CENTRE FOR SECURITY STUDIES | ARTICLE

January 2022

MARITIME SECURITY AND THE MISUSE OF AIS

Mihir Vikrant Kaulgud
Edited By: Aakrith Harikumar

This research article explores the issue of misuse of AIS (Automatic Identification System) which is a part of maritime cybersecurity, a growing area of concern globally. The first section focuses on the issue of maritime cybersecurity. The second and third sections focus on the basics of AIS and its security risks respectively. The fourth section discusses the various cases of misuse of AIS, which have mostly been linked to China and Russia. Finally, the article concludes by highlighting efforts to curb AIS misuse and strategies scholars have suggested governments and international organizations use.

Maritime Cybersecurity

As global maritime systems have grown in scale and complexity, the technology employed to assist these systems has also grown in sophistication. Cyber technology is critical to several facets of the maritime systems infrastructure such as seaport operations, cargo and shipping logistics, vessel traffic management, shipping line operations, and individual vessel operations.[1] There is an increasing integration of these systems, driven by market forces and progress in technology.[2] Therefore, the cybersecurity vulnerabilities of individual systems are compounded and multiplied in networks of those systems. One network can provide access to other networks, creating a "ripple effect" throughout a section of the system.[3] Therefore, the difficulty lies not in protecting individual vessels from cyber threats but in securing the broader "system of systems." This difficulty is compounded due to the myriad vendors, manufacturers and jurisdictions at play and the lack of a central authority that controls the broader system.[4] Due to these issues, the chances and consequences of system failure increase with increasing interconnectedness.[5]

Cybersecurity threats are either rooted in human error or malicious actors that exploit system vulnerabilities and human errors. Maritime cyberattacks, whether state-sponsored or not, can aid

[1] Kessler, Gary C. "Cybersecurity in the maritime domain." *USCG Proceedings of the Marine Safety & Security Council* 76, no. 1 (2019). https://commons.erau.edu/cgi/viewcontent.cgi?article=2377&context=publication
[2] DiRenzo, Joseph, Dana A. Goward, and Fred S. Roberts. "The little-known challenge of maritime cyber security." In 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA), pp. 1-5. IEEE, 2015. http://archive.dimacs.rutgers.edu/People/Staff/froberts/MaritimeCyberCorfuPaper.final.pdf.
[3] Kessler, "Cybersecurity in the Maritime Domain"
[4] Ibid.
[5] DiRenzo, Goward and Roberts. "The little-known challenge of maritime cyber security."

physical attacks such as piracy, theft, or destruction. These cyber-attacks can also be remotely executed, remaining stealthy and "below the radar. [6]" Therefore, they can be used in espionage or stealthy disruption of naval activity. Such attacks and disruptions affect both military and commercial naval activity. Around 90% of the world's trade happens by sea.[7] So, the Maritime Transportation System (MTS) is crucial for the world economy.[8] Cyber-attacks can disrupt businesses and generate losses by damaging goods, making them incur fines or legal issues.[9] Such attacks can also be pursued with a view of harming a particular state or region's economy or reputation.

They can cause damage to marine environments as well, in the case of manipulating technology to pollute outside of established norms and regulations. Other concerns include piracy, illegal fishing, and trafficking of people and illegal goods.[10] Therefore, while maritime security is concerned with protecting vessels and ports, it has implications for national, economic, environmental, and human security. Maritime cyber tech aids in cargo-related functions, propulsion, and navigation. Navigational systems such as the Electronic Chart Display System (ECDIS), Global Positioning Satellite (GPS), and AIS aim to aid crew members to accurately position their vessel and avoid getting lost or damaging other vessels or property. This involves transmitting and exchanging large amounts of crucial information about a given vessel and its position.[11]

[6] Jones, Kevin D., Kimberly Tam, and Maria Papadaki, "Threats and Impacts in Maritime Cyber Security," *Engineering & Technology Reference* (2016), https://pearl.plymouth.ac.uk/bitstream/handle/10026.1/4387/Jones_Tam_Papadaki_2016_Threats_and_%20Impacts_in_Maritime_Cyber_Security_Final.pdf?sequence=3

[7] Kraetzig, Nikita Marwaha "An Overview of Maritime and Port Security," *UP42 Official Website*, March 22, 2021, https://up42.com/blog/tech/an-overview-of-maritime-and-port-security.

[8] Jones, Tam, and Papadaki, "Threats and Impacts in Maritime Cyber Security."
[9] Ibid.
[10] Kraetzig, "An Overview of Maritime and Port Security."
[11] Jones, Tam, and Papadaki, "Threats and Impacts in Maritime Cyber Security."

Overview of AIS

Automatic Identification System was primarily designed to be a collision avoidance tool.[12] It transmits ship information such as ship details, position, speed, and course automatically to other ships and shore stations. AIS works by regularly exchanging dynamic navigational information and static data about ship details via Very High Frequency (VHF) radio transmissions between ships and maritime authorities.[13] It was standardized by the International Telecommunication Union (ITU) and adopted by the International Maritime Organization (IMO).[14] In 2002, under the Safety of Life Regulations (SOLAS), the IMO mandated that Class-A AIS transponders be fitted on all ships with a gross tonnage 300 or more, engaged in international voyages. Moreover, even if not engaged in international voyages, AIS is required on all cargo ships upwards of 500 gross tonnes and all passenger ships irrespective of size.[15]

According to the IMO, AIS must be switched on and transmitting/receiving at all times, except "when international agreements, rules or standards protect navigational information." AIS signals are picked up by other vessels or land-based receivers that are in range (10-30 miles). If not in range, the signals are picked up by satellite AIS receivers.[16] With a growing demand from smaller vessels exempt from the SOLAS mandate, Class B transponders were developed by 2003.[17] Over time, the use of AIS has branched out from the initial concern with anti-collision. Consequently, specialized AIS products, services and providers have emerged to fulfil different functions.[18] For example, Search and Rescue operations have begun to AIS SARTs (Search and Rescue Transmitters). Not insignificantly, they can improve the traffic control efficiency of harbours. For this paper, it is important to note that:

[12] "AIS Transponders," *International Maritime Organization*, 2019, https://www.imo.org/en/OurWork/Safety/Pages/AIS.aspx
[13] Balduzzi, Marco, Kyle Wilhoit, and Alessandro Pasta. "A security evaluation of AIS." *Trend Micro* (2014): 1-9.
[14] "AIS Frequently Asked Questions," *Navigation Center United States Coast Guard*, 2021, https://www.navcen.uscg.gov/?pageName=AISFAQ#5.
[15] "AIS Transponders," *International Maritime Organization*, 2019.
[16] "Land-Based and Satellite AIS Tracking - What's the Difference?," *ShipTracks*, July 24, 2019, https://shiptracks.com/updates/2019/07/24/satellite-vs-land-based-ais-tracking//
[17] Simon Tucker, "AIS History," *All About AIS*, 2012, http://www.allaboutais.com/index.php/en/aisbasics1/ais-history.
[18] Ibid.

1. AIS can be used for monitoring the security of sovereign maritime borders, identifying vessels that cross them and managing potential threats.[19]

2. AIS data and vessel tracking are almost always widely available on the internet via services like Marine Traffic and AISLive. These services display AIS targets either from their land-based receivers or use firms like Orbcomm, exactEarth and Spacequest to obtain satellite data.[20]

Security Risks of AIS

The design and functionality of AIS infrastructure have left it open to security risks, either due to dishonest usage by vessels or malicious meddling with a given vessel's AIS transmissions. The AIS system was meant to be a public safety tool. The IMO still maintains that this is the primary goal. Moreover, AIS standards employed by the IMO do not include message confidentiality or authentication of participating users.[21] The US Coast Guard Navigation Center notes that AIS is built to be an "open, non-proprietary, unencrypted, and unprotected radio system, intended to operate on non-secure VHF-FM channels.[22]" Therefore, virus or malware protection is not built into AIS devices. This reflects the fact that AIS was developed before cybersecurity became a major concern and opened the AIS network to many cybersecurity risks. Due to its open nature, AIS seems to run on the good faith that the information vessels are transmitting is indeed accurate.[23] To this end, the US Coast Guard recommends a "trust, but verify" approach. Since the pathways available to verification are time-consuming, they cannot be easily pursued in real-time. With a growing reliance on the maritime world's critical functions on cyber technology, this trusting approach seems to be vulnerable to exploitation and undermining by either state or non-

[19] Simon Tucker, "AIS applications," *All About AIS*, 2012, http://www.allaboutais.com/index.php/en/aisbasics1/ais-history.
[20] "Introduction to Automatic Identification Systems (AIS)" Spire : Global Data and Analytics, November 12, 2021.
[21] Litts, Robert E. "Security Improvements for the Automatic Identification System." (2021) https://digitalcommons.odu.edu/cgi/viewcontent.cgi?article=1225&context=ece_etds
[22] "AIS Frequently Asked Questions," *Navigation Center United States Coast Guard*, 2021.
[23] Litts. "Security Improvements for the Automatic Identification System." (2021)

state actors. The levels of sophistication of security breaches can vary from using Software-defined radio (SDR) and antennas[24]to using malicious email attachments.[25] Attackers often encourage and/or exploit human error in using the software. They are capable of sophisticated and coordinated attacks on a large scale. While encrypted AIS systems exist for vessels used in law enforcement, a secure public system is missing.[26] As mentioned earlier, the necessity of a secure public system ("system of systems") is immense due to the ripple effect caused by a security breach in one node of the network. Ghosting, hijacking, and spoofing of data are among major concerns when it comes to AIS security. There are a variety of threats that Balduzzi, Pasta and Wilhoit[27] have identified in their research as possibilities:

- Ship Spoofing: A malicious actor can create a fictitious ship and dynamic information for that fake ship - its course, speed, position, and destination. For instance, an attacker can create a scenario where a state's ship seems to be venturing into the waters of an enemy state, prompting it to take counteraction.

- Aids-to-Navigation Spoofing: Since AIS provides aids to navigation, an attacker can create false information about other vessels, buoys, or hazards like reefs to lure a ship off its course or make the wrong manoeuvre.

- Collision Spoofing: AIS primarily aims to assist ships to avoid collisions. An attacker can fake an on-board alert, which says that the ship is on a collision course and make the ship turn off course to avoid the faked collision.

- AIS-SART spoofing: The search and rescue functionality of AIS can be manipulated into making a ship attend a fake distress call, upon which a vessel is usually obliged to attend to the rescue operation.

- AIS Hijacking: The information transmitted, or signal used by existing AIS transponders of vessels can be taken over, modified, and/or replaced by malicious actors. For example, the AIS information provided by port authorities can be modified to meddle with a ship.

[24] Ibid.
[25] Kessler, "Cybersecurity in the maritime domain
[26] Litts, Robert E. "Security Improvements for the Automatic Identification System." (2021)
[27] Balduzzi, Wilhoit, and Pasta. "A security evaluation of AIS." (2014).

Vessels can be instructed to change frequencies that they are operating on and be completely in the hands of the hijackers.

Other possibilities include spoofing the weather forecast information ships receive (luring them into a storm) or jamming, disabling, or delaying AIS transmission of one or more ships. Not all of these possibilities have been implemented by cybercriminals. Moreover, in addition to the concerns mentioned above, AIS can simply be turned off or tampered with (contrary to IMO and several national regulations) to create an opening for activities such as illegal fishing or sanction evasion.

Misuse of AIS

AIS-equipped vessels have proliferated the misuse and abuse of this technology once thought to be a benign collision avoidance tool. There have been several reports and allegations of misuse by fishermen, shipping companies, chartered vessels, and rogue states. This has included vessels switching off AIS against regulations and becoming undetectable or hacking into the AIS systems to create ghost ships. Another kind of AIS misuse has been reported from the East China Sea, where fishermen installed AIS transponders on several buoys and fishing nets.[28] Vessels passing through those waters would register the buoys or nets on their ECDIS as other vessels, prompting their crew to chart a new course. But even after changing course, new AIS targets show up from more fishing nets and buoys. The ECDIS is overloaded and cannot distinguish between real ships and nets. This poses a danger to navigation. Ships may have to venture a considerable distance from their original course to find waters less clogged up with AIS targets. A similar misuse was detected by Global Fishing Watch, which used satellite data to track hundreds of illegal Chinese fishing vessels near North Korea.[29] These vessels were only detectable by satellite because they had turned their AIS transponders off. They were traced back to Chinese waters and ports. But

[28] Kovary, Laura "AIS Problems Revealed in East China Sea," *gCaptain*, December 27, 2018, https://gcaptain.com/ais-problems-revealed-in-east-china-sea/.
[29] David Hambling, "Hundreds of Illegal Chinese Fishing Vessels Spotted near North Korea," New Scientist (New Scientist, July 22, 2020), https://www.newscientist.com/article/2249582-hundreds-of-illegal-chinese-fishing-vessels-spotted-near-north-korea/

usually, such illegal vessels do not sail with registration papers or under the Chinese flag, making them difficult to regulate. This poses a problem for accountability and security-enforcement measures. In 2019, the United States government discovered that Chinese shipping companies were turning off their AIS transponders to ship Iranian oil.[30] In a bid to stop Iran's nuclear program, erstwhile president Trump had imposed sanctions on Iranian oil exports. China remained a buyer of Iranian oil, and the U.S caught one of their shipping companies transporting oil from Iran. The vessels of that company soon stopped transmitting their location via AIS, remaining undetectable for days. Thus, we see how AIS can be misused to skirt past sanctions imposed on a country. More questions were raised in early 2021 when a Chinese survey ship was caught sailing by the Indonesian coast guard without AIS near the Sunda Strait.[31] This is a strategically important strait, located at one of the choke points between the South China Sea and the Indian Ocean. It is unclear whether the ship was gathering naval intelligence, but it raised suspicions as it comes after the discovery of Chinese Unmanned Underwater Vehicles (UUVs) in Indonesian waters.

Another major concern is that many AIS transponders are manufactured in China and sold cheaply in the market. The Indian Coast Guard has reported several Indian vessels using Chinese AIS, despite having access to government-subsidized equipment. Chinese equipment is prone to glitching and identifies the vessels as Chinese. This poses problems for identifying navigation routes, tracking illegal fishing, and potential search and rescue operations. In June 2021, there was serious AIS abuse involving spoofing when a British warship - HMS Defender, and a Dutch frigate - HNLMS Evertsen were detected approaching Sevastopol in Crimea.[32] Russia controls these waters, even though other countries consider them Ukrainian. It was later discovered that these ships were docked in Odessa, and a hacker had virtually spoofed their course. Even though the misunderstanding was cleared up, it is a sign that international conflict could be sparked by the simple manipulation of AIS systems. A similar incident occurred with the Swedish Navy in the Baltic Sea when nine of their vessels' locations were spoofed to show them to be near

[30] Timothy Gardner, "U.S. 'Deeply Concerned' about Untrackable China Ships Carrying Iran Oil: Officials," *Reuters*, October 16, 2019, https://www.reuters.com/article/us-usa-iran-china-tankers-idUSKBN1WV0SE.
[31] H I Sutton, "Chinese Survey Ship Caught 'Running Dark' Give Clues to Underwater Drone Operations" *United States Naval Insitute*, January 16, 2021, https://news.usni.org/2021/01/16/chinese-survey-ship-caught-running-dark-give-clues-to-underwater-drone-operations.
[32] Tom Bateman, "Fake Ships, Real Conflict: How Misinformation Came to the High Seas," *Euro News*, June 28, 2021 https://www.euronews.com/next/2021/06/28/hms-defender-ais-spoofing-is-opening-up-a-new-front-in-the-war-on-reality

Kaliningrad.[33] The false AIS targets were indistinguishable from real ones and could only be confirmed as false after much coordination. Analysts have also found AIS tracks from simulated sailing races which were also uploaded to public AIS sites. Such false data interfere with real-time navigation and opens up questions about the integrity of AIS, which has become a crucial component of contemporary safe navigation. Global Fishing Watch confirmed, "false AIS positions for 15 navy vessels from seven countries, with many more vessels suspected of having fabricated positions." From patterns of these confirmed cases, nearly 100 naval vessels were identified to have had their AIS tracks falsified or spoofed.[34] There have been several such spoofing incidents confirmed or at least suspected.[35] Those affected seem to always be European or NATO vessels.[36]

Need and Possibility for Management

Maritime security demands that ways of managing and regulating AIS systems be found urgently. Both awareness and policy are needed.[37] Furthermore, this management needs to be collective because of the global nature of the maritime industry and security. The urgency is amplified when countries unilaterally begin creating laws about AIS that set the agenda, solidify their unilateral geopolitical interests, and put other countries on the backfoot economically and militarily. Such is the case with China. Recently, China passed a law that requires vessels that carry certain types of cargo to provide detailed information to the Chinese authorities when transiting through Chinese "territorial waters."[38] This is being interpreted as "lawfare" - another means China is using to cement its claim on the South China Sea, where it has been building military facilities on artificial

[33]Bjorn Bergman, "Systematic Data Analysis Reveals False Vessel Tracks," *Global Fishing Watch*, July 29, 2021 https://globalfishingwatch.org/data/analysis-reveals-false-vessel-tracks/
[34] Bjorn Bergman, "Systematic Data Analysis Reveals False Vessel Tracks," SkyTruth, July 29, 2021, https://skytruth.org/2021/07/systematic-data-analysis-reveals-false-vessel-tracks/
[35] Androjna, Andrej, Marko Perkovič, Ivica Pavic, and Jakša Mišković. "AIS Data Vulnerability Indicated by a Spoofing Case-Study." *Applied Sciences* 11, no. 11 (2021): 5015. https://www.mdpi.com/2076-3417/11/11/5015
[36] Mark Harris, "Phantom Warships Are Courting Chaos in Conflict Zones," *Wired*, July 29, 2021, https://www.wired.com/story/fake-warships-ais-signals-russia-crimea/
[37] Tam, Kimberly, and Kevin D. Jones. "Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping." *Journal of Cyber Policy* 3, no. 2 (2018): 147-164
[38] Manoj Joshi "How Beijing's New Maritime Rules in the South China Sea Will Affect India and Others," *The Wire*, 2018, https://thewire.in/south-asia/explained-what-lies-behind-beijings-new-maritime-rules-in-south-china-sea.

islands to claim “territorial waters" status. On 1 November, China passed two privacy laws that prevented Chinese firms from allowing foreign access to any data critical to China’s security or infrastructure. This has confused Chinese territorial AIS stations, after which they have subsequently stopped transmitting AIS data. This has further eroded the transparency of AIS and made it impossible to track vessels in and around China. Luft, Gonin and Pietraszewski[39], writing for the U.S Coast Guard, recommend international cooperation on the creation of “AIS 2.0.” This would begin with an international review of AIS and cybersecurity implications so that the technical requirements for the next generation of AIS systems can be defined. Moreover, they recommend that “defensive and offensive real-time cybersecurity methods and countermeasures” be deployed as soon as possible.[40]

Other scholars recommend taking technical tips from the aviation industry to make AIS more secure, including reinforcing methods of authenticating AIS targets in real-time and through predictive methods (using old AIS data to determine a verifiable pattern).[41] Several technical possibilities are being suggested in terms of different cryptography techniques as well.[42] Legally speaking, countries including India must incorporate AIS related clauses into their maritime contracts.[43] There can be international coordination regarding the same, with advanced states assisting the developing ones. Crew training can be implemented and standardized internationally to help crew identify anomalous AIS data and deal with threats. Codified procedures and operations checklists can be developed to prevent human error driven cyberthreats. It is clear that with growing maritime cybersecurity threats like AIS misuse, there is a need to create a robust international framework to deal with them through skill development, technical improvements, and legal means.

[39] Luft, Lee, Irene Gonin, and David Pietraszewski. “Researching Technology Improvements of AIS.” *United States Homeland Center Acquisition Directorate*, 2018. https://apps.dtic.mil/sti/pdfs/AD1060714.pdf
[40] Ibid. pg. 33
[41] Kessler, Gary C., J. Philip Craiger, and Jon C. Haass. "A taxonomy framework for maritime cybersecurity: A demonstration using the automatic identification system." *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation* 12, no. 3 (2018): 429.
[42] Goudossis, Athanassios, and Sokratis K. Katsikas. "Towards a secure automatic identification system (AIS)." *Journal of Marine Science and Technology* 24, no. 2 (2019): 410-423. https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2627210/Goudossis.pdf?sequence=4
[43] “India - the Need for Automatic Identification System (AIS) Clause in Indian Maritime Contracts” *Conventus Law*, 2020, https://www.conventuslaw.com/report/india-the-need-for-automatic-identification-system/

*****

Mihir Vikrant Kaulgud is a postgraduate student at the Jindal School of International Affairs and is an Editor at the Centre for Security Studies, JSIA. All views expressed in this publication belong to the author and do not reflect the opinion of the Centre for Security Studies.

Bibliography

"AIS Transponders," *International Maritime Organization*, 2019, https://www.imo.org/en/OurWork/Safety/Pages/AIS.aspx

"AIS Frequently Asked Questions," *Navigation Center United States Coast Guard*, 2021, https://www.navcen.uscg.gov/?pageName=AISFAQ#5.

Androjna, Andrej, Marko Perkovič, Ivica Pavic, and Jakša Mišković. "AIS Data Vulnerability Indicated by a Spoofing Case-Study." *Applied Sciences* 11, no. 11 (2021): 5015. https://www.mdpi.com/2076-3417/11/11/5015

Balduzzi, Marco, Kyle Wilhoit, and Alessandro Pasta. "A security evaluation of AIS." *Trend Micro* (2014): 1-9.

Bateman, Tom. "Fake Ships, Real Conflict: How Misinformation Came to the High Seas," *Euro News*, June 28, 2021 https://www.euronews.com/next/2021/06/28/hms-defender-ais-spoofing-is-opening-up-a-new-front-in-the-war-on-reality

Bergman, Bjorn "Systematic Data Analysis Reveals False Vessel Tracks," *Global Fishing Watch*, July 29, 2021 https://globalfishingwatch.org/data/analysis-reveals-false-vessel-tracks/

DiRenzo, Joseph, Dana A. Goward, and Fred S. Roberts. "The little-known challenge of maritime cyber security." In 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA), pp. 1-5. IEEE,

Goudossis, Athanassios, and Sokratis K. Katsikas. "Towards a secure automatic identification system (AIS)." *Journal of Marine Science and Technology* 24, no. 2 (2019): 410-423. https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2627210/Goudossis.pdf?sequence=4

Gardner, Timothy "U.S. 'Deeply Concerned' about Untrackable China Ships Carrying Iran Oil: Officials," U.S., October 16, 2019, https://www.reuters.com/article/us-usa-iran-china-tankers-idUSKBN1WV0SE.

Hambling, David. "Hundreds of Illegal Chinese Fishing Vessels Spotted near North Korea," New Scientist (New Scientist, July 22, 2020), https://www.newscientist.com/article/2249582-hundreds-of-illegal-chinese-fishing-vessels-spotted-near-north-korea/

Harris, Mark, “Phantom Warships Are Courting Chaos in Conflict Zones,” *Wired*, July 29, 2021, https://www.wired.com/story/fake-warships-ais-signals-russia-crimea/

“India - the Need for Automatic Identification System (AIS) Clause in Indian Maritime Contracts” *Conventus Law*, 2020, https://www.conventuslaw.com/report/india-the-need-for-automatic-identification-system/.

“Introduction to Automatic Identification Systems (AIS)” Spire : Global Data and Analytics, November

Jones, Kevin D., Kimberly Tam, and Maria Papadaki, “Threats and Impacts in Maritime Cyber Security,” *Engineering & Technology Reference* (2016), https://pearl.plymouth.ac.uk/bitstream/handle/10026.1/4387/Jones_Tam_Papadaki_2016_Threats_and_%20Impacts_in_Maritime_Cyber_Security_Final.pdf?sequence=3

Joshi, Manoj “How Beijing’s New Maritime Rules in the South China Sea Will Affect India and Others,” *The Wire*, 2018, https://thewire.in/south-asia/explained-what-lies-behind-beijings-new-maritime-rules-in-south-china-sea.

“Land-Based and Satellite AIS Tracking - What's the Difference?,” *ShipTracks*, July 24, 2019, https://shiptracks.com/updates/2019/07/24/satellite-vs-land-based-ais-tracking/

Litts, Robert E. "Security Improvements for the Automatic Identification System." (2021) https://digitalcommons.odu.edu/cgi/viewcontent.cgi?article=1225&context=ece_etds

Kessler, Gary C. "Cybersecurity in the maritime domain." *USCG Proceedings of the Marine Safety & Security Council* 76, no. 1 (2019). https://commons.erau.edu/cgi/viewcontent.cgi?article=2377&context=publication

Kessler, Gary C., J. Philip Craiger, and Jon C. Haass. "A taxonomy framework for maritime cybersecurity: A demonstration using the automatic identification system." *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation* 12, no. 3 (2018): 429.

Kovary, Laura “AIS Problems Revealed in East China Sea,” *gCaptain*, December 27, 2018, https://gcaptain.com/ais-problems-revealed-in-east-china-sea/.

Kraetzig, Nikita Marwaha “An Overview of Maritime and Port Security,” *UP42 Official Website*, March 22, 2021, https://up42.com/blog/tech/an-overview-of-maritime-and-port-security.

Luft, Lee, Irene Gonin, and David Pietraszewski. “Researching Technology Improvements of AIS.” *United States Homeland Center Acquisition Directorate*, 2018. https://apps.dtic.mil/sti/pdfs/AD1060714.pdf

Sutton, H.I, “Chinese Survey Ship Caught ‘Running Dark’ Give Clues to Underwater Drone Operations” *United States Naval Insitute*, January 16, 2021, https://news.usni.org/2021/01/16/chinese-survey-ship-caught-running-dark-give-clues-to-underwater-drone-operations.

Tam, Kimberly, and Kevin D. Jones. "Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping." *Journal of Cyber Policy* 3, no. 2 (2018): 147-164

Tucker, Simon “AIS History,” *All About AIS*, 2012, http://www.allaboutais.com/index.php/en/aisbasics1/ais-history.