 2017, MSC-FAL (1/Circ.3). pp. 1–6. Available at: [http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSCFAL1Circ.3%20%20Guidelines%20on%20Maritime%20Cyber%20Risk%20Management%20\(Secretariat\).pdf](http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSCFAL1Circ.3%20%20Guidelines%20on%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf), accessed on: 24 April 2021.
- IMO, 2018. ISM. International Safety Management Code; IMO Publishing: London, UK, 2018.
- IMO, 2020. *The International Convention for Safety of Life at Sea (Consolidated edition 2020)*; IMO Publishing, London, UK, 2020; pp. 15/34-15/35. ISBN: 9789280116908.
- Inside GNSS, 2019. Sinister Spoofing in Shanghai. Available at: <https://insidengnss.com/sinister-spoofing-in-shanghai/#:~:text=Someone%20has%20updated%2019th%20century,experts%20have%20never%20seen%20before>, accessed on: 10 May 2021.
- INTERTANKO, 2019. Jamming and Spoofing of Global Navigation Satellite Systems (GNSS). Available at: <https://www.maritimelglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf>, accessed on: 24 April 2021.
- ITU, 2014. ITU-R M.2287-0. Automatic identification system VHF data link loading.
- Jones, K.D., Tam, K. & Papadaki, M., 2012. Threats and Impacts in Maritime Cyber Security. *Engineering & Technology Reference*, 1(1). Available at: <http://dx.doi.org/10.1049/etr.2015.0123>.
- Kessler, G.C., 2020. Protected AIS: A Demonstration of Capability Scheme to Provide Authentication and Message Integrity. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 14(2), pp.279–286. Available at: <http://dx.doi.org/10.12716/1001.14.02.02>.
- Kjerstad, N., 2016. *Electronic and Acoustic Navigation Systems*, Alesund, Norway, Norwegian Institute of Science and Technology, ISBN: 978-82-92186-57-2.
- Marine Insight, 2020. Maritime Cyber-Attacks Increase by 900% in Three Years. Available at: <https://www.marineinsight.com/shipping-news/maritime-cyber-attacks-increase-by-900-in-three-years/#>, accessed on: 24 April 2021.
- 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*, 71(4).
- Natale, F. et al., 2015. Mapping Fishing Effort through AIS Data G. Tserpes, ed. *PLOS ONE*, 10(6), p.e0130746. Available at: <http://dx.doi.org/10.1371/journal.pone.0130746>.
- Piercy, N. & Giles, W., 1989. Making SWOT Analysis Work. *Marketing Intelligence & Planning*, 7(5/6), pp.5–7. Available at: <http://dx.doi.org/10.1108/eum000000001042>.
- Ramin, A., Mustafa, M. & Ahmad, S., 2020. Prediction of Marine Traffic Density Using Different Time Series Model From AIS data of Port Klang and Straits of Malacca. *Transactions on Maritime Science*, 9(2). Available at: <http://dx.doi.org/10.7225/toms.v09.n02.006>.

Sciancalepore, S. et al., 2021. Auth-AIS: Secure, Flexible, and Backward-Compatible Authentication of Vessels AIS Broadcasts. IEEE Transactions on Dependable and Secure Computing, pp.1-1. Available at:
<http://dx.doi.org/10.1109/tdsc.2021.3069428>.

Svilicic et al., 2019. A Study on Cyber Security Threats in a Shipboard Integrated Navigational System. Journal of Marine Science and Engineering, 7(10), p.364. Available at:
<http://dx.doi.org/10.3390/jmse7100364>.

Thornton, P., 2016. The ECDIS Manual, Reformatted 1st edition, Scotland, Witherby Publishing Group.

Weinrit, A., 2010. The Electronic Chart Display and Information System (ECDIS): An Operational Handbook, Poland, Gdynia Maritime University.