Maritime Cybersecurity: AIS Manipulation Motivations in the Maritime Domain

Aurora Thomas

Department of Global Studies & Maritime Affairs, California State University Maritime Academy

Dr. Christopher Chiego

December 2nd, 2022

Abstract

Maritime cybersecurity is an increasingly pressing worldwide problem. Recent reports exhibit that the maritime industry has taken a reactive approach to cybersecurity attacks, such as AIS (Automated Identification System) spoofing. AIS spoofing is when people deliberately distort information provided by the automated system. AIS spoofing (or awareness thereof) has increased, leaving ships' security at risk. AIS spoofing enables illegal, unregulated, undocumented (IUU) fishing, sand pirates, and environmental polluters to cause vast amounts of harm across the maritime domain. Currently, there are vast amounts of technological papers on the subject, but presently there is a gap in the literature on the motivations of actors utilizing AIS spoofing. Why do actors use AIS compared to other options? Which actors manipulate AIS? Which of these practices prove the biggest threat to environmental security? Why are mostly Russian, Iranian, Chinese, and North Korean actors mentioned in AIS spoofing? Is it a form of asymmetrical warfare? Why do hackers manipulate AIS to execute potential cyberattacks and environmental crimes in the maritime domain?

The Criminal's Boon

AIS (Automated Identification System) is a Global automatic Positioning System (GPS) that relies upon fitting small transponders on vessels. These transponders continuously transmit VHF (Very High Frequency) signals, alerting other vessels and shore stations with AIS receivers to a vessel's presence. In the past, AIS was only a short range high-intensity system with a 10-20 nautical mile range between transponder and receiver, but today's AIS signals can be received by properly equipped low-orbit satellites. This allows anyone using AIS to track and locate any vessel on earth from their desks or a ship's bridge and spoof, meaning they can change and manipulate data, AIS signals (BigOceanData, 2016) (See Appendix A).

Technical Contexts

AIS data is no longer just for navigation (See Appendix A). It is used by scientists and researchers for data gathering and ideas, such as using AIS data to estimate whale watching and migration patterns (Reimer et al., 2016; Yang et al. 2019; Almunia et al. 2021). Because of the benefits of having big data to utilize, AIS became a mandatory installation for internationally voyaging ships that have a gross tonnage of at least 300 tonnes and all passenger ships regardless of size (IMO, 2015). There are exceptions for security and safety reasons, such as shutting the system off in high-risk areas of piracy and robbery. The master can disable the system when going underway in areas where there may be an imminent threat to the safety and security of the ship, but it must be recorded and reported to the appropriate authority when this occurs. It still gets shut off for other commercial reasons, such as when a ship receives illicit cargo and does not want its voyage disclosed, it is part of spoofing. The resolution has been revised since the first one in 2002 as part of SOLAS (Safety of Life at Sea), but the foundation remains the same. Though not mandatory, some private and small vessels use AIS because of how easy it is to use and the benefits to their safety. Unfortunately, most fishing vessels, which tend to be under 300 tonnes, do not use AIS to avoid any policy enforcement for activities, such as IUU fishing, and when they do, spoofing occurs.

AIS spoofing has increased, or at least the knowledge of it occurring has proliferated, as its beneficial applications have grown. This system is vulnerable due to the easy accessibility and several opportunities for attackers to exploit the system. This paper will examine why illicit actors, from state governments to private actors, use AIS to hide their detrimental environmental activities. Why do actors manipulate AIS to execute potential cyberattacks and environmental crimes in the maritime domain? Why do they use AIS compared to other options? Which actors manipulate AIS? Which of these prove the biggest threat to environmental security? Through the use of case studies of environmental crimes utilizing AIS malpractice, this paper will attempt to answer the question. Due to economic factors, such as the ease of utilizing and operating it, and political factors, like the desire for states to obtain their own agenda, malicious actors can take advantage of AIS to enact damage upon the marine environment.

Hacking into AIS

AIS hackers have variegated ways of striking and inflicting harm upon the maritime domain. AIS data is an open source, its signals are not encrypted, nor does the information from the transponders undergo any authentication processes. There have been studies conducted that look into the discrepancies of AIS data and reports of ghost ships, such as one by Bjorn Bergman who confirmed 15 sets of AIS data were deliberately faked (See Appendix A) (Harris, 2021). With the great range of uses, the improvement of the system's technology, and the ease of using AIS receivers and transponders, data manipulation has proliferated in the last decade. Due to the ease of AIS, it has a dark figure of crime; not one person can fully figure out the extent at which

AIS spoofing occurs because no one can force a vessel to use it or to use it properly on or pinpoint the ones who misuse it. There have been plenty of studies and organizations that have tried, such as Ford et al. (2018), C4ADS (2019), Bergman (2019), and the U.S. Coast Guard (2014).

The mass applications of AIS make it a prime target for manipulation. There are several forms of spoofing AIS: ships, aid to navigation, collision, weather, AIS-SART spoofing, and AIS hijacking (CRFS, 2019). Baleful attackers have many attack possibilities through AIS's implementation and protocol specification. All of these can lead a vessel to dangerous waters due to the attacker's manipulation of the data, whether from a desk or from the ship itself. For GPS, one has to have the means to hack into a satellite. Global Navigation Satellite Systems (GNSS) is also harder to manipulate than AIS, as GNSS receivers can provide defense against such attacks (Psiaki & Humphrey, 2016). AIS, on the other hand, has not developed such defenses yet; especially ones that can be easily implemented to the thousands of ships that currently use AIS.

AIS exploitation does not exclusively endanger the vessel's crews or vessels. AIS's vulnerability is often abused to mask criminal actors' illicit activities, such as overfishing and sand theft, that endanger the maritime environment. With fishery collapses escalating, IUU fishing has surpassed piracy as the leading global maritime threat. Policies have been applied universally and fishing rights have been established and competed over. Fishermen have been innovating new ways to obtain and catch fish, despite any ecological consequences. Organized gangs have been dredging particular strains of sand to sell to construction companies, and with the demand of construction materials on the rise, this makes sand a 'soft gold'. Illegal sand mining risks people's livelihoods and the environment, as missing sand accelerates the erosion of islands and disrupts the environment (DTE Staff, 2016). With these gangs utilizing AIS spoofing to enact these crimes, they also take lives. These actors who utilize AIS for IUU fishing, risk the lives of everyone aboard the ships, and affect the lives of everyone on the globe by drastically damaging the environment by decimating the fish populations that three billion people depend on. Enforcing maritime policies protecting the environment are as pertinent as ever, but AIS spoofing makes it increasingly difficult to trace these crimes. Manipulating pieces of information that AIS provides makes it difficult to track the ship and know their location in reality. These actions make AIS data unreliable when the maritime industry relies upon it for trade. Satellite images can help with knowing when AIS data is manipulated, but cloudy days occur, and some AIS tracks do not necessarily coincide with satellite positioning.

States, such as North Korea, China, and Russia use AIS spoofing for their own political ends. North Korea utilizes this system to evade sanctions and subvert the UN and western authorities. China manipulates AIS to continue growing their lucrative fishing industry and fulfill construction needs, along with undermining Taiwanese government. Russia exploits AIS weaknesses and vulnerabilities to have plausible deniability in their actions on the world stage. This paper will argue that most cases of AIS spoofing come from these states as a tool of asymmetrical warfare against the West, especially the United States (U.S.). This is due to the ease of AIS manipulation and the employment of individual actors. This paper will demonstrate that as a widely used tool in the marine sector that has significant cyber security weaknesses, AIS has become a chosen tool for illicit activities and political subversion.

Literature Review

The Ease of AIS Manipulation

To hack into GNSS and GPS, one needs the resources to manipulate satellites. Most of the cases of GNSS spoofing align with Russian tactics and there have been false circling tracks spotted around Chinese ports inland (Psiaki & Humphreys, 2016; Xiaojun, 2021). Oil shipments have reports of GPS spoofing manipulation (Bergman, 2019; C4ADS, 2019). Now, GPS and GNSS spoofing can affect the operation of AIS, as AIS uses these coordinates to send information, when these GPS coordinates change, so does the information sent. According to Ben Farah et al. (2022) and Intertanko (2019), the GNSS spoofing attack is accomplished in two steps: the synchronization with the satellite's signal and then the increase of power to the transmitted signal. GNSS vulnerabilities include a lack of authentication and encryption. This is much more difficult than exploiting the myriad of vulnerabilities AIS has, and much more expensive. Private actors do not tend to use GPS and GNSS spoofing mechanisms due to the higher expense and narrow inclusivity in adjusting these signals.

There is a plethora of supposed solutions, such as an encrypted AIS (U.S. Coast Guard, 2014), ways to authenticate the signals and warn others at sea and port (Sciancalepore et al., 2022), anomaly detection such as TDOA (time difference on arrival) (Wolsing et al., 2022; CRFS, 2019). Due to the vast amount of AIS transponders already at sea and AIS stations and that some states refuse to implement some of these guidelines, there have been issues in implementing improvements. AIS is the key enforcement tool in environmental accountability, but due to its vulnerabilities it has been used mostly for avoiding detection, rather than for detection.

Evolution of AIS. When AIS was developed, there was little consideration for the security ramifications. AIS originated as a navigational safety aid to prevent ship collisions. Through the recent expansion of AIS's abilities due to Satellite AIS (S-AIS), which serves to detect AIS messages all over the world, AIS data in coastal regions can be viewed in near real time for free and historical AIS data can be bought from data vendors. This unencrypted data is presented and accessible on public websites by private organizations, such as MarineTraffic, who distribute and market this data. Concern about these websites has been brought to the attention of users and providers at IMO (International Maritime Organization) conferences from 2004 (MSC 79/5/10), but after nearly a decade and a half, these websites remain active without pseudonymization or encryption.

AIS: Safety Usage. While some aspects of the maritime industry can remain safe without AIS (Kessler et al., 2018), the system is invaluable due its versatility in supplementing situational and environmental data along with its ability to interface with other detection sources. Mariners, however, are dependent upon the AIS system because of its industry standard on international vessels and its usefulness. Due to the copious possibilities of AIS manipulation, mariners are taught not to rely on AIS solely, but in actuality it proves difficult (Wright et al., 2019). Its capacity to interface makes it a significant component in integrated warning and navigation systems and will undoubtedly continue being an essential asset in the maritime industry.

Cyber Vulnerabilities

AIS is seen as pregnable in the maritime cybersecurity community. There is a gap in the literature and research present in the literature addressing the motivations for misusing and exploiting AIS, which this paper will address. A recent paper published displays a machine learning model which allows computers to learn to understand the motivations for AIS disabling in regards to IUU fishing (Clavelle, 2022). Research has been conducted as to the vulnerability to AIS, but there is little to no research to why hackers use AIS when undertaking environmental crimes. One of the most cited papers on AIS security is Balduzzi et al. (2014), which provided a detailed security evaluation and categorized threats to AIS in three macro-categories; spoofing, hijacking, and availability disruption based upon radio frequency (See Appendix A). Balduzzi et al. (2014), Aziz et al (2020), and Emmens et al. (2021) argued that the attacks on AIS are mainly the fault of specific protocol weaknesses, such as the lack of integrity, authentication, validity, and timing checks. The lack of integrity checks allows interlopers to intercept transmissions due to unencrypted and unsigned AIS messages. The lack of authentication checks describes that no AIS protocol supplies a mechanism for authentication, meaning that anyone with an AIS packet can impersonate any other AIS device. There is no check for any geographic information, this lack of validity checks allows anyone to send an AIS message from any location. There is no time stamp verification, allowing hackers to replay valid AIS information at any other time of their choosing (See Appendix A).

Kessler (2020) addressed the vulnerability of the VHF radio frequency AIS uses, as stated from Balduzzi (2014) and Aziz et al. (2020), which can lead to an attacker commandeering the bandwidth. Once the attacker takes over the bandwidth, they can prevent other devices from transmitting, change assignment information, and negatively affect the synchronization process. Several authors also highlighted that AIS messages are not authenticated, nor validated; thus, these messages remain susceptible to unwarranted manipulations (Goudosis & Katsikas, 2019; Ford et al., 2018; Mednikarov et al., 2020). Kessler et al. (2018) stated that its vulnerabilities ultimately lie in AIS being constantly undermined and manipulated by multiple actors simultaneously. There have been proposed solutions, but none of them have been implemented within IMO. Multiple sources cite that the maritime industry should adopt some aspects of the aviation's industry version of AIS, such as ADS-B (Automatic

Dependent Surveillance- Broadcast) (Kessler et al., 2018; Balduzzi 2014). Though authors, such as Goudosis & Katsikas 2020, recognize that the ways AIS works in aviation cannot be applicable to the maritime industry. For example, the use of identity-based cryptography and symmetric cryptography is inapplicable because of the issues with implementing wireless communication and infrastructure within the maritime environment.

There is a substantial number of security evaluations of AIS, but there seems to be a lack of analysis on why hackers choose to take advantage of AIS's vulnerabilities to execute crimes and of an analysis on how the subterfuge of AIS indirectly impacts the marine environment. Due to the marine environment drastically changing everyday due to climate change and human malpractice, the significance of enforcing environmental regulations is high. AIS's use as an enforcement mechanism needs to improve due to the environmental damage already happening. Overfishing, sand theft, oil shipments, all are great stressors in the maritime environment. This paper intends to fill in the gap with evaluations of AIS's security with the cyber vulnerabilities, which enable actors to actively use AIS for their own ends.

Regulations of AIS

Some believe there should be more regulation on AIS and that people should no longer depend upon AIS for collision avoidance. Kessler et al. (2018) considered that the absence of AIS will not significantly reduce safety at sea due to the presence of other technologies, such as radar. Kessler et al. (2018) even suggested that it may harm the industry, especially when multiple attackers act simultaneously. The maritime industry would be just fine without AIS. However, AIS does provide invaluable data to researchers and allows for easier communication between ships. In a questionnaire for mariners on endangered whales, respondents stated that they would like whale alerts in real-time, leaving AIS to be the main source of data (Reimer et al., 2016). AIS will not go away anytime soon, as its applications vary beyond maritime situational awareness (MSA), such as maritime spatial planning (Wright et al., 2019). It has the ability to help enforce regulations, especially with the enforcement of environmental regulations. For example, Saravanan et al. (2019) states that AIS has the potential to alert fishermen when they cross over a maritime border and enter another state's waters.

Unlike aviation, the maritime industry does not implement centralized monitoring of information flow through traffic controllers, which means that any device using IoT can transmit and receive information that can be shared for ambiguous or unknown purposes. The U.S. is one of the top targeted countries for cyberattacks. These attacks have forced the U.S. to effectuate more stringent enforcement and regulations than of IMO. According to Hamrock (2019), the enforcement mechanisms of the United States particularly are more employed than those of IMO. As IMO works by acknowledging anarchy, this anarchy means that states can agree to the regulations or not. These international agreements are notoriously hard to enforce. States also have different rules when it comes to AIS. In states like Mauritius and Ecuador, AIS is mandatory for all vessels, but in states such as Canada, all vessels are exempt from these obligations. In the U.S., laws on AIS tend to be more specific, even stating the specific information regarding AIS receptors and can provide enforcement to any ship that is not under compliance under the law. Le Tixerant et al. (2018) believe that due to the value of marine spatial planning AIS provides, proactive measures should be taken in order to maintain its value as an effective tool in predicting maritime traffic. Other authors focused more on implementing regulations and modifications to the existing AIS technologically and how it may be used in big data to help in scientific studies and policies (Vasarhelyi, 2012; Yang et al, 2019; Wimpenny et al. 2022). These policies and studies can help mitigate crimes like overfishing.

Policy Challenges of AIS

Overfishing is one of the most significant threats to the world's oceans and security. Proper and effective fishery management has proven effective in supporting sustainable fishing and protecting fish populations. By creating policies that take away incentives to overfish, IUU fishing can decrease and stop undercutting local and international efforts to ensure sustainable fishing (Poling & Cronin, 2017). In the EU, only around 75% of fishing vessels over 15 meters in length adopted AIS after measures were adopted to make it compulsory (Natale et al., 2015). Though an increase of AIS devices has been implemented en masse, fishing and leisure boats have not followed. AIS does not provide any information on the precise métier during fishing trips, such as the type of gear used and targeted species for fishing boats. Overfishing poses a significant threat as fisheries can continue to collapse, leaving a large portion of the population without their main source of food.

Loopholes of AIS. McCauley et al. (2016) argues that AIS noncompliance and improper usage should no longer be legally acceptable, that enforcing rules on the high seas are possible through AIS, and when noncompliance gets better controlled, AIS data should be admissible in judicial court proceedings (See Appendix A). These reasonable requests remain difficult as the past primacy of privacy of the ocean tends to lean towards anonymity and international court proceedings are hard to enforce. Loopholes within AIS need to be addressed before then, as people continue executing illegal activities that promote social injustice at sea, undermine efforts at ocean management and sustainability, and steal biodiversity and profit from developing nations.

The scholarly community agrees that AIS needs added security and that its applications will continue to grow. There are several articles about the technical aspects of AIS and the benefits of big data, but there is an absence of why AIS is being manipulated recently in regards to the environment (Vasarhelyi, 2012; Tu et al., 2016; Arslanalp, 2019; Yang et al., 2019). None of the solutions for AIS has been implemented yet. Whatever security modifications made to AIS will need to be agreed upon by a significant number of maritime-oriented states to have any effective enforcement on environmental crimes on the high seas. The ease of utilizing AIS makes it a tempting target for manipulation. AIS's ability to offer a coat of anonymity leads to difficulty of enforcement and an enticing way to execute illicit activity a myriad of times.

Argument

Dark Figure of AIS Spoofing

AIS spoofing should be receiving more attention in international policy but has not for two key reasons. One is because the exclusion of vessels below 300 tonnes limits AIS enforcement and data gathering, as most fishing vessels are below 300 tonnes, especially local fishermen. The second reason is the unreliability of AIS data growing with increasing cases discovering significant amounts of AIS data to be false. Due to this, AIS data has not been utilized to its full extent or potential to improve life, transport, safety, and the environment at sea.

The temptation to simply turn off AIS to obtain illicit goods, such as fish and sand, overcomes the willpower and conscience of a human being in regard to abiding by international law and protecting the human race and viable state of nature. Due to the ease of AIS manipulation and the mass accessibility of AIS, it has now become the go-to mechanism for remaining hidden, while committing maritime environmental crimes. By using AIS spoofing, ships can obtain an alibi for their location during whatever time they would like on sites such as MarineTraffic, and when no one reports a ghost ship or a ship's presence, no one will know the ship's true location or actions unless satellite images and other methods can be obtained, and research can be conducted.

Compared to GNSS and GPS

There are other ways of spoofing, such as GNSS and GPS. The AIS hardware needed to transmit used to be expensive, but today the hardware has gotten more accessible to both receive and transmit messages, and it has also become more affordable for everyone. AIS spoofing can be done simply and easily with simple radio signals and directly from a ship. There are few obstacles to prevent someone from going online and buying all the equipment needed to establish an AIS station. Due to its easy accessibility, thousands of ships use AIS, but because of this ease of accessibility, people can program the AIS stations with any information they want. People can use AIS to change their vessel's name, position, SOG (Speed Over Ground), the type of vessel, and the IMO number, for relatively cheap, especially when the payoff for doing so is high, such as fish, sand, and illicit cargo.

Economic Reasons

The potential profits from simply manipulating AIS are massive; the cost of manipulation is not. Evading AIS tracking can save people from the hefty fee of trading with a sanctioned state, such as U.S. companies trading oil with Venezuela. Evading AIS tracking and utilizing AIS to trick others into believing buoys and small fishing boats are big ships, allows IUU fishermen to obtain a massive number of valuable fish that can be sold in markets without accountability. Sand pirates utilize AIS to mislead others so they can dredge enormous quantities of sand to sell to Chinese and Indian construction companies that view it as highly valuable due to their rapid growing infrastructure. Illicit actors will continue to utilize AIS's vulnerabilities to enact their own ends due to the easy access and manipulation and the high reward for natural resources to ignore guidelines and rules. For a mere $700 USD on the West Marine online store and the ease of utilizing AIS, an individual could make thousands, if not millions, of dollars manipulating AIS to exploit the seas natural resources.

Asymmetrical Warfare

The majority of AIS spoofing originates from or is associated with China, Russia, and North Korea. The U.S. and EU nations tend to have strong regulations on the use of AIS, while the other states actively misuse AIS. AIS spoofing is a form of asymmetrical warfare against Westernization. These actors have been able to gain power through becoming significant players in the world economy, by using these assets that have been granted to them. China, North Korea, and Russia are known for their cyber hacking tactics. AIS spoofing has become another unconventional tactic in the stratagem of these states to undermine western nations and the global economy, placing the environment as a victim of circumstance.

Methods. This paper will use qualitative evidence from think tanks, news articles, and peer reviewed papers to examine case studies, in which it is proven that AIS was misused to enact damage through falsified route information (including utilizing its switch-off capability) to anonymity to execute unsustainable practices for economic and political gain. Individual actors, even ones supported by state governments, now rely upon AIS to secure and manipulate locations and information to pursue their jobs discreetly and effectively. The ease of access and utilization of AIS results in states, private companies, and individuals manipulating it to evade detection easily and effectively, while extracting and draining the maritime domain's resources and viability.

Evidence

Political and Economic Agendas

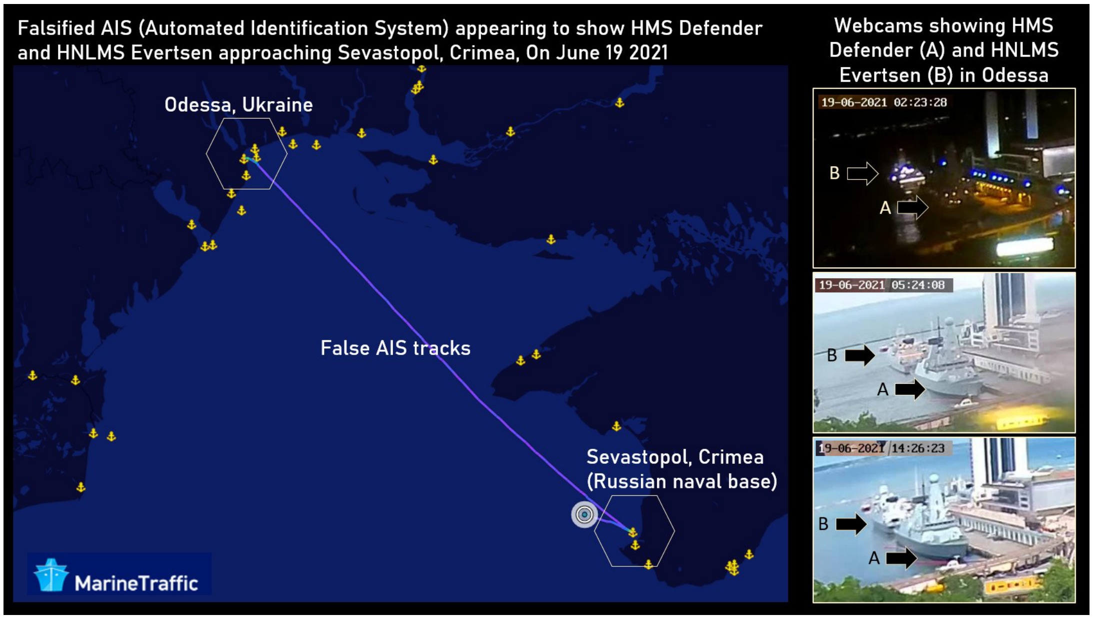
Tracking ships using AIS and its original significance as a tool for collision avoidance is still pertinent today. The benefits of tracking trade routes have several applications, such as planning sea routes, economic planning, and for policies that support safety at sea. This tracking provides researchers, policymakers, and people within the maritime industry insights to make decisions on trade routes and grants guidance to possible ideas and solutions. The threat AIS's vulnerability poses to them, however, is false data. Researchers do not know if the data they receive is false, unless they come across reports of people who saw it with their own eyes. Most of the time, anomalies can be tracked, but they cannot be definitively correct. Commercial ships trading with sanctioned countries, such as Venezuela, shut off AIS when interacting in their ports to evade extra taxes and fees from the trade (Kurmanaev, 2022). There are cases where collisions can be caused by AIS spoofing due to actors' motives to keep others away from the area, such as when fishers label their fishing buoys as big vessels, causing ships to steer off in another direction (Calnan, 2022). False data can affect the effectiveness of policy and policy creation, as the industry tries to predict routes that people take at sea to prevent traffic (Pallotta et al., 2013; Kundakçi & Nas, 2018; Novikov, 2019; Cerdeiro et al., 2020).

Oil. Nefarious groups, such as political and greedy individuals, can manipulate this data to change their voyage history to improve and keep steady relations with established governments. AIS allows companies to easily save money through fines and legal trouble when working with sanctioned states or when smuggling illicit goods. Companies, especially in seafood, energy, and construction, earn more profits by ignoring standards and regulations of AIS, then they do by proper usage of the technology. This happens all over the world with other forms of cargo, but these three are particularly damaging. Extracting fish from the ocean at massive amounts can easily lead to overfishing and when fisheries disappear, incentives to steal from other states Exclusive Economic Zones (EEZs) increase. When a ship undergoes an incident, especially those carrying fossil fuels as cargo, oil spills can occur, killing and disrupting the marine environment with the smuggling ship being held unaccountable (Zhu et al., 2022).

Russia's Invasion. States have used falsified tracking to fulfill their own political agenda. Russia has used AIS spoofing to fake the British warship, the *HMS Defender,* passing through a Russian naval base in Sevastopol before their invasion of the Ukraine (Gorenburg, 2021). Russia believes that the British warships had no innocent passage through these waters because Russia announced in April 2021 that the waters would close its territorial waters through October. However, the waters the *HMS Defender* actually passed through are recognized as Ukrainian territory, not Russian. Russia then utilized AIS spoofing to attempt to reveal a route that would be recognized as a violation of the Freedom of Navigation (FONOPS) on the world stage for their coast guard and fighter jets to harass the British warship*;* it would not have had valid reason to execute otherwise.

Figure 1

Fake AIS Tracks and Photos of HMS Defender at Port in Odessa


Falsified AIS (Automated Identification System) appearing to show HMS Defender and HNLMS Evertsen approaching Sevastopol, Crimea, On June 19 2021
Odessa, Ukraine
False AIS tracks
Sevastopol, Crimea (Russian naval base)
MarineTraffic
Webcams showing HMS Defender (A) and HNLMS Evertsen (B) in Odessa
19-06-2021 02:23:28
B
A
19-06-2021 05:24:08
B
A
19-06-2021 14:26:23
B
A

Note. The falsified AIS data tracks alongside photos of where the *HMS Defender* really is at the same time of the reported false tracks. Graphic from Sutton, H. (2021, June 21). *Positions of Two NATO Ships Were Falsified Near Russian Black Sea Naval Base*. USNI News. https://news.usni.org/2021/06/21/positions-of-two-nato-ships-were-falsified-near-russian-black-sea-naval-bas

This attempt to divert the *HMS Defender* away from Crimea's waters was ultimately fruitless, but it still enabled Russia to cause enough confusion to obtain an excuse to mobilize military forces for its intended agenda (Bateman, 2021). According to Sutton (2021), the British warships were caught on camera at a port in Odessa at the time the AIS data was taken. This falsified data allowed Russia to claim a violation of sovereignty and gave others enough misinformation to justify deploying their navy because they were defending their territory (Corfield, 2021).

Evasion of U.S. Sanctions. Private actors in oil companies utilize AIS spoofing to avoid sanctions, fees, and consequences for going against international or U.S. laws. Iran and Venezuela manipulate AIS to trade and distribute oil to one another (TankerTracker, 2022). The private actors who do exploit AIS to their advantage come from states that tend to ignore regulations originating from the West. The oil shipping companies that distort AIS tracking come from Iran, North Korea, Russia, and China; all nations notorious for attempting to take power from the West for themselves. Originally, only the world's militaries were able to utilize technology to hide a ship's location, but now ordinary companies manipulate their GPS location to appear anywhere in the world thanks to the ease of AIS (Goodman, 2022). Rogue shipping companies continue to utilize it, but it tends to only be on states actively hostile towards the West. In the case of Iran, ships employ the ease of AIS manipulation to gain inconspicuousness.

Iran's Evasion. Venezuela and Iran have deepened their relationship in defiance of U.S. sanctions as Venezuela exchanges gold and other goods for Iran's food, fuel, and condensate. This has led to reports of several tankers reportedly smuggling oil from Venezuela to Iran to evade U.S. sanctions, such as the *Calliop*. The *Calliop*, a tanker chartered by the National Iranian Oil Company (NIOC), disguised itself as *New Andros*, a tanker whose scraps reside in Pakistan, and an Iranian supertanker *Seacliff* to export oil to Venezuela (TankerTracker, 2020). It arrived at Venezuela's main oil port of Jose to load 1.9 million barrels of oil bound for Asia despite economic sanctions. The NIOC also sent a supertanker, called *Horse*, disguised as *Master Honey* as reported through AIS, to Venezuela to deliver condensate, a light form of oil, for Venezuela to blend with its heavy oil to formulate exportable oil, and traveled back to Iran (Kassai, 2020).

These multiple trips not only politically subvert the U.S., but they result in higher carbon emissions. Oil tankers comprise about 13% of maritime emissions (Olmer et al., 2017). Going back and forth from Iran to Venezuela, traveling consistently to other continents and across oceans, to avoid U.S. sanctions and accountability in reporting oil emissions results in a higher amount of carbon emissions, which aids in warming the oceans, altering marine ecology and the maritime environment (Greene et al., 2020). The U.S. Department of Justice has been able to intercept private tankers at times; they were able to intercept four private ships headed to Iran from Venezuela and seize 1.1 million barrels of Iranian gasoline (Parraga, 2020). Though, due to the nature of AIS, catching these cybercriminals still proves difficult, resulting in ineffective enforcement of U.S. sanctions. Undermining U.S. sanctions reveals weaknesses in its foreign policy and enables states, like Iran and Venezuela, to gain power and resources despite the world stages', or perhaps the western world's, views.

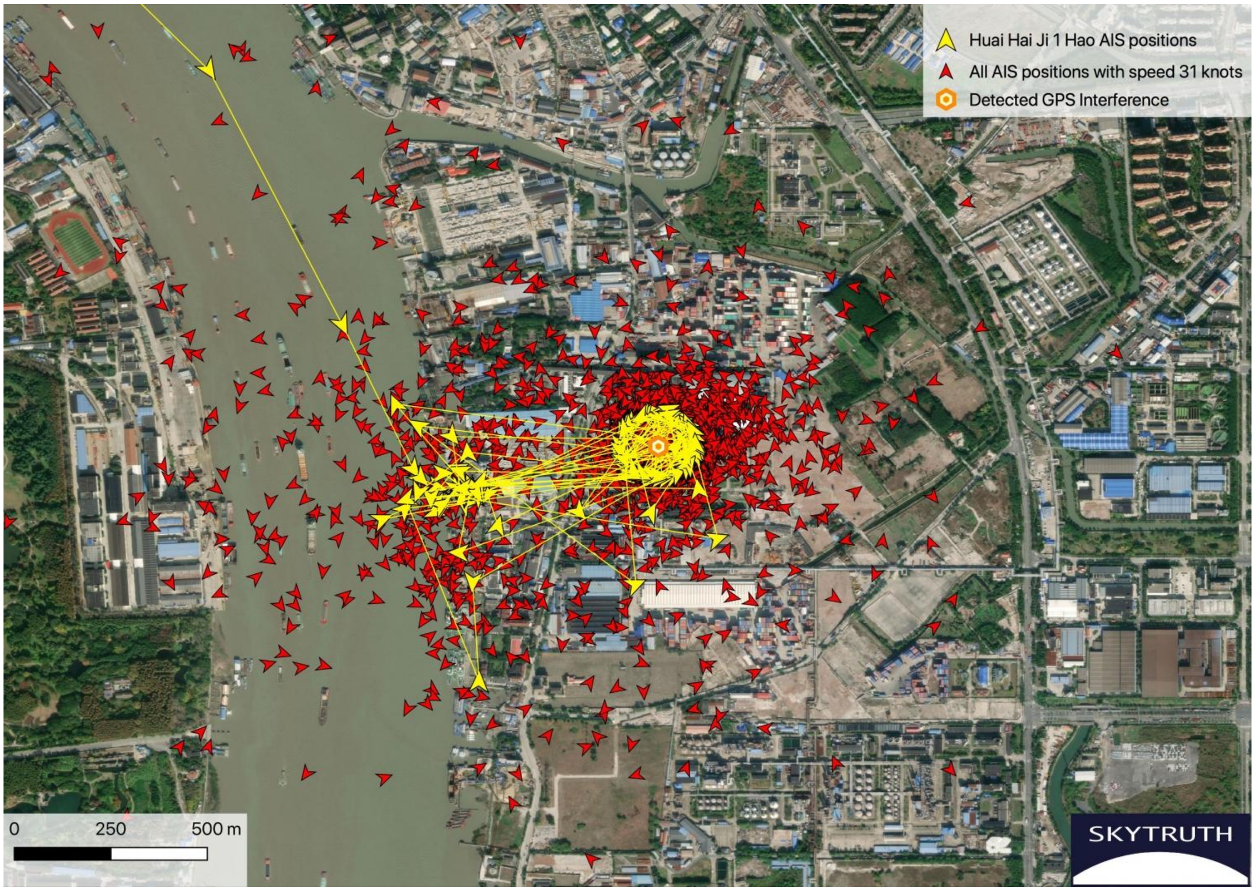
The practice of U.S. sanctions can work against its own allies. Banks in France have been fined billions of dollars for trading with Iran; straining U.S. relationships with its European allies, creating a backlash (Lynch, 2020). These sanctions have an adverse effect on the Iranian economy, even increasing the inflation rate of Iran to 45% in 2021 and Iran's oil exports decreased 50% (Katzman, 2022). Despite the weakening of Iran's economy, these sanctions do not achieve U.S. intentions. Iran continues with its nuclear program, has increased repression of its people due to social unrest, and other countries, like Europe and India, have found ways to bypass U.S. sanctions resulting in a subversion of U.S. power (Drezner, 2022). By manipulating AIS data, Iran can easily bypass U.S. sanctions and continue to export oil to other states and allow other states and private companies to join them to mitigate the effects of sanctions on their economy without lessening their military spending and giving up on their infamous nuclear program. With the continuance of the nuclear program and the exportation of oil with no enforcement, Iranian actors can subvert sanctions and continue malpractice towards the environment.

Venezuela is not the only state using AIS to evade U.S. sanctions with Iran or others. It is suspected that China is trading with Tehran due to "crop circles" or "spoofing circles", as seen in Figure 2. These circles are made up of AIS data points, where the vessel's GPS location jumps into a ring of data points on land and that these "crop circles" have been seen in both China and Iran (Goward, 2020). These circles confuse ship's captains and distort shipping traffic in these areas, creating ghost ships, and making mobile ships seem stationary. Bergman (2019) and Harris (2019) both hypothesize that a device has been designed at a point to distort AIS and GPS coordinates to hide oil transactions. Near the Chinese coast, 20 of these circles were found, 16 of them were oil terminals, while three were prominent government buildings in Shanghai and

Qingdao over the year of 2019 (Bergman, 2019). It is suggested that the government buildings have those circles for security purposes. The most frequent occurrence of the spoofing circles was at the port of Dalian, close to the border of North Korea (Goward, 2019).

Figure 2

AIS Spoofing through GPS manipulation "Crop Circle" at China oil terminal


Huai Hai Ji 1 Hao AIS positions
All AIS positions with speed 31 knots
Detected GPS Interference
0
250
500 m
SKYTRUTH

Note. One of the many "spoofing circles" at an oil terminal formed by AIS spoofing through GPS location manipulation. Bergman, B. (2019, December 12). Systematic GPS Manipulation Occuring at Chinese Oil Terminals and Government Installations. *SkyTruth*. https://skytruth.org/2019/12/systematic-gps-manipulation-occuring-at-chinese-oil-terminals-and-government-installations/

North Korea's Evasion. North Korea has employed AIS's vulnerabilities to their advantage, with the case of the ship *Kingsway*. Because North Korea is not an oil rich region, it heavily relies upon fuel imports. However, the United Nations Security Council (UNSC) sanctioned North Korea by placing a cap of 500,000 barrels on oil and refined petroleum product imports (CFR Editors, 2022b). The *Kingsway* was accused of smuggling "black gold" to North Korea in 2017 from other areas in the South China Sea, it was not until May 2021 that the vessel was detained at the port of Busan in South Korea (Jeongmin et al., 2021). These smugglers gain oil from the licit market to sell illegally to their foreign consumers, like North Korea. The *Kingsway* crew evaded authorities and undermined international law for four years, making millions by importing fuel to North Korea during that time (Kuo et al., 2021). This time, even though they were ultimately caught in the end, they were still able to subvert world authorities and harm the globe by supporting a hostile country with fossil fuels.

When a vessel disables their AIS, the ship and their cargo can disappear. They can switch their AIS back on and appear to be somewhere or assume a completely new identity. The *Kingsway* applied all these techniques, turning off its location when near North Korean waters, changing its name from *Alpha* to *Apex* to *Shun Fa*, even changing the IMO number and repainting the ship, and charting their AIS destinations to different locations to stay disguised from authorities (Dinsmore & Salzman, 2021). This vessel identity laundering causes grave harm in more ways than simply hiding smuggling ships. It could cause collisions when the ship is not inputted on AIS with the same dimensions as the existing ship, identity confusion, and international incidents if the ship has a hostile flag or no flag in another state's waters, making each occurrence a risk to maritime safety.

Through evading detection from multiple government authorities in accordance with the UNSC sanctions, the *Kingsway's* crew acted to subvert the UN and all states party to the sanctions. North Korea actively and aggressively acts to obtain power by undermining the UN in both conventional and unconventional ways. North Korea already embitters the UN directly by continuing with its nuclear program and by not actively participating in trade agreements within the organization. By orchestrating and exploiting the difficulty of enforcement at sea and the vulnerability of AIS, North Korea makes the UN appear as a less valid means of enforcement. By becoming an example of rebelliousness, North Korea's evasion of sanctions hinders enforcement at sea, and affects the reputation of UN member countries, especially UNSC members, such as the U.S. (Crummit, 2022). This also indirectly affects social justice at sea, because when people and other states witness the undermining of significant powers, the continued excessive extraction of resources, such as seabed drilling, can take place as it increases the chances of success in disregarding regulations than in earning less money and resources following regulations strongly influenced by the West. It also enables states to attack weaker state's resources and heighten destabilization, such as the mass amount of fishing off the Somalian coasts leading to a dangerous piracy problem in the waters, that has been abated due to tremendous international efforts (Paik, 2004).

The *Kingsway* is not the only case of a ship smuggling oil to North Korea. Since Taiwan's preferential fuel policies set the prices of oil and petroleum products lower compared to others in the region, it acts as a locale for smugglers to purchase their oil (Kuo et al., 2021). Taiwan has multiple free trade zones where several foreign buyers can purchase duty free (Jewell, 2022). These smugglers manipulate AIS because they want to lower their costs to optimize their benefits. This tempts several actors to accomplish their goals within the region to utilize Taiwan’s policies. The *New Konk* was yet another tanker identified by the UN as a ship illicitly smuggling oil to North Korea from China (Koetti, 2021). Pyongyang has been expanding its port, allowing North Korea to receive more imports (Byrne, 2021). Anomalies in AIS allow some experts to detect where these ship-to-ship cargo transfers occur(Shanthi et al., 2022; Ford et al., 2018; Miller et al., 2018).

Groups can utilize the malleability of AIS data to achieve political and economic goals. The goals can vary from creating reasons to act aggressively, strategic reasons, evading hefty fines, to actively subverting other states. The information manipulation of AIS results in groups taking advantage of the maritime domain for shipping, which can result in collisions, confusion, and in more carbon emissions that warms the oceans through the process of ocean acidification; making all these extraneous trips an unnecessary danger to the environment and to people. The continued damage to the environment due to this conflict makes these sanctions ineffective, persuading others to cause danger to the environment for their own gain.

Sand Pirates

Sand used to be viewed as a limitless resource. Today however, due to increased demand, sand is being exposed as a limited resource, much like fishing. Sand may seem like an endless supply, but usable sand is, in reality, a finite resource. Most usable sand grains are created and shaped by water. Humans use more sand than any other natural resource besides air and water, even more than oil (Beiser, 2018). Extracting too much sand at a time from one place severely damages the environment, changing the ecological and geographical make-up of the maritime domain, until eventually the area may be a completely different landscape.

Certain sands are known as “soft gold” in Asia due to the high demand of construction needs in China and India and are highly valuable to dredge for vast quantities (See Appendix B).

Due to these modern construction needs, sand is a valuable construction resource, but it also acts as a protection against erosion of land and the disappearance of bodies of water (Ayshwarya et al., 2019). The price of dredging and extracting sand in enormous amounts gives people more incentive to avoid permits and detection through technological means. It also promotes social injustice in the international community, as sand dredging tends to attack developing countries and states. Sand dredging is not an inconspicuous activity. By utilizing AIS, sand pirates can convince ships to move away from areas of illicit activity effortlessly.

Actors using GPS spoofing in the cases of sand theft are minimal, as governments tend to not support theft of their own land, especially China. Sand thievery does not support sustainable growth of the region, but does support the rapid urban and infrastructure growth, which puts a strain on government infrastructure as resources dwindle (Xu, 2014). Due to the complexity and difficulty of GPS and GNSS spoofing, cases where sand thieves that use it are few if there are any, since GPS spoofing normally requires access to satellites and GNSS spoofing requires more expensive equipment.

China's Private Sand Pirates. Illegal and mass sand dredging has grave environmental consequences as demonstrated with the devastation of China's freshwater Lake Poyang. Dredging ships, most disabling AIS, extracted millions of tonnes of sand from the shores and bed of the lake, severely reducing the water within it (Beiser, 2016). The lake appears completely different from what it was 20 years ago, it is now shallower with less smooth sand and several mining ships a day (Scarr & Sharma, 2021). The devastation of this lake and its biodiversity's gradual decimation due to sand dredging, can lead to disastrous results to lack of irrigated water for irrigation to shrinking habitats for birds and fish.

Since President Xi Jinping described the lake as China’s “kidney”, the devastation of the lake is unlikely to be directly connected to any government officials, and simply is the result of the lack of proactive environmental management (Yin & Peter, 2022). The authorities have started trying to remove illegal docks throughout the region by dismantling 1,254 out of the 1,361 discovered illicit docks (Xinde Marine News, 2018). The Shanghai authorities have actively tracked illegal sand mining in the region, meaning sand dredging in the region is executed by private actors, since China is actively making efforts to mitigate the environmental destruction (Shanghai Maritime Safety Administration, 2021). The Yangtze River possesses a large amount of usable sand connected to the Poyang Lake. AIS vulnerability is a serendipitous opportunity for people wanting to make money to feed the modern need for sand.

No matter the environmental impact, these people want to make money in a swift fashion, leading them to avoid detection when evading permits and possessing gross amounts of sand aboard the ship. Shanghai Maritime Safety Administration (MSA) in 2018 informed the media that 53 people have been killed due to marine accidents within the Yangtze River due to sand dredging (中国新闻网, 2019). The Shanghai MSA experiences difficulty enforcing the regulations against exploitation and extraction of resources, such as sand dredging, within its waters. It takes time for them to send a naval vessel once alerted; allowing time for the violating vessel to flee, taking with it tons of stolen sand from the Yangtze River (Xiao, 2000).

China’s Sand Warfare. China, however, has been accused of using sand dredging against Taiwan. Reports of it using the tactic of gray zone warfare has occurred, a strategy of exhausting Taiwan through areas of non-open combat (Braw, 2022). Due to the close history of Taiwan and the U.S., Taiwan often acts as a proxy for the U.S. in relations to China. This presents a way for China to undermine the U.S.’s power without sending troops and occupying

Taiwan directly. Stealing sand is a way to slowly undermine Taiwan's infrastructure and land, while supporting China’s own infrastructure and construction.

Case of Taiwan. China has a century of history against Taiwan. Since Taiwan is not officially a state, but makes attempts at its own sovereignty, China continues to find ways to control the territory. When Nancy Pelosi, an American senator, visited in August, China cited that as a violation of the ‘One China’ policy. To retaliate, China banned all exports of sand to Taiwan to harm Taiwan’s economy (FP Explainers, 2022). Along with banning sand exports, China actively uses AIS spoofing to steal sand from Taiwan’s Matsu Islands.

This undermines the livelihoods of the residents residing in these islands, in addition to their environment. The residents of the Matsu islands see 300 to 400 sand dredgers off their coast at times, and most residents can hear the sand dredgers. This technique has successfully spurred and nurtured fear among the residents on the Matsu islands, though China claims that they have nothing to do with the vessels (Watt, 2021). The active threat of the environment and the dormant threat of warfare and the possibility of Chinese naval boats approaching the islands, effectively applying pressure and exuding intimidation upon the inhabitants. This is just one of the many ways China is exerting pressure towards Taiwan and the West.

As soon as the Taiwan coast guard leaves, the sand dredgers come back with their AIS disabled, so the Taiwan coast guard cannot easily track them (Lee, 2021). It is nearly impossible for a patrol to enforce an armada of 200 sand dredgers to return sand back to their coastline. Taiwan has had little success in permanently turning away the Chinese sand dredgers because of their sheer vast numbers and because of its non-sovereign status but has effectively forced some Chinese sand dredgers to return the sand they stole. The difficulty of tracking these ships forces Taiwan to enforce round the clock patrols along what they perceive is their waters. The loss of sand in the modern age for Taiwan will undoubtedly harm its residents as they remain in fear and their economy.

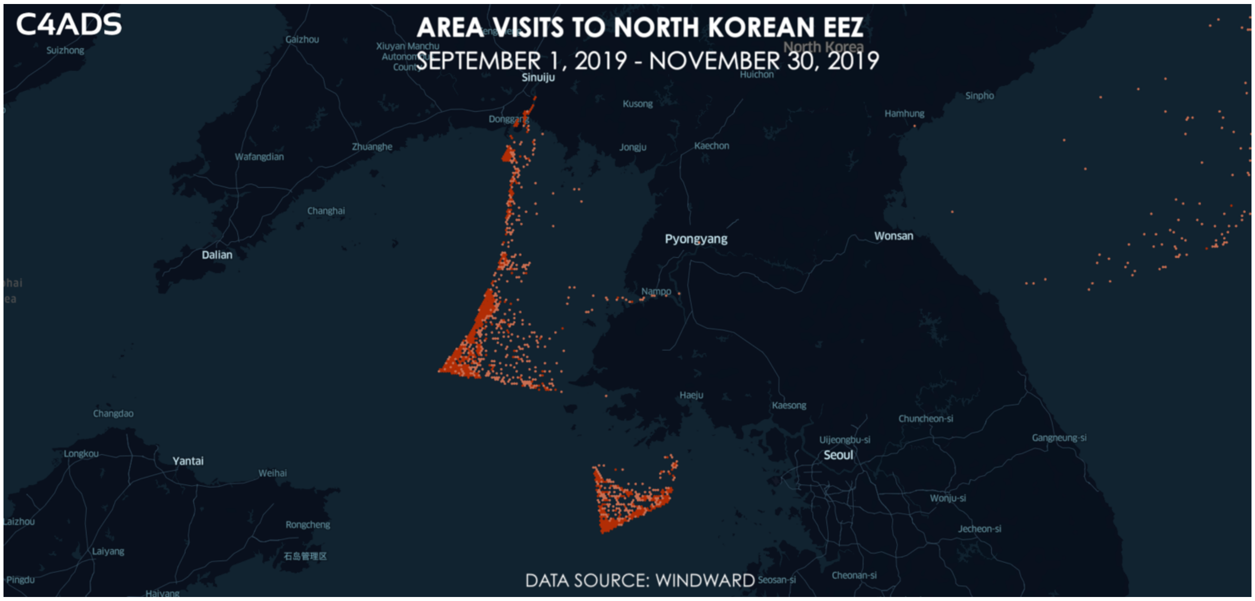
The number of Chinese excavators entering disputed Taiwanese waters have only increased with Taiwan expelling about 4,000 Chinese sand-dredgers and sand transporting vessels from its waters in 2020, a gargantuan 560% increase from the 600 Taiwan expelled in 2019 (Braw, 2022). The problem will only escalate within Taiwan's waters, especially during times when China wants to act aggressively towards the U.S. During the same time the sand dredgers were harassing island residents with the loud noises, blinding lights, and unwelcome presence, the Chinese flew 28 Chinese air force planes, including fighter jets (Teh, 2021). The massive increase in the number of sand dredgers is a sign of active gray-zone warfare that China will utilize more as tensions increase.

North Korea's Warfare. North Korea has dredged its own shores to sell sand to China. Due to the poor state of individuals in North Korea, using AIS spoofing is one of the only accessible ways to avoid authorities, whether international organizations or domestic ones (Kuo & Sung, 2020). North Korea's government does own five satellites, so there is a possibility that the government uses GPS and GNSS spoofing as well, but it would be like that of China's navigational system (CFR Editors, 2022a). North Korea most likely utilizes AIS due to its ease of use, along with the reports of crop circles around their own coastal port. AIS is significantly less expensive and more accessible to more of their professional crews in the maritime industry, as they can simply manipulate it from anywhere at any time.

North Korea has UN sanctions placed upon them in 2017 that bans them from selling, supplying, or transferring sand to other states. North Korea circumvents this sanction as well with the help of AIS distortion. Sand dredging activity increased with the need for infrastructure, so North Korea decided to take advantage of that (Smith, 2020). The sand dredgers deliver the sand to China to gain money for their economy. Yet, Kuo & Sung (2020) witnessed from inconsistent AIS tracking and surveillance that 279 ships moved off the coast of Haeju (a coastal city in North Korea) to China and witnessed through satellite images that the ships moving there were sand dredgers. Most of these ships were flagged as Chinese vessels or had Chinese names. North Korea continues to dredge mass amounts of sand, affecting the ecological makeup of the region. Sand dredging not only allows North Korea to gain money for the sand from China, but it allows the state to actively cause ecological harm to its neighbor South Korea and other states in the region to undermine their sovereignty and sabotage their security.

Figure 3

AIS Data of ships off the coast of Haeju



Note. AIS is turned on during this time, but many of the ships are suspected, and some confirmed, of using different names and flags of convenience. Graphic by Kuo, L., & Sung, L. (2020, March 3). *Against the Grain*. C4ADS. https://c4ads.org/commentary/against-the-grain/

China has encouraged other states to relax UN sanctions on North Korea. This is probably because North Korea aids them in their gray-zone warfare by undermining other states and supporting Chinese construction and infrastructure. Even though sand dredging can be seen from satellites and research from Kuo & Sung (2020) proves the involvement of over 279 ships with Chinese names or flags without any IMO numbers, the business remains opaque. There is a possibility of North Korea earning money from allowing a Chinese company to dredge the sand themselves (Berlinger, 2020). A UN report in April 2020, reported that North Korea had a profit of at least $22 million in 2019 using a substantial "sand-export operation" (Lederer, 2020). This helps fund North Korea's nuclear program, while aiding in the infrastructure to China and overall, subverts the validity of UN sanctions.

Social Injustice in Developing States. There is no evidence that AIS spoofing was involved, but no evidence was found at all in the case of Jamaica's stolen beach. No arrests, no breakthroughs were made when 500 tonnes of sand were stolen and relocated somewhere else in 2012. Ten years later, the case is scrapped, and the country has no clue where the sand went. Morocco has also supposedly stolen sand for the Western Sahara to replenish its tourist beaches. However, replacing sand on beaches grants only a false sense of security as the coastline, as sea-level rise will only increase the need for more and more sand to satisfy these false beaches (Tweedie, 2018). The negative impacts for the insatiable need for sand has led to sand smuggling, and thus an increased usage of using untraceable techniques of switching off AIS and changing the GPS signal.

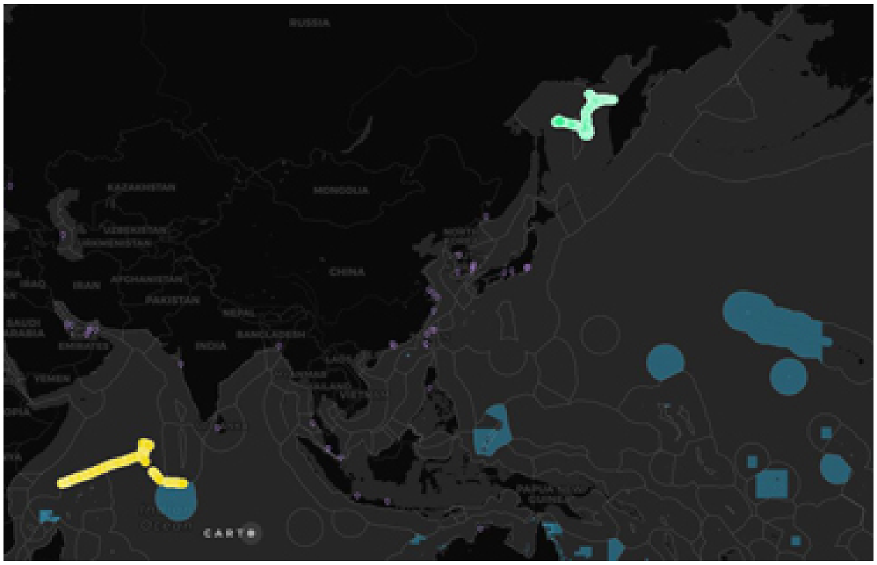
Greedy sand dredging is not the only activity that endangers the environment and can be utilized as a tool for asymmetric warfare that AIS spoofing can aid in its manipulation and misinformation tactics. Overfishing can degrade the resource security of other states and promote instability, while also allowing actors to profit from these resources. Sand dredging will continue to rise as developing countries grow and industrialize. AIS spoofing not only offers sand dredgers invisibility but offers other ways to aid in activities that promote over extracting resources, such as overfishing.

IUU Fishing

Overfishing is one of the most harmful threats to the world's oceans, making IUU fishing one of the most threatening illicit activities in the marine environment, exploiting the ocean's finite resources, changing physical characteristics, and affecting the fragility of its ecosystems (Environmental Defense Fund, 2022). Sixty-four percent of the world's oceans are outside national jurisdictions. These waters harbor unique marine diversity including highly endangered species (Collins et al., 2020). When people try to track ships known and associated with IUU fishing, the map is dark and bleak, displaying only two small routes that are supposed to ve the tracks of highly suspected IUU fishing vessels.

Figure 4

Snippet of IUU Vessel Tracker



Note. This tracker only displays highly suspected IUU vessels with their AIS on during the time of the picture. Godfrey, M. (2021, June 22). *IUU vessel-tracker shows possible widespread abuse of AIS switch-off capability*. https://www.seafoodsource.com/news/environment-sustainability/iuu-vessel-tracker-shows-possible-widespread-abuse-of-ais-switch-off-capability

Anonymity of Private Actors. The darkness and bleakness of this map is due to these fishing vessels abusing AIS's switch-off capability or misusing AIS by changing their identity (Godfrey, 2021). IUU fishermen, however, use other techniques of AIS to assist in acquiring mass quantities of fish. As mentioned before, fishermen misclassify buoys as big vessels, change their GPS location, and misidentify their MMSI number. Individuals also tend to disguise their own ship by either painting a different name on their ship or misrepresenting their flag. Individuals also do not tend to travel in fleets, enabling them to remain secretive as one vessel sends out a false signal that can cause an unknown amount of harm. Due to the well-known nature of Chinese fleets' connection to IUU fishing and AIS spoofing however, this section will focus on the state's use of AIS spoofing executed by the People's Republic of China (PRC) for fishing.

China has exhausted its fisheries on its shores, persuading its fishermen to find fish elsewhere to keep their lucrative industry successful. This has created conflicts with other countries, with the international community, and with other fishermen as well. This competition for resources has resulted in the raping of marine wildlife and biodiversity. Fishing vessels are now able to fish at mass and disregard environmental regulations or sustainable fishing practices of any nation. Instead of falsifying the lights to convince others that fishing vessels are cargo vessels, illicit actors can simply change what information is sent through AIS with simple clicks of a keyboard (U.S. Coast Guard Navigation Center, 2020). Since AIS technology is easier to manipulate and the ease of accessibility, fishermen, both state actors and individuals utilize it to cloak IUU fishing activity.

PRC's Fishing. IUU fishing does contain characteristics of government involvement, such as the case of China. China has a massive fishing industry that is heavily dependent upon for food and exportation. It is one of the largest maritime states and claims the largest fishery catch in the world (FAO, 2022). China has devastated its own fisheries, leaving it to pursue other high seas waters to extract fish. One of the reasons China is successful in the fishing industry is because Chinese fleets can fish for years at a time. They can fish for longer durations because they offload their catch into giant refrigerated vessels, or reefers, that can hold more than 15,000 cubic meters of fish to port (Goodman, 2021). This enables them to keep their fishing spot on the high seas and continue catching loads of fish to feed their industry. They also have their own cheap processing units, linking illegal fishing to labor abuses more so than any other crime like human or drug trafficking (CSIRO, 2020).

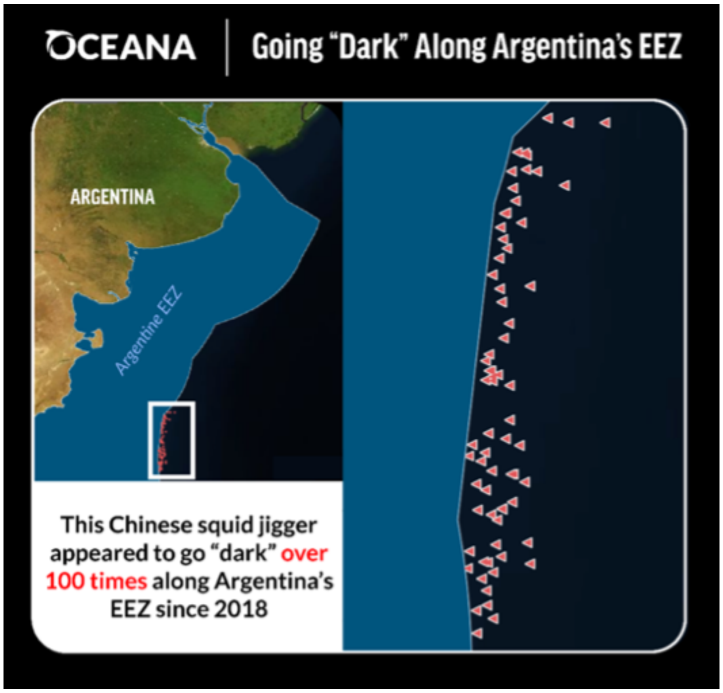
Complaints from the International Community. China today faces massive amounts of criticism from the international community and media about its usage of AIS spoofing, especially regarding its large fishing industry. There is a high demand in the market for marine life, especially fish, with koi fish being worth more than $80,000 dollars in Singapore (Gerstein, 2021). Another valuable catch has been the shortfin squid, earning China hundreds of millions of dollars in exports. Chinese fishing vessels utilize AIS spoofing to capture species such as the shortfin squid off the coast of Argentina. Several seafood squid industry representatives have been trying to even the playing field by attempting to enforce rules in transparency, by forcing AIS tracking to be readily available information to consumers.

This will most likely not even solve the problem, as China does its own fishing and processing to keep prices low and enticing for consumers. Fish imports have increased 500% since the 1990s, with most of the catch coming from less industrialized nations with high risk of the products coming from illegal sourcing. China has persistent exposure to IUU risk among fish imports (Willard, 2021). China's significant role in the seafood supply chain does not come without grievances from the international community. Argentina, along with many other states, do not appreciate China's exploitative fishing fleet invading its shores.

China's Encroachment of Argentina's EEZ. Chinese ships have been shot at, such as when Argentina launched an attack on a Chinese fishing vessel within Argentine waters (Whitehead, 2022). Argentina's waters contain mass amounts of shortfin squids and these Chinese fishing vessels are equipped as shortfin squid jiggers. Argentine ships have chased Chinese ships outside of their waters and shot at them. These incidents cause others to say that the situation is a "literal war" to keep their EEZ (Torrico, 2020). This severe, aggressive situation causes stress on relations between the states and the world stage.

Figure 5

AIS data Graphic of Argentina's EEZ


OCEANA
Going "Dark" Along Argentina's EEZ
ARGENTINA
Argentine EEZ
This Chinese squid jigger appeared to go "dark" over 100 times along Argentina's EEZ since 2018

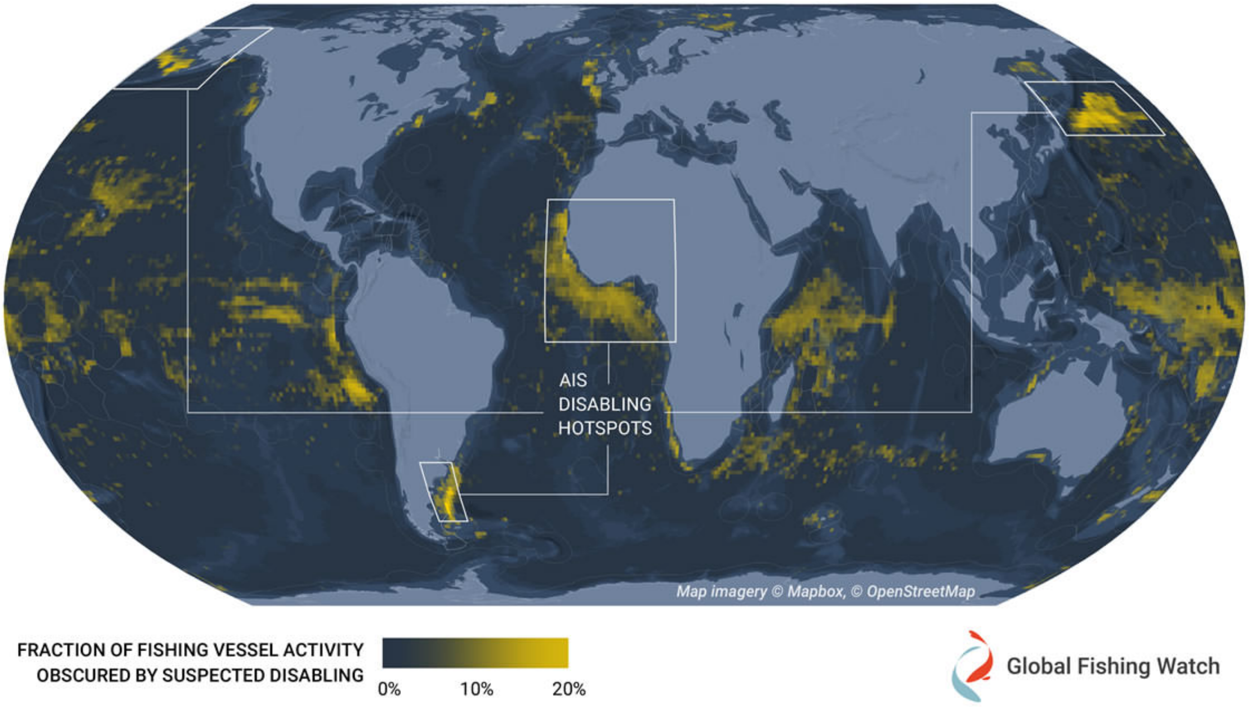
Note. This image shows vessels with AIS data switched on outside Argentina's EEZ. Torrico, G. (2020, December 28). South America plans regional response to illegal squid fishing. *Dialogo Chino*. https://dialogochino.net/en/extractive-industries/39004-south-america-plans-regional-response-to-illegal-giant-squid-fishing/

Though China's industrial IUU fishing leads to a highly strained ocean, stressing and depleting natural resources and ecosystems, it supports a large industry and economy for China. The disabling hotspots of AIS are present near the EEZs of Argentina, Northwest Pacific, and West African nations, regions where IUU fishing has a strong concern (Welch et al., 2022).

A study by Global Fishing Watch analyzed AIS disabling events driven by high chlorophyll levels as these levels indicate fishing ground quality (Clavelle, 2022). The model they use suspects that people disable their fishing vessel's AIS to hide good fishing grounds, as well as when a vessel is nearby sovereign waters of another country or near a refrigerated cargo vessel, which are used to transship catch. The continued evasion of accountability and consequences will lead to more strained resources as others continue to make money for their own benefit. IUU fishing actors not only use AIS spoofing to hide good fishing grounds, but to mainly hide their activities at sea. The chlorophyll of an area does not necessarily mark rich fishing grounds.

Figure 6

Map of AIS disabling


AIS
DISABLING
HOTSPOTS
Map imagery © Mapbox, © OpenStreetMap
FRACTION OF FISHING VESSEL ACTIVITY
OBSCURED BY SUSPECTED DISABLING
0%
10%
20%
Global Fishing Watch

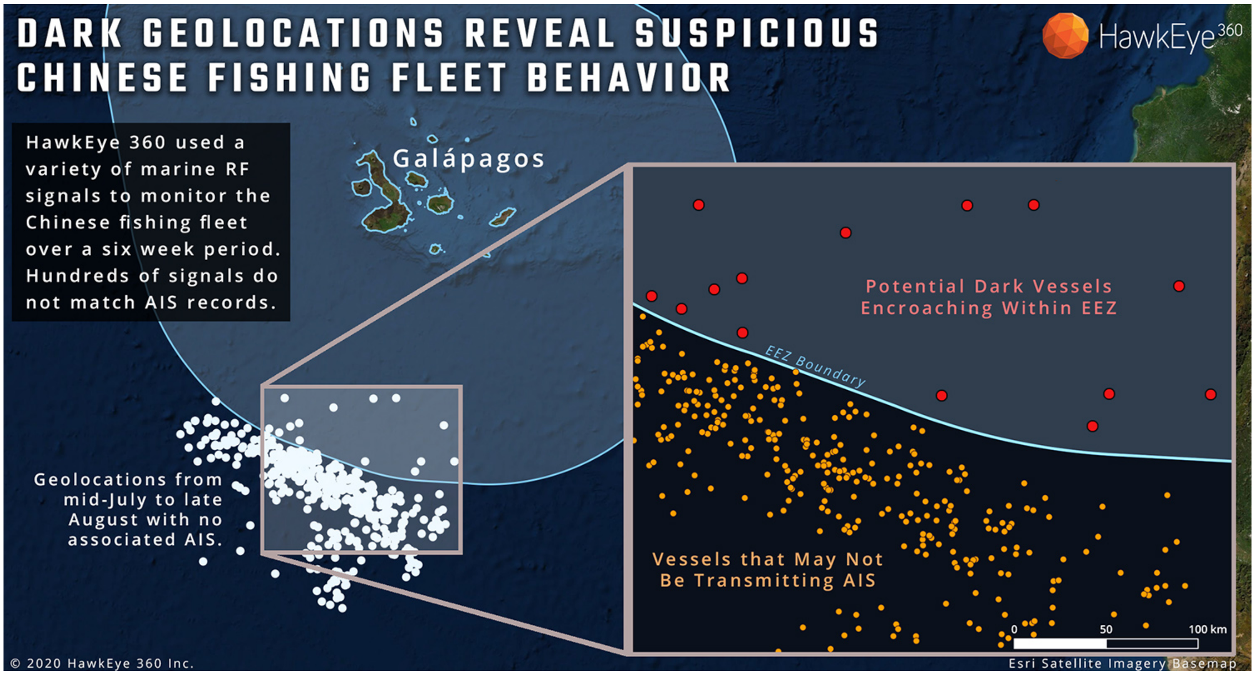
Note. This map highlights the AIS disabling hotspots. Map by Clavelle, T. (2022, November 2). Hotspots of Unseen Fishing Vessels Illuminate Areas of Concern for Illegal, Unreported and Unregulated Fishing. *Global Fishing Watch*. https://globalfishingwatch.org/research/hotspots-of-unseen-fishing-vessels-qa/

China will continue to support these actions because they realize the strategic value of increasing their economic worth and exploiting others' territories through accomplishing fishing endeavors by manipulating AIS. Argentina is well within the western hemisphere, meaning that it is well within the U.S.'s sphere of influence. China is willfully using its fishing industry to infringe upon and exploit the U.S. weaknesses in enforcement mechanisms in other states and other western states themselves to project more power in the world. AIS acts as an invisibility cloak for these actors because they are more likely to undertake these endeavors when no one knows that they are the ones sticking their hands in the cookie jar.

China's Attack on the Galápagos Islands. Other states have been alarmed about this, especially fishermen off the coast of the Galápagos islands (Urbina, 2020). While fishing on the high seas is legal, fishing within an EEZ is not. Fishing close to the Galapagos islands presents the fear of endangered species going extinct due to the massive amount of fishing and the high value of rare species on the elite Asian market. A case study from Hawkeye 360 (2021) identified that numerous vessels in one of the globe's top fishing fleets stopped transmitting VHF signals on their AIS for more than eight hours and may have penetrated into Galápagos's EEZ. This strongly indicates that IUU fishing occurred in the area; especially since the EEZ of the Galapagos is 700,000 km.

Figure 7

AIS Disabling Reveals Suspicious Chinese Fishing Fleet Behavior


DARK GEOLOCATIONS REVEAL SUSPICIOUS CHINESE FISHING FLEET BEHAVIOR
HawkEye 360
HawkEye 360 used a variety of marine RF signals to monitor the Chinese fishing fleet over a six week period. Hundreds of signals do not match AIS records.
Galápagos
Potential Dark Vessels Encroaching Within EEZ
EEZ Boundary
Geolocations from mid-July to late August with no associated AIS.
Vessels that May Not Be Transmitting AIS
0
50
100 km
© 2020 HawkEye 360 Inc.
Esri Satellite Imagery Basemap

Note. This map unveils suspicious AIS behavior within the EEZ of the islands. Graphic by HawkEye 360. (2021). Potential Chinese illegal Fishing Seen from Space. *HawkEye 360.* https://www.he360.com/resource/potential-illegal-fishing-seen-from-space/

In 2017, an incident occurred where the Ecuadorian Navy seized a Chinese vessel within the Galapagos Marine Reserve that had 300 tonnes of marine life, consisting mostly of sharks, on board (Tan, 2020). The continued pillaging of the Marine Reserve can lead to the cultural, historical, and ecological loss in the home of Darwin's idea of evolution. The island is already experiencing the dramatic effects of climate change in its marine reserves, but overfishing could drastically weaken the islands' rich biodiversity and threaten the livelihoods of thousands there. By demonstrating to the world that the PRC can harm this internationally treasured place with little consequence and is willing to go into other states' EEZs, it displays its new global power while growing its economy.

IUU fishing can lead to a growth in AIS manipulation further as fisheries collapse. It is unlikely that AIS manipulation and IUU fishing will stop due to environmental consequences. Its utilization for gray-zone warfare alone should also suggest an increase in AIS spoofing in the years to come as tensions between the West and East rise. Though PRC does fish legally within the high seas, its unsustainable practices will eventually lead to the collapse of fisheries and will act aggressively by infringing upon other states' EEZs. There can be a mechanism for mitigating these disasters, such as increased patrols, but there is no stopping the manipulation of AIS due to its accessibility, ease of manipulation, and mass usage. There is no enforcement mechanism yet to force other ships to turn on their AIS and there is no international law stating that fishing vessels under 300 tonnes need to switch AIS on.

Findings

Overfishing is one of the biggest threats to environmental security which the manipulation of AIS enables. It promotes destabilization, environmental harm, and lowers security at sea. Sand dredging will eventually become one of the most harmful practices at sea, but since vast sea level rise has not occurred yet, it is not as dangerous as overfishing. Evading sanctions, carrying harmful cargo, and fabricating stories of supposed infringement of sovereignty cause international disputes and can cause environmental harm. Fabricating stories to justify aggressive actions and evading sanctions do not directly alter the ecological makeup of an environment and damage millions, or perhaps billions, of livelihoods like overfishing and sand dredging do.

AIS actors, whether state or private, manipulate and distort AIS information due to its ease, mass of application, and information malleability. Due to GNSS and GPS's lack of accessibility, expenses, and the high level of cyber competence needed to utilize and manipulate these devices, they are not ideal to use individually by private actors or individuals overseas working on behalf of the state. Private actors manipulating AIS are harder to spot as they hide their flags and do not have a strong national link, leading to strong anonymity. Cases of AIS spoofing are easier to spot when a whole state and company acts upon it with several vessels. Individual AIS spoofing cases are harder to discover in media sources of think tanks, news, and peer-reviewed papers due to their generally anonymous nature.

State actors, people acting on behalf of the state, are easier to identify as they tend to use the same tactics and have the state to defend them against international incidents. State actors tend to use AIS spoofing to enact crimes against the maritime domain and leave the degradation of the environment as collateral damage to enact asymmetrical warfare tactics. The West may also have AIS spoofing cases, but none that utilize state-sponsored spoofing known at this moment. This is due to the power of states in the West, especially the U.S., possesses now, leading to more conventional means of warfare and strategy implemented by Westernized nations.

When researching AIS spoofing, no significant or any AIS spoofing cases were found that were executed or suspected to be executed by any NATO (National Atlantic Treaty Organization) states on Google Scholar, Google, JSTOR, New York Times, MDPI, and ProQuest. AIS spoofing was a form of a use for private gains, but recently, especially as evidenced by the "crop circles" seen in China, these states are actively looking for ways to manipulate the information provided by AIS. In manipulating AIS in such ways, these states undermine safety at sea and subvert the international community in their attempt to accurately track vessels at sea.

Recommendations

Future Research

Examining AIS spoofing through case studies enables a specific and nuanced view of the motivations behind manipulating AIS, along with explaining the context at which the spoofing occurs to justify the motivations. Unfortunately, the research cannot present an accurate picture of the numbers or a first hand investigation of AIS spoofing, as most of the research was qualitative and done through online databases. The lack of accessibility to raw S-AIS data makes the paper lack accurate real-world cases and numbers. Future research on the motivations for AIS spoofing will benefit by having data on the number of ships utilizing GPS, GNSS, and AIS and comparing those numbers, raw data on conspicuous data tracks, and route information, along with the nationality of the ships suspected of AIS spoofing.

Due to the nature of AIS spoofing, whatever data looked at can be manipulated and unless a person is on a boat in that ocean or can look at photographs and observe AIS maps at the same time, no one can know with completely certainty where these ships were or who is participating in sand dredging, IUU fishing, or story fabrication. The research also did not address sources that were not in English, meaning that most of the sources did not come from the regions – China, North Korea, and Russia – which the researcher found to be the focus of AIS spoofing cases. For future research, looking up AIS spoofing in Russian, Korean, and Chinese will most likely prove more useful in developing more sources and gathering a more neutral view on the motivations behind AIS manipulation.

Enforcement

To mitigate AIS spoofing, there must be more ways of investigating when AIS spoofing occurs, such as the methods employed by Bergman (2019). There needs to be a device that can force a boat to switch on their AIS and verify the information through an authentication system, like those proposed by others in the technological community (Goudosis & Katsikas, 2020; Kessler, 2020; Sciancalepore et al., 2022). There could also be a device or method developed to pinpoint where the devices manipulated AIS data into "spoofing circles" are coming from to enable mariners at sea to avoid those areas and to possibly narrow down those areas for truth-seeking purposes. AIS spoofing will always be an ongoing enforcement problem for as long as AIS exists, and its information remains easily malleable and manipulated.

References

Almunia, J., Delponti, P., & Rosa, F. (2021). Using Automatic Identification System (AIS) Data to Estimate Whale Watching Effort. *Frontiers in Marine Science*, *8*. https://www.frontiersin.org/articles/10.3389/fmars.2021.635568

Androjna, A., Perkovič, M., Pavic, I., & Mišković, J. (2021). AIS Data Vulnerability Indicated by a Spoofing Case-Study. *Applied Sciences*, *11*(11), 5015. https://doi.org/10.3390/app11115015

Arslanalp, S., Marini, M., & Tumbarello, P. (2019). *Big Data on Vessel Traffic: now casting Trade Flows in real time*. IMF. https://www.imf.org/en/Publications/WP/Issues/2019/12/13/Big-Data-on-Vessel-Traffic-Nowcasting-Trade-Flows-in-Real-Time-48837

Ayshwarya, A., Dhanalakshmi, R., Usha Rani, P., Haripriya, S., & Joshna, R. (2019). Image Processing and IoT Based Sand Theft Detection and Indication System. *International Journal of Innovative Technology and Exploring Engineering*, *9*(1S), 170–174. https://doi.org/10.35940/ijitee.A1036.1191S19

Aziz, A., Tedeschi, P., Sciancalepore, S., & Pietro, R. D. (2020). SecureAIS - Securing Pairwise Vessels Communications. *2020 IEEE Conference on Communications and Network Security (CNS)*, 1–9. https://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*, 436–445. https://doi.org/10.1145/2664243.2664257

Bateman, T. (2021, June 28). *Fake ships, real conflict: How misinformation came to the high seas*. Euronews.

https://www.euronews.com/next/2021/06/28/hms-defender-ais-spoofing-is-opening-up-a-new-front-in-the-war-on-reality

Beiser, V. (2016, August 4). *Is Shanghai's Appetite for Sand Killing China's Biggest Lake?* Pulitzer Center. https://pulitzercenter.org/stories/shanghais-appetite-sand-killing-chinas-biggest-lake

Beiser, V. (2018). *The World in a Grain : the Story of Sand and how it Transformed Civilization*. Riverhead Books.

Berlinger, J. (2020, June 10). *North Korea might be making millions—And breaking sanctions—Selling sand. Yes, sand. | CNN Business*. CNN. https://www.cnn.com/2020/06/09/business/north-korea-sand-intl-hnk/index.html

Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., & Bellekens, X. (2022). Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. *Information*, *13*(1), Article 1. https://doi.org/10.3390/info13010022

Bergman, B. (2019, December 12). Systematic GPS Manipulation Occuring at Chinese Oil Terminals and Government Installations. *SkyTruth*. https://skytruth.org/2019/12/systematic-gps-manipulation-occuring-at-chinese-oil-terminals-and-government-installations/

BigOceanData. (2016). *The Definitive AIS Handbook*. Global Vessel Solutions.

Braw, E. (2022, July 11). *China's Sand Dredgers Run Gray Zone Warfare in Taiwan*. https://foreignpolicy.com/2022/07/11/china-stealing-taiwan-sand/

C4ADS. (2019). *Above us only stars: Exposing GPS Spoofing in Russia and Syria*. https://www.arcgis.com/apps/Cascade/index.html?appid=b919c8d91b0a4f868f02acfdebc428d7&classicembedmode

Calnan, K. (2022). Conversation on AIS Misuse. California State University Maritime Academy.

Cerdeiro, D., Komaromi, A., Liu, Y., & Saeed, M. (2020). World Seaborne Trade in Real Time: A Proof of Concept for Building AIS-based Nowcasts from Scratch. *International Monetary Fund*, 44.

Collins, J. E., Vanagt, T., & Huys, I. (2020). Stakeholder Perspectives on Access and Benefit-Sharing for Areas Beyond National Jurisdiction. *Frontiers in Marine Science*, *7*, 265. https://doi.org/10.3389/fmars.2020.00265

Corfield, G. (2021, June 24). *Russia spoofed AIS data to fake British warship's course days before Crimea guns showdown*. https://www.theregister.com/2021/06/24/russia_ais_spoofing/

CFR Editors. (2022, June 28). *What's the Status of North Korea's Nuclear Program?* Council on Foreign Relations. https://www.cfr.org/backgrounder/north-korea-nuclear-weapons-missile-tests-military-capabilities

CFR Editors. (2022, July 27). *What to Know About Sanctions on North Korea*. Council on Foreign Relations. https://www.cfr.org/backgrounder/north-korea-sanctions-un-nuclear-weapons

CRFS. (2019, August 8). AIS Spoofing Detection with TDOA. *CRFS - Spectrum Monitoring and Geolocation*. https://www.crfs.com/blog/ais-spoofing-detection-with-tdoa/

Crummit, K. (2022, April 15). Nations Collaborate to Prevent North Korea from Evading UN Sanctions. *United States Department of State*. https://www.state.gov/dipnote-u-s-department-of-state-official-blog/nations-collaborate-to-prevent-north-korea-from-evading-un-sanctions/

CSIRO. (2020, October 13). *CSIRO busts evidence of illegal fishing and associated crime*. CSIRO. https://www.csiro.au/en/news/news-releases/2020/csiro-busts-evidence-of-illegal-fishing-and-associated-crime

Dinsmore, N., & Salzman, D. (2021, September 13). *What is vessel identity laundering and why does it matter?* Windward. https://windward.ai/blog/north-korean-sanctions-evasion-identity-laundering-explained/

Drezner, D. W. (2022). How not to sanction. *International Affairs*, *98*(5), 1533–1552. https://doi.org/10.1093/ia/iiac065

DTE Staff. (2016, June 27). *Illegal sand mining around the world: Islands disappear; livelihoods at stake*. Down to Earth. https://www.downtoearth.org.in/news/mining/illegal-sand-mining-around-the-world-islands-disappear-livelihoods-threatened-54580

Emmens, T., Amrit, C., Abdi, A., & Ghosh, M. (2021). The promises and perils of Automatic Identification System data. *Expert Systems with Applications*, *178*, 114975. https://doi.org/10.1016/j.eswa.2021.114975

Environmental Defense Fund. (2022). *Overfishing: The most serious threat to our oceans*. Environmental Defense Fund. https://www.edf.org/oceans/overfishing-most-serious-threat-our-oceans

FAO. (2022). *The State of World Fisheries and Aquaculture 2020 in Sustainability in Action*. Rome: Food and Agriculture Organization. https://doi.org/10.4060/ca9229en

Gerstein, J. (2021, September 28). *Singapore is being terrorized by the country's growing population of adorable otters, who've eaten thousands of dollars' worth of expensive koi fish*. Insider. https://www.insider.com/singapore-otters-killing-thousands-of-dollars-of-koi-fish-2021-9

Godfrey, M. (2021, June 22). *IUU vessel-tracker shows possible widespread abuse of AIS switch-off capability*. https://www.seafoodsource.com/news/environment-sustainability/iuu-vessel-tracker-shows-possible-widespread-abuse-of-ais-switch-off-capability

Goodman, J. (2021, September 24). *Great Wall of Lights: China's sea power on Darwin's doorstep | AP News*. https://apnews.com/article/china-oceans-overfishing-squid-294ff1e489589b2510cc806ec898c78f

Goodman, J. (2022, February 8). *Digital warfare tech at sea helping US foes evade sanctions – APEX-Venezuela*. https://apexven.org/digital-warfare-tech-at-sea-helping-us-foes-evade-sanctions/

Gorenburg, D. (2021, July 1). *The HMS Defender Incident: What happened and What Are the Political Ramifications? | Russia Matters*. https://www.russiamatters.org/analysis/hms-defender-incident-what-happened-and-what-are-political-ramifications

Goudossis, A., & Katsikas, S. K. (2019). Towards a secure automatic identification system (AIS). *Journal of Marine Science and Technology*, *24*(2), 410–423. https://doi.org/10.1007/s00773-018-0561-3

Goudosis, A., & Katsikas, S. K. (2020). Secure AIS with Identity-Based Authentication and Encryption. *TransNav, International Journal on Marine Navigation and Safety Od Sea Transportation*, *14*(2). http://www.transnav.eu/Article_Secure_AIS_with_Identity-Based_Authentication_and_Encryption_Goudosis,54,1003.html

Goward, D. (2019, December 17). *Chinese GPS spoofing circles could hide Iran oil shipments*. GPS World. https://www.gpsworld.com/chinese-gps-spoofing-circles-could-hide-iran-oil-shipments/

Goward, D. (2020, May 26). *New GPS "circle spoofing" moves ship locations thousands of miles*. GPS World. https://www.gpsworld.com/new-gps-circle-spoofing-moves-ship-locations-thousands-of-miles/

Greene, S., Jia, H., & Rubio-Domingo, G. (2020). Well-to-tank carbon emissions from crude oil maritime transportation. *Transportation Research Part D: Transport and Environment*, *88*, 102587. https://doi.org/10.1016/j.trd.2020.102587

Harris, M. (2019, November 15). *Ghost ships, crop circles, and soft gold: A GPS mystery in Shanghai*. MIT Technology Review. https://www.technologyreview.com/2019/11/15/131940/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/

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

Hamrock, S. (2019). *Maritime Cyber Security: A Comparative Analysis of U.S. and International Regulation on AIS Data Receptors* [Thesis, Texas A&M]. https://oaktrust.library.tamu.edu/handle/1969.1/175401

HawkEye 360. (2021). Potential Chinese illegal Fishing Seen from Space. *HawkEye 360*. https://www.he360.com/resource/potential-illegal-fishing-seen-from-space/

IMO. (2015). *Revised Guidelines for the ONboard Operational Use of Shipborne Automatic Identification Systems (AIS)*. IMO.

Intertanko. (2019). *Jamming and Spoofing of Global Navigation Satellite Systems (GNSS)*. https://www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf

Jeongmin, K., O'Caroll, C., & Jung, W.-G. (2021, August 20). *South Korea detaining North Korea-linked ship suspected of sanctions violations*. NK News - North Korea News. https://www.nknews.org/2021/08/south-korea-detaining-north-korea-linked-ship-suspected-of-sanctions-violations/

Kundakçi, B., & Nas, S. (2018). Mapping Marine Traffic Density by Using AIS Data: An Application in the Northern Aegean Sea. *Polish Maritime Research*, *25*, 49–58. https://doi.org/10.2478/pomr-2018-0131

Kassai, L. (2020, September 22). Venezuela and Iran Buck U.S. Sanctions Again to Export Crude. *Bloomberg*. https://gcaptain.com/venezuela-and-iran-buck-u-s-sanctions-again-to-export-crude/

Katzman, K. (2022). *Iran Sanctions Congressional Research Service Report* (No. RS20871; p. 100). Congressional Research Service. https://sgp.fas.org/crs/mideast/RS20871.pdf

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), 279–286. https://doi.org/10.12716/1001.14.02.02

Kessler, G. C., Craiger, P., & Haass, J. C. (2018). A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, *12*(3), 429–437. https://doi.org/10.12716/1001.12.03.01

Koetti, C. (2021, March 24). How Illicit Oil Is Smuggled Into North Korea With China's Help. *The New York Times*. https://www.nytimes.com/2021/03/24/world/asia/tankers-north-korea-china.html

Kuo, L., & Sung, L. (2020, March 3). *Against the Grain*. C4ADS. https://c4ads.org/commentary/against-the-grain/

Kuo, L., Sung, L., Byrne, J., & Byrne, J. (2021, March 22). *Black Gold*. C4ADS. https://c4ads.org/reports/black-gold/

Kurmanaev, A. (2022, September 3). How Fake GPS Coordinates Are Leading to Lawlessness on the High Seas. *The New York Times*. https://www.nytimes.com/2022/09/03/world/americas/ships-gps-international-law.html

Le Tixerant, M., Le Guyader, D., Gourmelon, F., & Queffelec, B. (2018). How can Automatic Identification System (AIS) data be used for maritime spatial planning? *Ocean & Coastal Management*, *166*, 18–30. https://doi.org/10.1016/j.ocecoaman.2018.05.005

Lee, Y. (2021, February 5). *China's latest weapon against Taiwan: The sand dredger*. Reuters. https://graphics.reuters.com/TAIWAN-CHINA/SECURITY/jbyvrnzerve/

Lynch, C. (2020, December 23). Iran: Maximum Pressure, Minimum Gain. *Foreign Policy*. https://foreignpolicy.com/2020/12/23/iran-maximum-pressure-trump-policy/

Marine Traffic. (n.d.). *What kind of information is AIS-transmitted?* MarineTraffic Help. Retrieved October 1, 2022, from https://help.marinetraffic.com/hc/en-us/articles/205426887-What-kind-of-information-is-AIS-transmitted-

Maritime Safety Committee (MSC). (2004). *Report of the Maritime Safety Committee on its seventy-ninth Session*. 58–59.

McCauley, D. J., Woods, P., Sullivan, B., Bergman, B., Jablonicky, C., Roan, A., Hirshfield, M., Boerder, K., & Worm, B. (2016). Ending hide and seek at sea. *Science*, *351*(6278), 1148–1150. https://doi.org/10.1126/science.aad5686

Miller, N. A., Roan, A., Hochberg, T., Amos, J., & Kroodsma, D. A. (2018). Identifying Global Patterns of Transshipment Behavior. *Frontiers in Marine Science*, *5*. https://www.frontiersin.org/articles/10.3389/fmars.2018.00240

Natale, F., Gibin, M., Alessandrini, A., Vespe, M., & Paulrud, A. (2015). Mapping Fishing Effort through AIS Data. *PLOS ONE*, *10*(6), e0130746. https://doi.org/10.1371/journal.pone.0130746

Novikov, A. (2019, June 5). *Creating sea routes from the sea of AIS data.* Medium. https://towardsdatascience.com/creating-sea-routes-from-the-sea-of-ais-data-30bc68d8530e

Olmer, N., Comer, B., Roy, B., Mao, X., & Rutherford, D. (2017, October 17). Greenhouse gas emissions from global shipping, 2013–2015. *International Council on Clean Transportation*.

https://theicct.org/publication/greenhouse-gas-emissions-from-global-shipping-2013-2015/

Pallotta, G., Vespe, M., & Bryan, K. (2013). Vessel Pattern Knowledge Discovery from AIS Data: A Framework for Anomaly Detection and Route Prediction. *Entropy*, *15*(6), Article 6. https://doi.org/10.3390/e15062218

Parraga, M. (2020, December 14). Iran uses disguised tanker to export Venezuelan oil—Documents. *Reuters*. https://www.reuters.com/article/venezuela-iran-cargo-idUSL1N2IQ1OZ

Perinchery, A. (2022, April 28). We Are Taking Sand for Granted, and Now a Sand Crisis Is Coming. *The Wire*. https://science.thewire.in/environment/unep-sand-crisis-report/

Poling, G. B., & Cronin, C. (2017). *Illegal, Unreported, and Unregulated Fishing as a National Security Threat*. Center for Strategic and International Studies (CSIS). https://www.jstor.org/stable/resrep23297

Psiaki, M. L., & Humphreys, T. E. (2016). GNSS Spoofing and Detection. *Proceedings of the IEEE*, *104*(6), 1258–1270. https://doi.org/10.1109/JPROC.2016.2526658

Reimer, J., Gravel, C., Brown, M. W., & Taggart, C. T. (2016). Mitigating vessel strikes: The problem of the peripatetic whales and the peripatetic fleet. *Marine Policy*, *68*, 91–99. https://doi.org/10.1016/j.marpol.2016.02.017

Salopek, P. (2019, June 26). *Inside the deadly world of India's sand mining mafia*. Environment. https://www.nationalgeographic.com/environment/article/inside-india-sand-mining-mafia

Saravanan, K., Aswini, S., Kumar, R., & Son, L. H. (2019). How to prevent maritime border collision for fisheries?-A design of Real-Time Automatic Identification System. *Earth Science Informatics*, *12*(2), 241–252. https://doi.org/10.1007/s12145-018-0371-5

Scarr, S., & Sharma, M. (2021, July 19). *Devoured: How China's Poyang lake was decimated by dredging and sand mining*. Reuters. https://graphics.reuters.com/GLOBAL-ENVIRONMENT/SAND-POYANG/qzjpqxxabvx

Sciancalepore, S., Tedeschi, P., Aziz, A., & Di Pietro, R. (2022). Auth-AIS: Secure, Flexible, and Backward-Compatible Authentication of Vessels AIS Broadcasts. *IEEE Transactions on Dependable and Secure Computing*, *19*(4), 2709–2726. https://doi.org/10.1109/TDSC.2021.3069428

Shanghai Maritime Safety Administration. (2021). *Police catch 32 suspects in sand mining cases*. https://english.shanghai.gov.cn/nw48081/20210322/963573d4308d4c299ef7c0ba00ed137c.html

Smith, J. (2020, March 4). North Korea exported sand to China in violation of U.N. sanctions, group says. *Reuters*. https://www.reuters.com/article/us-northkorea-china-sanctions-idUSKBN20R0WB

Sutton, H. (2021, June 21). *Positions of Two NATO Ships Were Falsified Near Russian Black Sea Naval Base*. USNI News. https://news.usni.org/2021/06/21/positions-of-two-nato-ships-were-falsified-near-russian-black-sea-naval-base

Tan, A. (2020, July 29). *260 Chinese fishing vessels surround Galápagos marine reserve, home to endangered species*. Mothership. https://mothership.sg/2020/07/chinese-fishing-vessels-galapagos/

TankerTracker. (2020, December 14). *TankerTrackers.com, Inc.* TankerTrackers.Com. https://tankertrackers.com/articles/the-vlcc-we-identified-in-venezuela-loading-oil-on-behalf-of-iran

Teh, C. (2021, June 15). *China's latest tactic to exert control over Taiwan? Using hundreds of dredgers to carve sand from its coast.* Insider. https://www.insider.com/china-deploys-armada-of-sand-dredgers-carve-up-taiwans-coast-2021-6

The Wire Staff. (2020, June 24). *Unnao: Journalist Who Reported on "Sand Mafia" Killed*. The Wire. https://thewire.in/media/shubham-mani-tripathi-journalist-killed-unnao-sand-mafia

Torrico, G. (2020, December 28). South America plans regional response to illegal squid fishing. *Dialogo Chino*. https://dialogochino.net/en/extractive-industries/39004-south-america-plans-regional-response-to-illegal-giant-squid-fishing/

Tu, E., Zhang, G., Rachmawati, L., Rajabally, E., & Huang, G.-B. (2016). *Exploiting AIS Data for Intelligent Maritime Navigation: A Comprehensive Survey*. http://arxiv.org/abs/1606.00981

Tweedie, N. (2018, July 1). Is the world running out of sand? The truth behind stolen beaches and dredged islands. *The Observer*. https://www.theguardian.com/global/2018/jul/01/riddle-of-the-sands-the-truth-behind-stolen-beaches-and-dredged-islands

Urbina, I. (2020, August 17). *How China's Expanding Fishing Fleet Is Depleting the World's Oceans*. Yale E360.

https://e360.yale.edu/features/how-chinas-expanding-fishing-fleet-is-depleting-worlds-oceans

U.S. Coast Guard. (2014). *Encrypted Automatic Identification System (EAIS) Interface Design Description (IDD)*.

U.S. Coast Guard Navigation Center. (2020). *International & U.S. Inland Navigation Waters*. NOAA. https://nauticalcharts.noaa.gov/publications/coast-pilot/docs/NavigationRulesStandardSize.pdf

Watt, L. (2021, June 16). *Line in the sand: Chinese dredgers are stealing Taiwan, bit by bit*. Nikkei Asia. https://asia.nikkei.com/Spotlight/The-Big-Story/Line-in-the-sand-Chinese-dredgers-are-stealing-Taiwan-bit-by-bit

Welch, H., Clavelle, T., White, T. D., Cimino, M. A., Van Osdel, J., Hochberg, T., Kroodsma, D., & Hazen, E. L. (2022). Hot spots of unseen fishing vessels. *Science Advances*, *8*(44), 11. https://doi.org/10.1126/sciadv.abq2109

Whitehead, J. (2022, January 28). *Maritime conflict heats up as China's fishing fleet goes dark in Argentine waters*. Courthouse News Service. https://www.courthousenews.com/maritime-conflict-heats-up-as-chinas-fishing-fleet-goes-dark-in-argentine-waters/

Willard, D. (2021, September 15). *Breaking down China's seafood trade pathways*. EDFish. https://blogs.edf.org/edfish/2021/09/15/breaking-down-chinas-seafood-trade-pathways/

Wolsing, K., Roepert, L., Bauer, J., & Wehrle, K. (2022). Anomaly Detection in Maritime AIS Tracks: A Review of Recent Approaches. *Journal of Marine Science and Engineering*, *10*(1), 112. https://doi.org/10.3390/jmse10010112

Wright, D., Janzen, C., Bochenek, R., Austin, J., & Page, E. (2019). Marine Observing Applications Using AIS: Automatic Identification System. *Frontiers in Marine Science*, *6*. https://www.frontiersin.org/articles/10.3389/fmars.2019.00537

Xiao, M. (2000). *China maritime safety administration in the new millennium: Challenges and strategies*. World Maritime University. https://commons.wmu.se/all_dissertations/424/

Xiaojun, K. (2021, June 29). *GNSS spoofing threat in China and beyond | Maritime security*. Risk Intelligence. https://www.riskintelligence.eu/background-and-guides/background-gnss-spoofing-in-china-and-beyond

Xinde Marine News. (2018, September 27). *China unveils scheme to weed out illegal docks at Yangtze_信德海事网－专业海事信息咨询服务平台*. https://www.xindemarinenews.com/en/regulations/2018/0927/7434.html

Xu, S. (2014). *Navigation safety analysis and assessment of entry and departure of Shanghai Port for international cruises* [Malmo, Sweden]. World Maritime University.

Yang, D., Wu, L., Wang, S., Jia, H., & Li, K. X. (2019). How big data enriches maritime research – a critical review of Automatic Identification System (AIS) data applications. *Transport Reviews*, *39*(6), 755–773. https://doi.org/10.1080/01441647.2019.1649315

Yin, X., & Peter, T. (2022, August 24). China's shrinking "kidney" lake lays bare growing climate challenges. *Reuters*.

https://www.reuters.com/world/china/chinas-shrinking-kidney-lake-lays-bare-growing-climate-challenges-2022-08-24/

Zhu, G., Xie, Z., Xu, H., Wang, N., Zhang, L., Mao, N., & Cheng, J. (2022). Oil Spill Environmental Risk Assessment and Mapping in Coastal China Using Automatic Identification System (AIS) Data. *Sustainability*, *14*(10), Article 10. https://doi.org/10.3390/su14105837

中国新闻网. (2019). *涉海运输内河船违法AIS设备在上海集中销毁*. https://baijiahao.baidu.com/s?id=1648643608274487560&wfr=spider&for=pc

Appendix A

These signals provide three types of information: static, dynamic, and voyage. Static information is inputted upon installation. It includes the vessel's name, call sign, and Maritime Mobile Service Identity (MMSI) number. The dynamic information AIS uploads automatically including the ship's navigational status, the speed over ground (SOG), and the position of the vessel. The voyage information is manually updated by the crew which contains the estimated time of arrival for the ship's destination, and the vessel's destination (Marine Traffic, 2016).

Utilizing the internet, AIS providers gather and interchange AIS data which enables them to offer data visualization, monitoring, and reporting in free and commercial forms. Maritime authorities use current AIS data to promote Safety of Life at Sea (SOLAS), since AIS enables port authorities to warn ships about hazards such as low tides and shoals, search and rescue (SAR), or to aid a vessel's navigation. The signals and additional information can then be received by any vessel, land station, or satellite with an AIS receiver (See Figure 8) and commonly displayed on screen utilizing chart-plotting software.

AIS enables traffic monitoring, navigational aid, SAR operations, collision avoidance, and accident investigations. AIS started developing in the 1990s and its purpose was for collision avoidance and maritime situational awareness (MSA). AIS data has evolved over the years from navigation-oriented resources to other applications including vessel performance monitoring, emission accounting and trade analysis.

The system contains unencrypted VHF signals that can easily be manipulated by anyone with access to materials to broadcast a higher signal simultaneously with the vessel at the same frequency and change the message. The evolution from the short-range exchange of data to the exchange of data on the Internet of Things (IoT) from satellite, enables AIS to transmit and receive information that is seized and shared for several unknown purposes.

AIS spoofing includes fabricating valid AIS information remotely, such as a non-existent ship or aid of navigation, from not anywhere close to a body of water or an AIS station. AIS hijacking incorporates altering any information about existing AIS stations, such as SOG, cargo, location, and the flag of the country of a real vessel. Availability disruption occurs over radio frequency and mostly deals with an attacker impersonating a maritime authority.

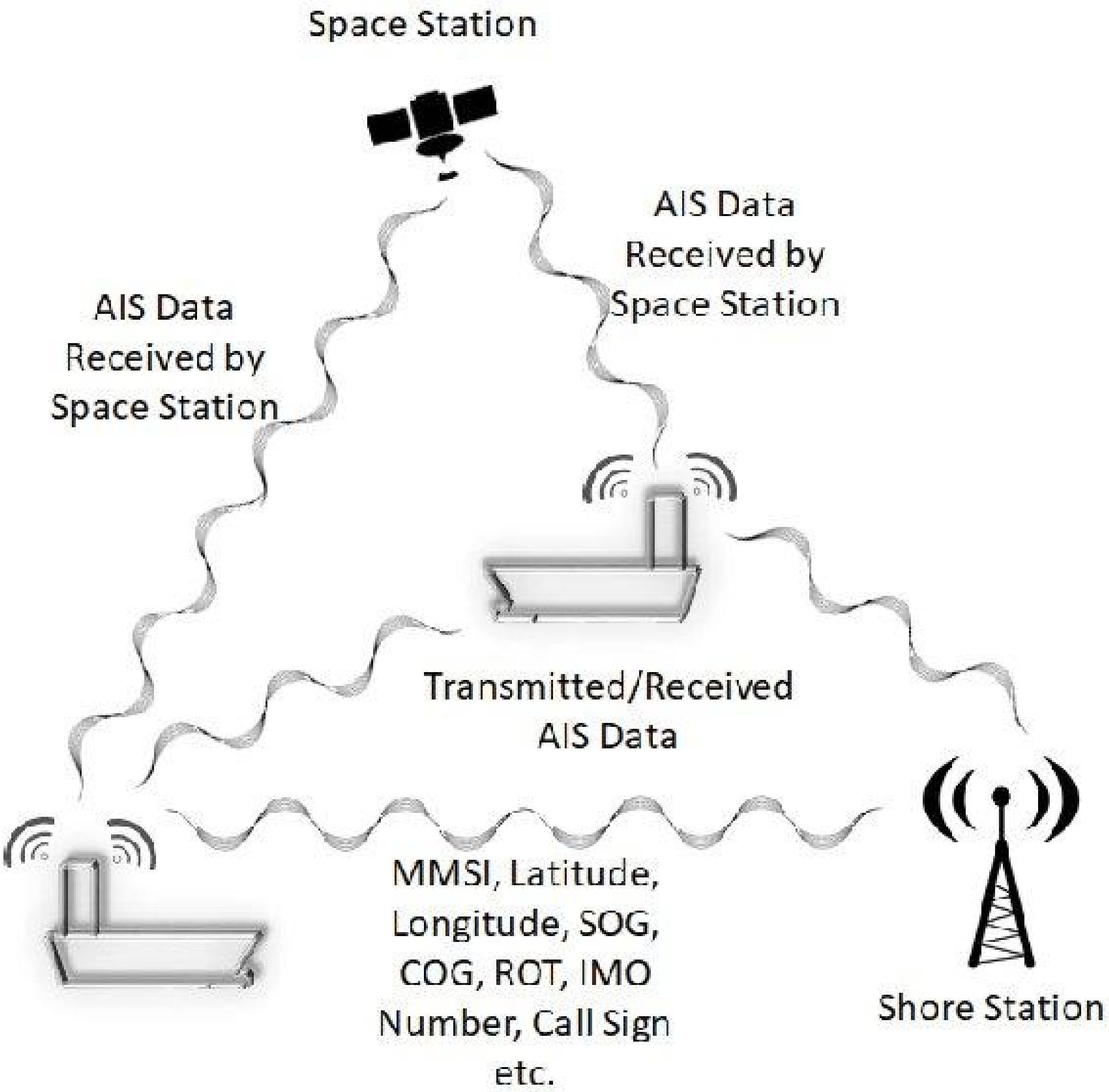
Through these vulnerabilities, an actor with ill intentions can: spoof a non-existent aid to navigation or vessel, replay AIS events, send false meteorological information, modify vessel information sent through VHF, set off a denial-of-service attack on the AIS broadcast system, and send false SOS (Save Our Ship) or collision alerts. Since AIS does not allow any system of checks for these pieces of information, the information sent is less reliable and the data remains vulnerable to distortion. Malicious actors remain tempted to distort AIS for their own purposes due to the high reward of their crimes, such as pirates spoofing AIS to redirect ships to rob, IUU fishers utilize AIS manipulation to remain hidden and mislead authorities and others, and enable thieves to dredge sand and minerals (Emmens et al., 2021).

The difficulty of high seas management concerns the globe and can become easier with the adoption of AIS integrating with parallel closed-access systems. McCauley et al. (2016) states this AIS integration will increase transparency with the improving the view of vessel activity which can aid in ocean management and cites evidence that it is possible to equip all commercial fishing vessels in the world and enforce the use of it. The lack of legislative support for regulating and modifying AIS will lead to the continued exploitation of AIS's vulnerabilities.

Data analytics can help greatly by examining when and what vessels are spoofing or turning off their AIS transponders.

Figure 8

The Working Principle of AIS


Space Station
AIS Data Received by Space Station
AIS Data Received by Space Station
Transmitted/Received AIS Data
MMSI, Latitude, Longitude, SOG, COG, ROT, IMO Number, Call Sign etc.
Shore Station

Note. A visual on how AIS works. Kundakçi, B., & Nas, S. (2018). Mapping Marine Traffic Density by Using AIS Data: An Application in the Northern Aegean Sea. *Polish Maritime Research*, *25*, 49–58. https://doi.org/10.2478/pomr-2018-0131

Appendix B

India's Sand Mafia. India's infrastructure boom has caused massive environmental effects on India already. India's sand industry is accused of consisting of prominent members such as businessmen and politicians. There have been links present between sand mafia bosses and police chiefs, causing an unfortunate pattern between most journalists who try to cover the sand mafia and death of said journalists (The Wire Staff, 2020). The sand mafia has also killed law enforcement officers that have tried to halt the sand-mining of India's rivers. The sand mafia earns most of its money through extorting domestic laborers, inflating prices, and police bribes, but there have been other reports exhibiting the extent of India's greed for sand (Salopek, 2019). The loss of sand in India's region puts its people at high risk, as it increases the turbidity of the water, affecting its oxygen content and the creatures that can survive there, along with causing the disappearance of deltas (Perinchery, 2022). AIS spoofing is one of the essential ways that the sand mafia can deliver sand throughout the region.

The author feels that there must be AIS spoofing within this area, as the sand mafia has connections all over Asia, but was unable to find quality resources within the subject area. This is most likely due to the deaths of most journalists, researchers, and law enforcement officer's covering the topic. Sand mafias run deep throughout the regions of developing countries, making coverage difficult and dangerous, resulting in the lack of publicly available and quality information. There was a link that seemed to have quality and available information on the topic but directed the author to an error page across other devices.