1. Introduction
   1. As IUUF and sanction evasion becomes more prevalent, recognizing and combating AIS spoofing will be important for mariners and nation states to protect their natural resources and national security.
2. Overview
   1. What literally is this?
      1. What does it mean to do AIS spoofing?

* Used to describe intentional manipulation of vessel characteristics including: identity, positional, navigational, and speed data. Includes both altercation and fabrication of data.
  + 1. What laws and language exist?
* AIS is mandated for ships exceeding 300 gross tonnage and for all passenger ships.
  + 1. How is it done? (quotes from Polestar Global)
       1. Long Term Anchor
       2. Circle
       3. Slow Roll
       4. Pre-programmed route
  1. Major Actors (who does this and why?)
     1. China or other entities engaging in IUUF, to fish endangered species, to fish in illegal locations.
     2. Russia, to falsify operations and stir trouble.
     3. Actors looking to avoid sanctions. Typically, North Koreans and Russians or Indians trying to hide the locals of their cargos.
  2. Major Issues (define problems caused by each of the reasons to spoof)
     1. Impersonation
        1. “In the early hours of June 19, the site's tracking data showed the HMS Defender and a Dutch frigate, HNLMS Evertsen, approaching the port of Sevastopol in Crimea. The strange thing is, they weren't there.” (Bateman, 2021).
     2. Obfuscation
        1. “Such switching to low power transmit mode could be indicative of suspicious activity since coastal Base Stations will be less likely to receive ship transponder messages.” (Kelly, 2022, p. 2).
     3. Spoofing Attack by Hostile Entities
        1. “Driving a vessel off course or re-routing it by spoofing the presence of virtual aids to navigation (VAtoN) via a spoofed ‘AIS Message 21’” (Wimpenny et al., 2022, p. 334).
        2. “Spoofing a vessel’s reported position by providing it with false DGNSS corrections via a spoofed ‘AIS Message 17’” (Wimpenny et al., 2022, p. 334).
        3. “Performing denial of service attacks by misusing AIS channel management broadcasts via spoofing ‘AIS Message 22’” (Wimpenny et al., 2022, p. 334).
     4. Disguising illegal activity.
        1. “As reported by C4ADS, smugglers suspected of evading sanctions on North Korea have turned to this scheme to create fraudulent identities for sanctioned ships.” (Sasson, 2021).
  3. Solutions proposed by experts.
     1. Using RADAR and satellites and base stations
        1. Pros: Don’t have to push software out on the fleet, uses existing technology.
        2. Cons:
           1. Requires additional resources for law enforcement to man RADAR and Satellite stations to check the validity of AIS data.
           2. “RADARSAT imagery data acquisition time and AIS data acquisition time may be different, the target vessel may move away from one position to another during the period of two different data acquisition times; therefore, the association between imagery and AIS data may not be very conclusive.” (Guo, 2014, p. 1).
     2. AISChain and BATMAN
        1. Pro: Using computing power to detect suspicious activity requires no additional equipment, and programming is cool.
        2. Con: AI Partnership with Law Enforcement may lead to violent overreaches in the event of false positives.
     3. Public Key System (Securing the automatic identification system (AIS): using public key cryptography to prevent spoofing whilst retaining backwards compatibility) all of these are (Wimpenny et al., 2022, p .335).
        1. Pros:
           1. “Using PKC to ‘digitally sign’ messages, as capable of providing unequivocal evidence that all AIS message types originate from genuine sources and so can be trusted.”
           2. “direction-finding techniques can only confirm a signal is on a correct bearing.”
        2. Cons:
           1. “AIS lacks sufficient bandwidth to routinely authenticate all messages.”
           2. “Phasing in the proposed solution is likely to be a slow process, both politically and technically.”
           3. Difficult to establish trust, must choose between Certificate Authority or Web of Trust method. Both require trusting a 3rd party to vouch for the validity of the 2nd party’s key.
     4. Compare and contrast Solutions.
        1. Surprising no-one, it’s to take elements from all three. This is most costly, but most effective.
           1. Public Key strategy means that you can be very sure that the AIS message you receive is unaltered and from the correct person, but people can still force the AIS to transmit bad data.
           2. Using AI to detect the classic patterns of spoofed AIS information can detect when someone could be lying.
           3. RADARSAT and Low Power detection to catch dishonest vessels red handed.
           4. Of course, none of this is worth anything unless the Coast Guards of the world commit to stopping vessels, arresting smugglers, and fining owners for deliberately transmitting false AIS data.
  4. Possible Negatives from our favorite solution
     1. Negative Impacts to Industry
        1. Upgrading the computers in the AIS transponders may cost a little extra money.
     2. Negative Impacts to Environment
        1. AISChain and the spoofing detecting AI “BATMAN” may require a lot of processing time and electricity, most if not all may be from non-renewable sources.
        2. RADARSAT detection stations are not carbon neutral.
     3. Negative Impacts to Society
        1. Big Brother Spying on ships to make sure they are who they say they are, where they say they are, that they’re going where they say they’re going, and that when they get there, they will do what they said they’ll do is ethically tenuous.
     4. Negative Impacts to Profession
        1. The problem of establishing trust in the public key strategy opens a nest of problems relating to reliability and liability of Certificate Authorities or the peers in a web of trust. Could be a Flag-of-Convenience situation but in the tech space.
        2. Use of AI based systems may make it harder for an honest vessel to be proven innocent if their true data happens to set off a flag in the program.
  5. Positive Impacts from our favorite solution
     1. Positive Impacts to Industry
        1. More effective tracking of vessels with AIS without the spoofed data clouding the pool may mean additional transparency and safety in the waterways, leading to reduced insurance premiums.
     2. Positive Impacts to Environment
        1. Help to catch illegal fishing operations and dark-oil smuggling.
     3. Positive Impacts to Society
        1. Reduce likelihood of successful maritime cyber-terrorist attacks.
     4. Positive Impacts to Profession
        1. Knowing that you can trust your AIS data means that officers can be less paranoid about the screens matching reality and can more easily make collision avoidance decisions.
  6. Conclusion
     1. Influence of (our favorite solution) on the careers of the people who are listening to us right now.
        1. No matter what solution ends up getting picked, this generation of officers will be on deck when the change is implemented. Understand what an anti-spoofing software update means as far as what you have to do as the mate to ensure it’s working correctly, start thinking about how to explain it to the weathered old hulks, and be aware that no solution can make all forms of cyber attack through AIS impossible. Always check your contacts on the radar and visually, and call the captain before you start worrying.
  7. Class Discussion Questions.
     1. Joey’s Questions.
        1. What solution do you think is the best? Is there something obvious I didn’t think of?
        2. What should be the role of law enforcement in such a case? Can detection of probable spoofing be an actionable reason to get a warrant?
        3. What kinds of spoofing attacks might still get through the solution we picked?
        4. Can it be considered an act of war to launch an AIS based cyber attack like in the case of the Defender?
        5. Should the AIS legal requirement be expanded to include more vessels?
     2. Ben’s Questions.
        1. 1
        2. 2
        3. 3
        4. 4
        5. 5