Under the Radar: Weaponizing Maritime Transponders in Strategic Competition

Description

Throughout the summer and fall of 2023, Peopleâ??s Liberation Army Navy (PLAN) and China Coast Guard (CCG) vessels have repeatedly blockaded Filipino shoals and naval outposts in the South China Sea, restricting freedom of movement and preventing resupply efforts. The CCG continues to employ water cannons, lasers, and floating underwater barriers against Filipino boats in order to usurp control over the Republic of the Philippinesâ?? maritime territory. While PLAN vessels assume a standby role and the CCG acts as the aggressor, a third, lesser-known Chinese fleet is heavily involved in these naval operations: the Peopleâ??s Armed Forces Maritime Militia, or PAFMM.

The PAFMM is a state-created maritime militia composed of â??commercialâ?• fishing vessels and their crews. It directly supports the PLAN by using swarming tactics to assert physical control over disputed maritime territory and physically block other naval vessels from reclaiming their waters. PAFMM fleets have also been implicated in causing massive environmental damage and economic losses via the destruction of Filipino coral reefs.

The presence of tens, if not hundreds, of vessels in a relatively small maritime domain seems hard to go unnoticed. However, PAFMM vessels disappear from or falsify their identities on global shipping trackers, making it incredibly difficult to locate PAFMM activity and prosecute involved parties. This new trend is enabled by manipulating their vessel signatures on Automatic Identification Systems.

Exploiting a weakness in maritime tracking

An Automated Identification System, or AIS, is a maritime transponder used to transmit a vesselâ??s identity and location to a worldwide network. While intended to be used to track vessels and maintain crewsâ?? situational awareness, criminal actors manipulate their shipsâ?? AIS signatures to hide or fake their locations and disguise illicit activities. Strategic competitorsâ??specifically Russia, China, and Iranâ??are also beginning to use AIS manipulation, but with increasing technological complexity. Simpler forms of AIS manipulation are used as an economic tool for their commercial shipping fleets, letting them conduct trade in direct violation of international sanctions to fund their militaries and wartime activities. However, the vulnerabilities inherent in AIS make it easy for technologically advanced state-level actors to hack and weaponize AIS to fabricate a potential *casus belli* in disputed maritime regions. Artificial intelligence and technological surveillance are used to identify low-tech

spoofing actors, but cannot be used to stop state-sponsored AIS manipulation, making AIS vulnerabilities a grave naval security concern.

AIS broadcasting is required by the International Maritime Organization (IMO) for all ships above 500 gross tonnage, any ship over 300 gross tonnage on an international voyage, or any passenger vessel (e.g., cruise ships and ferries). Individual countries and supranational entities can also mandate AIS for smaller ships within their waters. However, AIS data is transmitted over unprotected very high frequency (VHF) radio bands, making the system susceptible to exploitation by malefactors who want to circumvent maritime law and do not want to be tracked on the high seas. AIS vulnerabilities lead to four principal threats: going dark, spoofing, hijacking, and availability disruption.

Crews can turn off their shipsâ?? AIS transponders, allowing them to â??go darkâ?• and roam the seas mostly undetected. Illegal, unreported, and unregulated (IUU) fishing fleets often disable their AIS transponders and â??go darkâ?• next to contested maritime boundaries or exclusive economic zones (EEZs), which they would not otherwise be able to legally enter. For instance, in 2019, the South Korea-flagged vessel *Oyang 77* penetrated the Argentinean EEZ, turned its transponder off to avoid detection, and illegally caught over 310,000 pounds of seafood.

AIS spoofing or manipulation describes broadcasting an AIS message with fake position or identity data to disguise a shipâ??s identity or location. A prime example is the vessel *Kingsway*, which evaded international authorities for over four years while skirting U.N. Security Council-imposed sanctions and profiting from oil trade with North Korea. It repeatedly changed its vessel identification number, name, flag, and paint scheme, while spoofing its location via AIS to avoid being tracked as it continued to engage in sanctions evasion. Spoofing multiple false characteristics via AIS in this manner is an increasingly common strategy.

AIS hijacking occurs when a malefactor adjusts AIS data packets from another partyâ??s vessel to display false information. This technique is similar to AIS spoofing, but spoofing is used to fake oneâ??s own vesselsâ?? information, while hijacking is used to fake someone elseâ??s. For example, researcher Mario Balduzzi was able to hijack the AIS transponder of the U.S.-flagged *Eleanor Gordon* and faked its position to appear in the middle of Dallas, Texas.

Lastly, AIS availability can be disrupted by overwhelming rate-limited AIS receivers with random data. This approach would render AIS receivers onboard ships and at ground stations unusable, as they would be unable to distinguish real AIS reports amid the influx of fake signals. AIS availability disruption is technologically challenging to accomplish as it requires sophisticated programming skills; to the authorâ??s knowledge, it has not been used maliciously at the time of this writing. However, Balduzzi et al. have performed multiple simulated availability disruption attacks to demonstrate their

effectiveness.

Spoofing

While all four types of AIS deception can be used on the high seas, some are used more frequently than others. AIS disruption is the most technologically difficult to accomplish, as it requires advanced programming knowledge to spoof signals and an understanding of AIS receiver limitations. On the other hand, despite being the technologically simplest option, turning off oneâ??s AIS transponder creates a gap in the vesselâ??s AIS transmission history, which can be easily found through AIS tracking services like *MarineTraffic*. Such an anomaly can put a dark ship and its crew under scrutiny. Thus, malign actors are gradually shifting away from going dark and towards AIS manipulation and hijacking.

AIS Manipulation Strategies

AIS spoofing is an effective method to disguise gray zone or illegal maritime activities, as it can be used to realistically fake oneâ??s location and activities. According to Dr. Joshua Tallis at the Center for Naval Analyses (CNA) in an interview for this piece, â??If you can make it look like youâ??re somewhere else doing a credible or licit type of transaction or activity, it reduces scrutiny on youâ?• from law enforcement, insurance companies, marine traffic sites, and other watchdogs. Three main subcategories of AIS manipulation strategies are being leveraged more widely: location tampering, the use of zombie vessels, and AIS handshakes.

Location tampering occurs when an actor generates fake GPS location data and applies it to its AIS signature to disguise its location. Vessels often spoof multiple GPS points to create a fake track, rather than just disguising a singular position. This can be accomplished via GPS tampering, done either onboard a vessel or from shore. Location tampering is the simplest and most common form of AIS spoofing, as it can be accomplished by any actor with access to AIS transponders or data streams, and it disguises oneâ??s activities better than going dark. In 2023 over 50 oil tankers appeared on AIS trackers transiting to the Atlantic via the Cape of Good Hope and the West African coastline. However, Spire Maritime discovered that these vessels were actually entering the Venezuelan EEZ and likely taking on Venezuelan oil in breach of international oil sanctions, which they were able to do undetected by spoofing their AIS locations. These vessels would then return to Chinese or Malaysian ports while reporting their true positions and offload their illicit cargo as if it was a routine voyage. However, to an external observer solely viewing their AIS transmissions, it would look like the sanctions evasion never happened.

According to *Windward*, zombie vessels use â??a scrapped vesselâ??s identity to perform illicit operations without legal repercussions.â?• When a vessel is scrapped, its identity is not always scrapped with it. A non-seaworthy shipâ??s identity can be â??resurrectedâ?• by placing its Maritime Mobile Service Identity (MMSI) and other AIS identity characteristics on a floating vessel. For example, a Marshall Islands-flagged vessel was scrapped on April 21st, 2022; two months later, it appeared to be floating again, when its identity was assumed by a ship known for sanctions evasion.

AIS handshakes occur when two vessels with similar physical characteristics get physically close and temporarily exchange AIS identities. The vessel carrying cargo now has the AIS signature of the decoy vessel, letting it travel undercover while appearing to be the other vessel. Meanwhile, the decoy vessel maintains its position while pretending to be the original cargo-carrying vessel, allowing both ships to maintain mostly continuous AIS tracks. Once the two rendezvous again, they re-swap identities and carry on, making it appear like the original vessel never visited its secret destination. As AIS handshakes involve a swap and re-swap of identities at pre-arranged locations, handshakes must occur with the consent and knowledge of both vessels involved (hence the term â??handshakeâ?•). For example, in the Gulf of Oman on April 26th, 2020, the Saint Kitts and Nevis-flagged *Giessel* temporarily swapped its identity with a slightly smaller vessel. The original *Giessel* likely then went to an Iranian port and loaded crude oil, while the â??fakeâ?• *Giessel* maintained the pre-swap position of the original vessel. The original *Giessel* returned to the meeting point and identities were re-swapped, allowing the original *Giessel* to resume its travels like nothing had transpired â?? except that it now had a full draft.

Deceptive tactics

Identifying AIS manipulators

With over 400,000 AIS broadcasting devices operating worldwide and thousands of ships on the seas at any given time, it is almost impossible to manually filter through AIS data to identify every AIS spoofing ship and operator. However, new technologies can help law enforcement agencies and insurance companies identify and track AIS manipulators. Websites like *MarineTraffic* track the AIS signatures of almost all broadcasting vessels worldwide and maintain vessel histories and tracks. Companies like *Windward* and *HawkEye 360* use artificial intelligence and data processing algorithms to look for ships displaying unusual AIS tracks, such as stopping in the middle of the ocean for extended periods, zigzagging, or disappearing and reappearing somewhere completely different. They can then flag such vessels for further investigation. Radar monitoring and time difference of arrival (TDOA) analyses can also help identify spoofed ships or ones that display fake AIS data.

If a vessel is suspected of spoofing, its AIS tracks can be compared with satellite imagery or radio frequency detection in the region it reports its position from to confirm its presence or lack thereof. If the shipâ??s crew can be identified, tracking their social media posts can also reveal clues as to their true location. However, as noted above, it is technologically difficult to surveille the thousands of ships sailing the oceans daily, and these are primarily used as investigative tools if a specific ship exhibits suspicious behavior.

For instance, on Jan. 18th, 2023, over three tons of cocaine was seized off Western Saharaâ??s coast from Togo-flagged cargo vessel *Blume*. According to *Windward*, the *Blume* had changed its MMSI identifier multiple times and regularly altered flags, but also went dark immediately after a drastic change in course â?? all unusual activities for regular cargo vessels. *Blume* is an example of how AIS data manipulation can easily disguise vessels by changing their reported characteristics and flags, a vulnerability susceptible to exploitation by malefactors. However, it also showcases how easy it is to identify ships going dark, which immediately places them under suspicion. This explains the new trend of bad actors moving away from going dark towards more complex AIS spoofing.

AIS and strategic competition

While AIS manipulation has direct applications for criminal actors, strategic competitors â?? specifically Russia, China, and Iran â?? are beginning to rely on AIS spoofing as well. These countriesâ?? usage of AIS spoofing can be placed in two broad categories: â??low-techâ?• spoofing methods, such as going dark or faking oneâ??s location, and â??high-techâ?• methods, such as hijacking and network disruption. Much like criminal actors, Russia, China and Iran also rely on low-tech AIS manipulation, but specifically use these methods to subvert international sanctions. However, unlike criminal actors, Russia, China and Iran have the technological capability to use high-tech AIS spoofing strategies in direct support of offensive military activities, prompting dire maritime security concerns.

Low-tech spoofing to evade sanctions

According to *Windward*, over half of location tampering incidents between 2021 and 2023 occurred near Iran and were assessed to be associated with petrochemical transfers. Iranian-flagged oil tankers have also engaged in oil trade with Syria, exporting over $1 billion worth of oil in a six-month period. Similarly, throughout the war in Ukraine, increasing numbers of large vessels have been going dark or spoofing their locations in the Russian-controlled Kerch Strait, enabling the continuation of Russian maritime trade despite heavy sanctions on Russian shipping. Many ships conducting AIS manipulation in these regions or under the aforementioned countriesâ?? flags do so to evade global sanctions, simultaneously bringing back profit to their governments through state-owned enterprises.

An example of state-sanctioned commercial shipping using AIS spoofing is the fleet of the National Iranian Oil Company (NIOC), which charters vessels to trade with Venezuelaâ??s sanctioned oil industry. The NIOC-linked tanker *Calliop* turned into a zombie vessel by adopting the identity of the scrapped vessel *Ndros*, while another ship switched AIS identities from *Horse* to *Master Honey* to enter the Venezuelan port of Jose and offload oil.

Like Russia and Iran, the Chinese government permits and engages in commercial AIS spoofing to trade with sanctioned entities. Sanctioned vessels like the *Kingsway* regularly travel between North Korean and Chinese ports and offload cargo like coal and oil. In an interview with naval expert Brent Sadler at The Heritage Foundation, he pointed out that the regularity of sanctioned vessels conducting business in Chinese ports results from Chinaâ??s â??nefarious intentâ?• and intentional subversion of international law.

Ship

Thus, much like commercial AIS spoofing, state-sanctioned AIS manipulation is an economic tool for the commercial shipping fleets of Russia, Iran, and China, used to disguise violations of sanctions on the high seas. State actor-endorsed AIS spoofing can be directly linked to illegal military development. The United States Attorneyâ??s Office indicted five Russian nationals and two oil traders as key parts of a global criminal conspiracy. Oil smuggling between Russia, China, and Venezuela â?? most likely relying on some form of AIS manipulation â?? was used to fund a German front company, which purchased sensitive U.S. military technologies and brought them back to Russia. Similarly, the U.S. Department of the Treasury has identified a network linking Iranian oil smuggling to the Russian government along with funding for the Iranian Revolutionary Guard Corps (IRGC) and Hezbollah. For Russia, China, and Iran, illegal shipping activities such as these directly fund war efforts and accelerate illegal military technology transfers.

High-tech spoofing as a political naval tool

In addition to using simpler forms of AIS manipulation to help illegally fund their war chests, Russia, China, and Iran also employ AIS spoofing as an offensive instrument of statecraft. With their continual development of advanced cyberwarfare capabilities, Russia, China, and Iran have the ability to employ AIS manipulation tactics in complex and harder-to-detect ways. Sanctions evasion relies on isolated ships going dark or faking their locations, which is relatively easy to accomplish. However, with advanced cyber capabilities, these states can hide or spoof the locations of entire flotillas in concert with each other to disguise massive naval activities, wreak havoc by disrupting AIS availability within a locale, or hijack and spoof the locations of ships for propaganda.

When conducted by state actors, AIS spoofing is a political activity designed to directly push and subvert recognized maritime boundaries while simultaneously projecting naval power. As CNAâ??s Dr. Joshua Tallis told the author, â??AIS spoofing [and] disabling is an inherently political activity, because it assumes the implied sovereignty of existing maritime demarcations.â?• For instance, when a vessel fakes its location outside of an EEZ but secretly trespasses into it to fish, spoofing its AIS signature implies that the vesselâ??s crew acknowledges that they cannot legally enter the EEZ without permission, which means that they recognize the maritime boundaries of the country whose EEZ they illegally entered. It also shows that the crews (and, if conducting state-sanctioned activities, their governments) are intentionally disregarding and subverting the international rule of law governing EEZs.

Chinese fishing fleets frequently engage in this practice around EEZs in the Pacific, particularly in the Taiwan Strait and off the western coast of South America. Brent Sadler noted in an interview that these fleets often have a singular AIS account for all their ships and use it on hacked AIS transponders, allowing them to avoid the costs of setting up individual AIS systems and skirt around EEZ regulations. Many of these boats are also linked to the PAFMM. Chinese fishing fleets and the PAFMM are instrumental in securing Chinaâ??s territorial claims around the Nine-Dash Line.

In addition to employing AIS spoofing *en masse* to hide oneâ??s own naval activity, AIS spoofing and hijacking can also be applied to large numbers of non-owned vessels to disrupt shipping operations. For instance, in 2019, the Port of Shanghai employed AIS â??crop circles,â?• a practical application of AIS availability disruption. By hacking AIS transponders to generate fake data (in the shape of a circle) and overload AIS receivers, Chinese state-sponsored hackers were able to distort commercial vesselsâ?? AIS locations, generate false collision reports, and even disable shipsâ?? AIS transponders remotely. Similarly, in May 2023, pro-Russian hackers hacked the AIS signatures of a number of merchant vessels to draw AIS tracks resembling the â??Zâ?• symbol associated with the Russian war effort. Though ultimately harmless, the exercise demonstrates the utility of AIS hacking for propaganda generation, and shows that with advanced technology, multiple ships can be AIS-hacked at once to produce a singular effect.

AIS spoofing as *casus belli*

While state-sponsored AIS spoofing can be used to create propaganda, it can also be used to target specific ships, whether commercial or military. A technologically savvy malefactor could hijack any vesselâ??s AIS and spoof its location into waters it should not be in, fabricating a *casus belli*.

To Russia, China, and Iran, spoofing the locations of ships â?? whether spoofing their own to safety, or spoofing others into a danger zone â?? is a political action used to enforce their ideas of maritime boundaries. As Dr. Tallis from CNA explains, â??itâ??s aboutâ?¦ either clarifying or muddying (depending on the objective) who has the right to be where.â?• Spoofing someone elseâ??s ships into oneâ??s territorial waters (either internationally recognized or claimed) helps to push a state narrative of state-claimed-rights, and can act as a perfect pretext for diplomatic incidents, fueling state propaganda, or even as a justification for direct assault or a declaration of war.

Iran has used this strategy to justify civilian cargo ship seizures, such as that of the *Stena Impero* in July 2019, leading the U.S. Department of Transportationâ??s Maritime Administration to warn vessels in the Arabian Gulf of the risks of â??GPS interference, AIS spoofing,â?• and communications faking and jamming. Due to the lack of safeguards on AIS systems, the same strategy can be applied to military naval vessels as well, as demonstrated by Russia in 2021.

On June 23rd, 2021, *HMS Defender* sailed through Crimean waters. According to its AIS track, the Royal Navy vessel went 1.8 nautical miles inside disputed waters and continued on course. According to a BBC journalist onboard, over 20 Russian naval vessels and air assets shadowed and buzzed the *Defender*, fired warning shots, and supposedly dropped bombs near the ship, warning that it was in Russian territorial waters. If the *Defender* had switched off its AIS, or had its AIS spoofed from the disputed region a few miles further into internationally recognized Russian waters, the Russian military would have a pretext to declare a violation of its maritime territory and take offensive military action against the *Defender* and its crew. Thankfully, this did not happen. However, as shown by Iranian spoofing of commercial vessels and subsequent seizures, along with the likely Russian-sponsored spoofing of two NATO warships off the coast of Sevastopol and even the spoofing of a carrier strike group, spoofing an enemy navy vesselâ??s location and using it as a cause for offensive activity is a distinct possibility in maritime gray zone areas.

Combatting AIS weaknesses

Non-state actors use AIS spoofing to enable smuggling of illegal goods, trade with sanctioned entities, and other illegal activities. However, state actors â?? particularly Russia, China, and Iran â?? are starting to adopt the same techniques and use them for sanctions evasion along with offensive naval posturing. Commercial AIS spoofing directly supports Russiaâ??s war effort, the IRGC, and the North Korean military. Additionally, the PLAN and its merchant marines regularly tamper with their AIS signatures to disguise illegal fishing activities, violate other countriesâ?? EEZs, and exercise greater naval control over the Taiwan Strait. Similarly, Russia has used AIS manipulation of NATO ships, especially in the lead-up to and during its war with Ukraine, to provoke diplomatic conflict and generate

propaganda, and Iran uses AIS manipulation to drive ships into its waters and seize them.

Identifying criminal actors and low-tech state-sponsored entities who use AIS spoofing can be done relatively easily, thanks to a combination of massive real-time global AIS datasets and artificial intelligence algorithms that can detect discrepancies within them. However, it is not sufficient to merely identify instances of high-tech state-sponsored AIS hacking, hijacking, and disruption. These activities drastically increase the danger of seizures and attacks on commercial shipping and other naval vessels operating near Russian, Iranian, and Chinese-claimed territorial waters. To eliminate a possible maritime *casus belli* against U.S. and partner naval forces worldwide, concrete action must be taken to make it difficult or impossible for state actors to hijack AIS.

The most direct way to combat AIS vulnerabilities to hacking is to secure AIS signals. AIS signals are currently transmitted over unencrypted channels, which, as discussed above, can be spoofed with ease using commercially-available tools. However, these channels can be secured through an authentication or encryption mechanism, which would be compatible with current AIS receivers without needing hardware adjustments. By encrypting AIS channels, it becomes more difficult for a malefactor to spoof a vesselâ??s location, and even more so to hack the AIS transponder of a ship.

The emergence of AIS spoofing and manipulation represents a significant and evolving trend with implications for maritime irregular warfare. By enabling state and non-state actors to conceal or falsify the locations and identities of vessels, these tactics introduce a complex layer of deception and strategic ambiguity in the maritime domain. This not only complicates the enforcement of international maritime law, but also heightens the risks of escalation and provocation of maritime conflicts.

The modern threat landscape is characterized by asymmetric warfare, emerging technology, and gray zones. AIS manipulation is a prime example of how these characteristics come together to make the line between deception and reality as elusive and shifting as the sea itself.

Umar Ahmed Badami is a sophomore at Georgetown Universityâ??s School of Foreign Service and an intern for the Irregular Warfare Initiative.

The views expressed are those of the author and do not reflect the official position of the United States Military Academy, Department of the Army, Department of Defense, or Georgetown University.

Date Created
2023/12/05