TRANSNAV
http://www.transnav.eu
the International Journal
on Marine Navigation
and Safety of Sea Transportation
Volume 12
Number 3
September 2018

DOI: 10.12716/1001.12.03.01

A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System

G.C. Kessler, J.P. Craiger
Embry-Riddle Aeronautical University, Daytona Beach, FL, United States

J.C. Haass
Embry-Riddle Aeronautical University, Prescott, AZ, United States

ABSTRACT: The maritime transportation system is increasingly a target of cyber attacks. This paper describes a taxonomy that supports the creation of adversarial cyber models, risk mitigation, and resiliency plans as applied to the maritime industry, using the Automatic Identification System as a specific illustration of the approach. This method has already been applied to the aviation sector; retooling it for a maritime example demonstrates its broad applicability to the transportation sector, in general.

1 INTRODUCTION

Cybersecurity vulnerabilities, exploits, and threats are on the rise across all critical infrastructure sectors, particularly transportation. In previous work, the authors proposed a graph-based, communications-oriented framework and taxonomy with which to create adversarial models, risk mitigation, and resiliency plans for the aviation sector (Haass, Craiger, & Kessler, 2018). We propose to apply this framework and taxonomy to maritime systems in order to demonstrate the general applicability of the methodology.

There are many analogues between the aviation and maritime transportation sectors; whereas aviation has airport operations, air traffic control, airline operations, aircraft operations, and unmanned aircraft systems, maritime has port operations, vessel traffic services (VTS), shipping line operations, vessel operations, and unmanned maritime systems, respectively. Both sectors have manufacturing, cargo and passenger transport, and handoffs of passengers and cargo to other modes of transportation. Both have a broad variety of users, including commercial, military, individual, corporate, and public sector craft. And both are subject to attack by a variety of cyber actors, ranging from criminals and hacktivists, to spies, terrorists, and information warriors. Indeed, there are similarities to other transportation sectors (e.g., trucking and railroads), as well as other critical infrastructure sectors.

Numerous maritime-specific communications systems are used for navigation, ship-to-ship and ship-to-shore information exchange, vessel management and control, cargo scheduling and management, passenger entertainment, and safety. Most of these systems were created without cybersecurity in mind and well before the widespread cyberattacks that are now so common on the Internet. From maritime automated navigation systems and the Automatic Identification System (AIS) to Global Navigation Satellite Systems (GNSS) and the Long-Range Identification and Tracking (LRIT) network, it is clear that it is important to design, deploy, and maintain critical maritime systems with appropriate adversarial models, risk frameworks, and resiliency plans (Kessler, 2019).

Using a general system-of-systems approach outlined in a review paper by Haass, Sampigethaya, and Capezzuto (2016) and an aviation-specific application of the approach described by Haass et al. (2018), this paper provides a framework for addressing maritime cybersecurity challenges in a systematic fashion, rather than on an isolated and *ad hoc* system-by-system or protocol-by-protocol basis (Mansouri, Gorod, Wakeman, & Sauser, 2009). Where possible, a system will be isolated and reflected in the decision tree taxonomy. Dependencies and shared assumptions can be expressed with a language useful for the many constituents within the maritime environment. Through the application of this framework, many cybersecurity issues can be addressed, including communication challenges that will be particularly important as unmanned and autonomous systems are incorporated into the shared maritime space (MarEx, 2018; Ridden, 2018).

2 THE MARITIME SYSTEM

The importance of the maritime transportation system (MTS) to the global and national economy cannot be over-stated. Globally, roughly 94,000 ships, with an asset value of nearly $1.5 trillion, transport more than $19 trillion of cargo each year, with an annual trade value increase of about 3% (Barki & Délèze-Black, 2017).

In the U.S. alone, 53% of imports and 38% of exports are by ship, and maritime represents the largest import/export transportation modality. Furthermore, the U.S. has been the largest importer and second largest exporter of containerized cargo for most of the last decade (World Shipping Council, n.d.). Maritime cargo contributes at least $649 billion annually to the U.S. gross domestic product and supports more than 13 million jobs. The U.S. MTS also includes 25,000 miles of navigable channels, more than 360 ports, at least 3700 marine terminals, and more than 12 million recreational boats (DOT, n.d.).

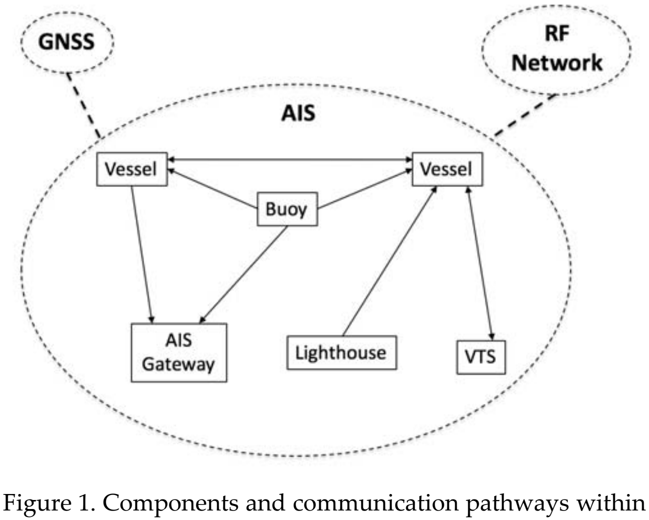


Figure 1. Components and communication pathways within the AIS system, and dependencies upon the Global Navigation Satellite System and Radio Frequency(RF) Network.

The global maritime system -- including all civilian, commercial, and military ship traffic -- is actually a system of systems. Each system can be described as a set of components and the communication pathways between those components. Of course, one system can also be seen as having dependencies upon other systems as all of the systems intercommunicate (Figure 1).

There are many communications systems used within the MTS including all of the data networking at ports, on board ships, within a shipping line, between supply chain partners, and more. Communications within and between systems are dependent upon protocols whose behavior will be dictated by the specific system. Vulnerability analysis requires recognition of the uniqueness of each system and application, and needs to include the examination of all types of disruption ranging from weather to hostile actions; this is known as the *all-hazards approach*. This categorization distinguishes between vulnerabilities that impact only cyber systems (e.g., data, information, and communication) from those that include cyber-physical threats (e.g., control, navigation, or other systems) (Roberts, 2015; Serpanos, 2018). Indeed, this categorization also allows us to distinguish between vulnerabilities that we can control or mitigate (e.g., attacks by people) and those that we cannot control (e.g., nature, weather, stochastic failure).

An individual ship is itself a complex cyber-physical network node with a large variety of communication systems for crew, passengers, external sources, and internal operations, including:

- Bridge Navigation Systems (e.g., GPS, Electronic Chart Display and Information System [ECDIS], AIS, LRIT)
- External Communication Systems (e.g., satellite communications, FleetBroadband, Internet)
- Mechanical Systems (e.g., main engine, auxiliary engine, steering control, ballast management)
- Ship Monitoring and Security Systems (e.g., closed-circuit television, Ship Security Alert System [SSAS], access control systems, sensors)
- Cargo Handling Systems (e.g., valve remote control systems, level/pressure monitoring systems)
- Other specialized networks (e.g., Combat Command & Control Systems on warships, Entertainment Systems and Point-Of-Sale terminals on passenger vessels; Vessel Management Systems on commercial fishing vessels)

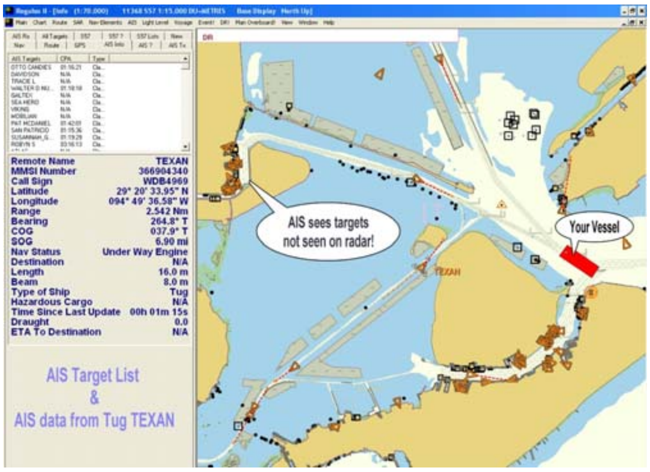
Ship electronics, sensors, and actuators are all integrated within the communication systems listed above. Internet-of-Things (IoT) devices will become increasingly ubiquitous as smart ships and smart ports evolve. The huge amount of information gathered by Vessel Data Recorders (VDR) demonstrate the complexity and number of critical components that a cybersecurity taxonomy must address when considering event logging or cybersecurity incidents.

The proposed framework supports the assignment of types of vulnerabilities, attacks, and exploits with their potential disruptive effects, ranging from critical (e.g., vessel stability and safety) to minor (e.g., reduction in entertainment or service quality). Cyber components include the core software, computing, and network infrastructure of the ship itself, together with additional shipping line-specific software systems. Additionally, GPS, ECDIS, AIS, and other systems include real-time updates while underway, and can include different nodes as the vessel crosses global boundaries.

An adversary can be thought of as another part -- albeit a malicious one -- of the system of systems. An actor is *malicious* if they attempt to modify, subvert, or in any other way cause the cyber or cyber-physical system to behave beyond the limits of its intended operation. For purposes of the remainder of this paper, we will explore AIS in some detail as an example of the application of this analysis.

3 AIS BACKGROUND

The Automatic Identification System is a tracking system that allows a vessel to view local marine traffic (i.e., within 10-20 nautical miles) and to be seen by other nearby ships or AIS equipment installations. AIS was originally designed so that a ship fitted with an appropriate chartplotter could view the local traffic and quickly determine any given ship's name, unique International Maritime Organization (IMO) registration number, size (i.e., length, beam, draft, and gross tonnage), position (latitude and longitude), course, bearing, destination, status (e.g., anchored, docked, underway under power, etc.), and other information (Figure 2). More recently, many Web sites collect and aggregate AIS information and have created a database so that anyone can look up information about any AIS-equipped vessel in near-real-time (Figure 3).

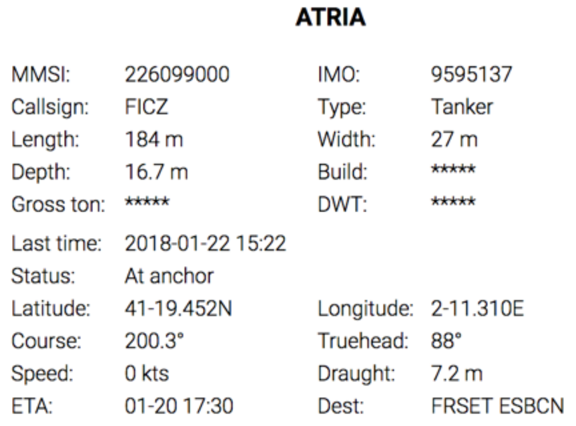


Remote Name	TEXAN
MMSI Number	366904340
Call Sign	WDB4969
Latitude	29° 20' 33.95" N
Longitude	094° 49' 36.58" W
Range	2.542 Nm
Bearing	264.8° T
COG	037.9° T
SOG	6.90 mi
Nav Status	Under Way Engine
Destination	N/A
Length	16.0 m
Beam	8.0 m
Type of Ship	Tug
Hazardous Cargo	N/A
Time Since Last Update	00h 01m 15s
Draught	0.0
ETA To Destination	N/A

Figure 2. Chartplotter display including AIS data, showing ships in the local area (from *https://www.navcen.uscg.gov/images/WhatYouSeeWithAIS.jpg*).

AIS was introduced in the 2002 International Convention for the Safety of Life at Sea (SOLAS). Chapter V of the SOLAS agreement, titled "Safety of Navigation," mandates that ships of a certain size and/or function carry AIS transceivers as an additional safety measure (IMO, 2002). Ships in U.S. waters generally fall under U.S. Coast Guard (USCG) regulations; 33 CFR 164.46 defines AIS requirements, which include all vessels of 1600 or more gross tons, commercial power vessels 65 or more feet (19.8 meters) in length, and a power vessel certified to carry more than 150 passengers; warships are exempted from AIS requirements although all modern warships carry AIS (USCG, 2018).

A key component of AIS is the use of precise positioning technology. AIS does not specify -- nor does it depend upon -- which GNSS is employed; AIS merely broadcasts a position using a feed from the ship's navigation and positioning system. That said, any cybersecurity vulnerabilities in the vessel's GNSS will affect the precision of the AIS transmissions regarding location. GNSS vulnerabilities, particularly those related to GPS, are integral to AIS vulnerabilities but will not be specifically addressed in this paper (except as they affect AIS) (Czaplewski & Goward, 2016).



ATRIA

MMSI:	226099000	IMO:	9595137
Callsign:	FICZ	Type:	Tanker
Length:	184 m	Width:	27 m
Depth:	16.7 m	Build:	*****
Gross ton:	*****	DWT:	*****
Last time:	2018-01-22 15:22		
Status:	At anchor		
Latitude:	41-19.452N	Longitude:	2-11.310E
Course:	200.3°	Truehead:	88°
Speed:	0 kts	Draught:	7.2 m
ETA:	01-20 17:30	Dest:	FRSET ESBCN

Figure 3. AIS information from a Web aggregator (screen shot from *http://www.findship.co*).

AIS communications protocols are described in International Telecommunication Union Radiocommunication sector (ITU-R) Recommendations M.585-7 and M.1371-5 (ITU, 2014, 2015). AIS employs a shared radio-communication channel using a form of time-division multiple access (TDMA). Time on the radio channel is divided into 2,250 slots per minute so that each slot has a duration of 26.67 milliseconds. The protocol defines how AIS stations stay in synchronization so that they do not overlap their transmissions and advertise when they will be transmitting next. New AIS stations, such as those on a ship coming within radio range close to other ships, can also be added to the lineup of transmitters on the channel (Wikipedia, 2018).

SOLAS-compliant Class A AIS transponders employ a Self-Organizing TDMA (SOTDMA) broadcast mode, transmitting information every 2 to 10 seconds while underway[1] and every three minutes while at anchor; these transponders can also transmit and receive safety-related text messages. Less expensive Class B AIS transponders employ a Carrier-Sense TDMA (CSTDMA) broadcast mode, transmitting dynamic information (e.g., position, course, and speed) every 30-180 seconds, static data (e.g., vessel name and IMO number) every six

[1] The rate of transmission is dependent upon the ship's speed and whether they are changing course or not; faster and/or maneuvering vessels transmit more frequently than slower vessels that are on a steady course.

minutes, and, optionally, safety-related text messages (Shine Micro, n.d.; Wikipedia, 2018).

AIS messages are formatted according to the National Marine Electronics Association (NMEA) 0183 serial communications protocol standard and are referred to as *sentences*. The two common AIS sentences are !AIVDM (data received from other vessels) and !AIVDO (vessel's transmitted information). There are just over two dozen AIS message types. At a data rate of 9600 bits/sec, messages are limited to 256 bits of information per time slot. AIS employs maritime very high frequency (VHF) channels 87B (161.975 MHz) and 88B (162.025 MHz) (Raymond, 2016; Wikipedia, 2018.

4 SECURITY CONCERNS

AIS improves vessel traffic management and safety through increased situational awareness. AIS messages, however, are transmitted in plaintext, which introduces a potential security risk since these unencrypted AIS messages can be read by anyone with a receiver. Add to this the Web sites with instructions for building AIS receivers using inexpensive hardware[2] and open source software[3], and it is clear that AIS is vulnerable to a variety of exploits.

Attacks on AIS, and information in general, can affect the information's confidentiality, integrity, and availability (the so-called *CIA Triad*) as well as three other characteristics, namely, possession, authenticity, and utility; these six together are sometimes called the *Parkerian Hexad* (Parker, 2015):

– *Confidentiality* refers to protecting information from unauthorized access or disclosure.
– *Integrity* refers to the state of information being free from inadvertent or deliberate manipulation.
– *Availability* refers to the users' ability to access information when needed.
– *Possession* (or *control*) refers to the loss of data by the authorized user (even if the "thief" cannot access the data).
– *Authenticity* (aka *authentication*) refers to being able to prove the identity of the sender of information.
– *Utility* refers to the usefulness of the data to the user (e.g., possessing encrypted data without a decryption key or receiving a message to do something after the date when the action is required are examples of low utility)

Plaintext messages have long been a security vulnerability in the storage of data on computers and transmission of data on networks. Various types of protections have been implemented in order to protect information and information systems from attacks on all elements of the Parkerian hexad. Cryptography plays a particularly key role in protecting the confidentiality, integrity, and authenticity of information. In its most simple form, the process of creating encrypted ciphertext requires the original unencrypted plaintext message, an encryption algorithm, and a key (or, sometimes, two keys). Secret key cryptographic protocols protect data confidentiality because ciphertext is unreadable as long as the key required to decrypt the message remains secret. One-way cryptographic hashes are used to verify the integrity of a message, using a mathematical algorithm that provides a digital fingerprint of the message; changing even one bit in a message will cause the hash value to change, indicating that the content of the message has changed. Message authentication codes (MAC) use a shared secret key and can be used to verify the integrity of a message, as well as providing authentication, verifying the identity of the message sender. Authentication can also be provided using public key cryptographic methods (Kessler, 2018).

The AIS protocols provide no internal mechanism for message integrity and encryption. While some AIS products have the ability to transmit and receive using an encryption mode, the methods are proprietary and are designed to allow a "fleet" of ships to see each other but not be seen outside of the encrypted group. Indeed, the U.S. Coast Guard has described Encrypted AIS (EAIS) for military and law enforcement purposes, although products implementing that specification are not generally available to civilian classes of vessels (USCG, 2014).

AIS was designed to assist vessels in situational awareness by providing them knowledge of maritime traffic beyond their ability to visualize it and beyond the capability of traditional radar. By the nature of AIS broadcasts, then, a lot of information can be received by anyone who just wants to know what is going on in their proximity, which might include individuals with nefarious intent such as pirates, terrorists, or other criminal actors. But this level of *information leakage* is nothing compared to aggregation sites that broadcast on the Web the location of thousands of ships around the globe, such as FindShip, MarineTraffic, VesselFinder, Vesseltracker, and many more. The IMO Maritime Safety Committee warned about the dangers of this information leakage as far back as 2004, noting that "the publication on the world-wide web... of AIS data transmitted by ships could be detrimental to the safety and security of ships and port facilities and was undermining the efforts of the Organization and its Member States to enhance the safety of navigation and security in the international maritime transport sector" (IMO, 2018, para. 1).

5 THREAT ASSESSMENTS

There are a variety of approaches to examining the security threat landscape in any system. We will examine several here and apply them to AIS. Figure 4 provides a graphical overview of AIS components, communication pathways, and threat vectors. In this description, each component -- including bad actors -- is shown along with communication links composed of valid messages, software-based threats, and radio frequency-based threats. This is a similar approach taken by graph theory, by identifying the communicating elements and the communication

[2] E.g., https://www.partmarine.com/blog/wireless_ais_howto
[3] E.g., https://opencpn.org

links (Boukhtouta, Mouheb, Debbabi, Alfandi, Iqbal, & El Barachi, 2015).

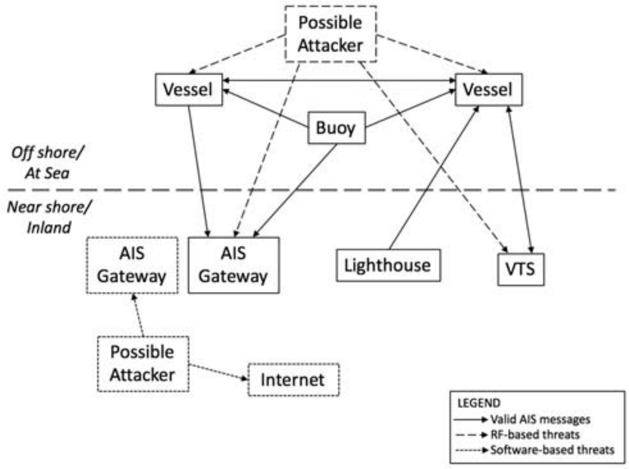


Figure 4. AIS components, communication pathways, and attack vectors (modified from Balduzzi, Wilhoit, & Pasta, 2014)

As mentioned earlier in the paper, there are lessons that the various transportation sectors can learn from each other in terms of cybersecurity. A great deal of work has gone into studying security vulnerabilities of Automatic Dependent Surveillance-Broadcast (ADS-B), a system for providing aircraft in flight with the same situational awareness as AIS provides ships at sea. It has been instructive to see how some of the ADS-B security literature applies to the maritime domain.

Based upon a threat assessment model for ADS-B described by Gauthier and Seker (2018), we can identify three primary types of intentional, human-initiated cyberattacks on AIS:

- Disruption of GPS[4] signals
- Jamming of the wireless communications
- Manipulation of AIS transmissions

This perspective is very much in line with the system of systems approach; each of the three main categories actually represents a different system that must be secured in order to secure AIS; namely, GNSS or other positioning systems, radiocommunication propagation paths, and AIS transceivers. We can further subdivide the AIS category above into:

- Message injection (spoofing)
- Message deletion (denial-of- service)
- Message modification (alteration of message contents (data diddling)

Strohmeier et al. (2015) identified five primary threat categories to ADS-B that can also apply to AIS; the first is a passive attack and the remaining are active attacks:

- *Eavesdropping* is a simple, passive attack that can be easily accomplished since AIS is, by definition, a broadcast radio system. Furthermore, messages are generally transmitted in an unencrypted state.
- *Jamming* can occur at both the ground station level or at the vessel level, and can include an attack accomplished by jamming radio signals or a denial-of-service attack making AIS transmission slots unavailable.
- *Message injection* involves inserting spurious messages into the vessel traffic communication system. This is possible because AIS messages are unencrypted and the source of the message is not authenticated.
- *Message deletion* is accomplished through destructive or constructive interference, the latter of which is accomplished by producing a significant number of bit errors in the message, causing the receiving party to drop the message due to data corruption.
- *Message modification* is initiated by altering a message's bit stream, generally by bit-flipping (i.e., changing a 0 to a 1 or a 1 to a 0) or overshadowing (i.e., using a high-power transmission source to overwrite part of, or an entire, target message).

In an effort to apply these two approaches, plus the Parkerian Hexad described earlier, we need to identify some specific potential information security vulnerabilities in AIS. Combining attack descriptions from a variety of sources (including Balduzzi et al., 2014; Gauthier & Seker, 2018; Purton, Abbass, & Alam, 2010; and Strohmeier, Lenders, & Martinovic, 2015), we can identify the following cyber threats to AIS:

1 GPS signal jamming
2 GPS device failure or poor quality transmissions
3 AIS device powered down
4 AIS device malfunction
5 AIS programming error
6 AIS radio channel jamming
7 AIS radio transmission bit errors
8 AIS vessel spoofing
9 AIS traffic eavesdropping
10 AIS system flooding
11 Ghost vessel
12 Closest Point-of-Approach/AIS Search-and-Rescue Transponder (CPA/AIS-SART) spoofing
13 Vessel disappearance
14 Aids-to-Navigation (AtoN) spoofing
15 Data diddling
16 Weather forecast spoofing

Table 1 summarizes these cyber threats to AIS and classifies them according to the Parkerian Hexad vulnerability, and using the systems approach and categories described above.

Table 1 suggests that while the Parkerian Hexad provides a useful way to generally categorize the impact of vulnerabilities, it is not useful in describing specific threat vectors and vulnerabilities in given cyber systems. This said, this table does seem to suggest that there are more threats to integrity and authenticity than to availability, which is not surprising given the lack of integrity and authentication checks in AIS. We also see that models that focus only on human-initiated attacks are not sufficient to describe the suite of threats to information within a given system.

[4] Any references to *GPS* also applies to any GNSS.

Table 1. AIS Cyber Risk Summary Using Descriptors from the Parkerian Hexad (Parker, 2015), Systems Approach (Gauthier & Seker, 2018), and Threat Category Approach (Strohmeier et al., 2015).

Attack	Parkerian Hexad	Systems	Threat Category
GPS jamming	Availability	GPS/Jamming	Jamming
GPS failure/poor transmission	Availability	GPS	(nature, installation)
AIS device off	Availability	(human error)	(human error)
AIS malfunction	Availability	(nature)	(nature)
AIS bad data	Integrity, Availability, Utility	(human error)	(human error)
AIS jamming	Availability	Jamming	Jamming
AIS bit errors	Availability	(nature)	(nature)
Vessel spoofing	Integrity, Authenticity	Msg. injection	Msg. injection
Eavesdropping	Confidentiality, Authenticity	n/a	Eavesdropping
Flooding	Availability	Msg. injection	Msg. injection
Ghost vessel	Integrity, Authenticity, Utility	Msg. injection	Msg. injection
CPA/AIS-SART spoofing	Integrity, Authenticity, Utility	Msg. injection	Msg. injection
Disappearance	Integrity, Availability	Msg. deletion	Msg. deletion
AtoN spoofing	Integrity, Authenticity, Utility	Msg. injection	Msg. injection
Data diddling	Integrity, Availability, Authenticity, Utility	Msg. modification	Msg. modification
Weather spoofing	Integrity, Authenticity, Utility	Msg. injection	Msg. injection

Table 1 also suggests that while the "systems of systems" method is an inviting approach to understanding the vulnerabilities in the system in question -- here, AIS -- it does not necessarily help in the defense of that system. In particular, an AIS device vendor or software designer must be aware of AIS dependencies on GPS and radio frequency (RF) vulnerabilities but, in fact, cannot do anything to control them. As an example, AIS will fail if someone turns off the GPS receiver yet no AIS protections can defend against that eventuality. Indeed, if we were to analyze every GPS and radio transmission vulnerability in order to understand AIS, we would have to consider additional systems' vulnerabilities as they might impact GPS and radio. Ultimately, someone designing AIS equipment has to be aware of the dependency on GPS, for example, and may even put in some mechanisms to test the integrity of the GPS feed, but cannot protect AIS from all of the problems that GPS might have.

6 RISK ASSESSMENT AND MANAGEMENT

The threats identified above include intentional attacks from human bad actors as well as errors due to natural causes. In order to prepare appropriate risk management plans, a proper risk assessment must be performed. Common risk management analysis for information systems includes accounting for natural threats or hazards (e.g., hurricanes, floods, and blizzards) as well as equipment failure. This all-hazards approach speaks to the fact that a natural disaster is as devastating as a deliberate attack but, from the perspective of initial response, all that matters is the immediate impact of an event rather than the actual attack vector.

Identifying vulnerabilities is only the first step in building a cyber defense and understanding the true potential impact of these vulnerabilities. Not all vulnerabilities are equally exploitable or likely; therefore, a risk assessment must be conducted on each vulnerability so that one can determine how to manage these risks. Unless clear quantitative measures are available, a qualitative approach is commonly employed to describe such characteristics as a vulnerability's likelihood of exploit, severity should the exploit be realized, ease of attack, and whether it is a human-initiated attack (including human error) or a natural hazard (Table 2). Note that these categorizations are relative to the AIS system rather than the vessel itself; i.e., a vulnerability that is critical to AIS is bad news for the ship but, by itself, not critical to its operation.

Table 2. Risk Management Approach.

Attack	Source	Likelihood	Severity	Ease
GPS jamming	A	4	2	3
GPS failure/poor transmission	H	3	3	n/a
AIS device off	A	4	1	1
AIS malfunction	H	5	1	n/a
AIS bad data	A	3	3	1
AIS jamming	A	5	2	3
AIS bit errors	H	3	3	n/a
Vessel spoofing	A	4	2	2
Eavesdropping	A	1	4	1
Flooding	A	4	3	3
Ghost vessel	A	4	3	3
CPA/AIS-SART spoofing	A	5	2	3
Disappearance	A	4	2	3
AtoN spoofing	A	4	2	3
Data diddling	A	3	2	3
Weather spoofing	A	4	3	3

Source: A = human-initiated attack, H = natural hazard
Likelihood: 1 = Frequent, 2 = Probable, 3 = Occasional, 4 = Remote, 5 = Unlikely
Severity: 1 = Catastrophic, 2 = Critical, 3 = Marginal, 4 = Negligible
Ease of attack: 1 = Trivial, 2 = Simple, 3 = Difficult, 4 = Very difficult

There are a number of conclusions that can be drawn from Table 2. First, while there are more potential intentional threats than natural hazards, they tend to have about the same likelihood (hazards: μ=3.67, σ=1.15; intentional threats: μ=3.77, σ=1.01). Second, the most vulnerable attack vectors on AIS are those where data can be inserted into the system; many of these attacks can be realized in software-generated transmissions rather than by attacking the radio frequencies themselves. Third, the most severe attack on AIS is when the AIS receiver is off; at that point, a vessel is driving blind with respect to AIS information. Fourth, the most significant vulnerabilities in AIS affect individual AIS messages rather than the entire AIS system itself. Finally, most of the intentional threats result directly from the fact that AIS messages are neither encrypted nor authenticated, coupled with the lack of integrity checking and bit-error correction mechanisms.

Finally, ease of attack is, in some sense, the most difficult to quantify because the feasibility of an attack often depends upon the adversary. An attack that is beyond the means of a "pedestrian" hacker might be well within the cyberattack toolkit of a nation-state. In any case, this table seems to suggest that none of the identified vulnerabilities in AIS are "very difficult" to exploit.

7 FUTURE RESEARCH

Understanding the vulnerabilities of AIS provides a number of ideas about where to shore up the system. There are a variety of directions that might lead to added security in AIS; some of these ideas are borrowed from the aviation industry. Consider:

– Some form of physical (radio transmission) layer authentication. This methodology varies in its difficulty, cost, and scalability, and would require additional AIS software and/or hardware, but would not change the AIS protocol itself (Strohmeier et al., 2015).
– Use of Kalman filtering or other techniques to track relative signal strength of individual ship transmissions in order to detect possible spoofing of that ship by an attacker. The cost and difficulty for such an approach would be low although scalability might be difficult. As above, no new AIS messages would be required (Strohmeier et al., 2015).
– Encrypted AIS (EAIS) has already been proposed (USCG, 2014) and some variants are in limited use for special-purpose fleets. EAIS, however, has limited utility for any vessel outside of the "trusted" group. Using some form of lightweight public-key infrastructure (PKI) for AIS communication security, not terribly unlike the use of certificates in the Secure Sockets Layer (SSL) already in widespread use on the Web, could prevent certain types of attacks, such as man-in-the-middle spoofing. The downside to this approach is the high degree-of-difficulty to design and implement, and likely high cost to deploy widely (Strohmeier et al., 2015).
– An AIS position message contains a ship's latitude, longitude, course (bearing), rate and direction of turn, and speed. The rate at which these messages are transmitted is based upon the vessel's speed and whether it is maneuvering; in any case, a ship will change position by no more than about 230 feet (69 meters) between sequential reports. It should be relatively simple, therefore, for a receiver to predict the sender's approximate location at the next transmission. Predictive AIS has been described by a number of sources as a way to use historic AIS information to predict the path of other vessels (Hexeberg, Flåten, Eriksen, & Brekke, 2017; Last, Bahlke, Hering-Bertram, & Linsen, 2014; Mazzarella, Arguedas, & Vespe, 2015), and these methods are already used for research and practice for additional collision avoidance techniques and better understanding of traffic patterns. But if a station stores the position at just the last transmission, it can predict a range where the sender should be at the next transmission. If the next announced position, or any of the associated message parameters, vary greatly from the prediction, that could indicate an integrity problem. This type of capability would require additional software, but would be relatively simple and inexpensive to deploy, and could be a simple add-on to existing equipment without requiring any change to the AIS protocol.

8 CONCLUSIONS

We have all become more and more dependent upon technology. Many younger mariners do not recall a day at sea without radar, GPS, AIS, ECDIS, and the other myriad data, communication, and navigation systems aboard today's large ships. Indeed, the U.S. Navy stopped teaching celestial navigation in 1996 due to the prevalence of GPS; they brought it back 20 years later most likely due to the susceptibility of cyber threats against GPS (Hrala, 2016). Hardware engineers, software developers, protocol designers, and researchers must maintain awareness of the potential cyber threats and vulnerabilities in all systems that they build and this security awareness must be built-in from the beginning of a project. The framework and taxonomy proposed here are small steps that demonstrate that these methods can be employed throughout the transportation sector and, presumably, applied to other critical infrastructures.

The model described here focuses on identifying vulnerabilities in our systems rather than identifying threat actors. A well-known cybersecurity maxim states, "If you know the vulnerabilities (weaknesses), you've got a shot at understanding the threats (the probability that the weaknesses will be exploited, how, and by whom)... But if you focus only on the threats, you're likely to be in trouble" (Johnston, 2018, p. 10). The object lesson is that if you concentrate on who is trying to attack you, you will mostly likely get it wrong because it is hard to correctly predict threats and, in any case, as suggested above, threats are beyond your control. Vulnerabilities, on the other hand, are easier to identify, particularly if you think like an attacker.

In terms of the improved situational awareness promised by AIS, it is important to realize that while loss of AIS decreases safety in the immediate area, there are many other mechanisms to compensate for its loss, such as radar, radio, increased human lookouts, etc. AIS, then, is an important part of vessel safety but its absence does not cause safety at sea to fall apart. The potential devastating impact of AIS vulnerabilities would come about if attackers relentlessly exploited the lack of integrity and authentication checking, and bombarded the system with enough bogus messages so as to threaten the very veracity of the system. Indeed, in this latter case, AIS could be viewed as doing more harm than good, and if only a tiny fraction of AIS messages are fake, users will lose confidence in the entire system.

REFERENCES

Balduzzi, M., Wilhoit, K., & Pasta, A. (2014, December). *A Security Evaluation of AIS*. Trend Micro Research Paper. Retrieved from https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-security-evaluation-of-ais.pdf

Barki, D., & Déléze-Black, L. (Eds.) (2017). *Review of Maritime Transport 2017*. United Nations Conference On Trade And Development, UNCTAD/RMT/2017. New York: United Nations. Retrieved from http://unctad.org/en/PublicationsLibrary/rmt2017_en.pdf

Boukhtouta, A., Mouheb, D., Debbabi, M., Alfandi, O., Iqbal, F., & El Barachi, M. (2015). Graph-theoretic characterization of cyber-threat infrastructures. *Digital Investigation, 14*, S3-S15. Retrieved from https://www.dfrws.org/sites/default/files/session-files/paper-graph-theoretic_characterization_ of_cyber-threat_infrastructures.pdf

Czaplewski, K., & Goward, D. (2016, June). Global Navigation Satellite Systems – Perspectives on Development and Threats to System Operation. *TransNav, The International Journal on Marine Navigation and Safety of Sea Transportation*, *10*(2), 183-192. https://doi.org/10.12716 /1001.10.02.01

Gauthier, R., & Seker, R. (2018, January). Addressing Operator Privacy in Automatic Dependent Surveillance - Broadcast (ADS-B). In *Proceedings of the 51st Hawaii International Conference on System Sciences (HICSS)*, Waikoloa Village, HI, USA, pp. 52-61.

Haass, J., Craiger, J.P., & Kessler, G.C. (2018). A Framework and Taxonomy for Aviation Cybersecurity. In *Proceedings of the 2018 IEEE National Aerospace & Electronics Conference (NAECON) 2018*, July 23-26, 2018, Dayton, Ohio. Los Alamitos (CA): IEEE Press.

Haass, J.C., Sampigethaya, K., & Capezzuto, V. (2016, July). Aviation Cybersecurity: Opportunities for Applied Research. *Transportation Research Board TR News Magazine, (304)*39-43.

Hexeberg, S., Flåten, A.L., Eriksen, B.H., & Brekke, E.F. (2017). AIS-Based Vessel Trajectory Prediction. In *Proceedings of the 2017 20th International Conference on Information Fusion (Fusion)*, Xi'an, pp. 1-8. https://doi.org/10.23919/ICIF.2017.8009762

Hrala, J. (2016, February 12). The Scary, Practical Reason The US Navy Is Once Again Teaching Celestial Navigation. *Science Alert* Web site. Retrieved from https://www.sciencealert.com/the-scary-practical-reason-the-navy-is-once-again-teaching-celestial-navigation

International Maritime Organization (IMO). (2002, July 1). *International Convention for the Safety of Life at Sea (SOLAS)*, Chapter V (Safety of Navigation), Regulation 19 (Carriage requirements for shipborne navigational systems and equipment). Retrieved from https://mcanet.mcga.gov.uk /public/c4/solas/index.html

International Maritime Organization (IMO). (2018). Maritime Security - AIS Ship Data. *AIS Transponders* Web page. Retrieved from http://www.imo.org/en/OurWork/Safety/Navigation/Pages/AIS.aspx

International Telecommunication Union (ITU). (2014, February). *Technical Characteristics for an Automatic Identification System Using Time Division Multiple Access in the VHF Maritime Mobile Frequency Band*. M-Series: Mobile, radiodetermination, Amateur and Related Satellite Services. ITU-R Recommendation M.1371-5. Retrieved from https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.1371-5-201402-I!!PDF-E.pdf

International Telecommunication Union (ITU). (2015, March). *Assignment and Use of Identities in the Maritime Mobile Service*. M-Series: Mobile, radiodetermination, Amateur and Related Satellite Services. ITU-R Recommendation M.585-7. Retrieved from https://www.itu.int /dms_pubrec/itu-r/rec/m/R-REC-M.585-7-201503-I!!PDF-E.pdf

Johnston, R.G. (2018, August). Vulnerabilities Trump Threats Maxim. *Security Maxims*. Right Brain Sekurity. Retrieved from http://rbsekurity.com/Papers/security maxims with axe.pdf

Kessler, G.C. (2018, August 11). An Overview of Cryptography. Retrieved from https://www.garykessler.net/library/crypto.html

Kessler, G.C. (In press, expected 2019, Spring). Cybersecurity in the Maritime Domain. *Proceedings of the USCG Marine Safety & Security Council*.

Last, P., Bahlke, C., Hering-Bertram, M., & Linsen, L. (2014, September). Comprehensive Analysis of Automatic Identification System (AIS) Data in Regard to Vessel Movement Prediction. *The Journal of Navigation*, *67*(5), 791-809. https://doi.org/10.1017/S0373463314000253

Mansouri, M., Gorod, A., Wakeman, T.H., & Sauser, B. (2009). A Systems Approach to Governance in Maritime Transportation System of Systems. *Proceedings of the IEEE International Conference on System of Systems Engineering (SoSE)*. Albuquerque, NM.

MarEx. (2018, April 3). Kongsberg and Wilhelmsen Launch Autonomous-Shipping JV. *The Maritime Executive*. Retrieved from https://www.maritime-executive.com/article/kongsberg-and-wilhelmsen-launch-autonomous-shipping-jv

Mazzarella, F., Arguedas, V.F., & Vespe, M. (2015). Knowledge-Based Vessel Position Prediction Using Historical AIS Data. In *Proceedings of 2015 Sensor Data Fusion: Trends, Solutions, Applications (SDF)*, Bonn, 2015, pp. 1-6. https://doi.org/10.1109/SDF.2015.7347707

Parker, D.B. (2015). Toward a New Framework for Information Security? In S. Bosworth, M.E. Kabay, & E. Whyne (Eds.), *Computer Security Handbook*, 6th ed. (pp 3.1-3.23). Hoboken, NJ: John Wiley & Sons, Inc.

Purton, L., Abbass, H., & Alam, S. (2010). Identification of ADS-B System Vulnerabilities and Threats. In *Proceedings of the Australasian Transport Research Forum 2010*, 29 September - 1 October 2010, Canberra, Australia.

Raymond, E.S. (2016, August). AIVDM/AIVDO Protocol Decoding. Version 1.52. Retrieved from http://catb.org/gpsd/AIVDM.html

Ridden, P. (2018, September 4). Unmanned Surface Vessel Successfully Crosses Atlantic. *New Atlas* Web site. Retrieved from https://newatlas.com/offshore-sensing-sailbuoy-met-atlantic/56204/

Roberts, F.S. (2015, January). Vulnerabilities of Cyber-Physical Systems: From Football to Oil Rigs. Retrieved from http://www.dimacs.rutgers.edu/People/Staff/froberts/CyberPhysicalSystemsFootballOilRigs1-3-15.pptx.pdf

Serpanos, D. (2018, March). The Cyber-Physical Systems Revolution. *Computer*, *51*(3), 70-73.

Shine Micro. (n.d.). AIS Overview. Retrieved from https://www.shinemicro.com/ais-overview/

Strohmeier, M., Lenders, V., & Martinovic, I. (2015). On the Security of the Automatic Dependent Surveillance-Broadcast Protocol. *IEEE Communications Surveys & Tutorials*, *17*(2), 1066-1087.

U.S. Coast Guard (USCG). (2014, June 4). *Encrypted Automatic Identification System (EAIS) Interface Design Description (IDD)*. Command, Control, and Communications Engineering Center (C3Cen).Retrieved from https://epic.org/foia/dhs/uscg/nais/EPIC-15-05-29-USCG-FOIA-20151030-Production-2.pdf

U.S. Coast Guard (USCG). (2018, July 24). AIS Requirements. USCG Navigation Center Web site. Retrieved from https://www.navcen.uscg.gov/?pageName=AISRequirementsRev

U.S. Department of Transportation (DOT). (n.d.). Marine Transportation System (MTS). Maritime Administration (MARAD) Web site. Retrieved from https://www.marad.dot.gov/ports/marine-transportation-system-mts/

Wikipedia. (2018, July 17). Automatic Identification System. Retrieved from https://en.wikipedia.org /wiki/Automatic_identification_system

World Shipping Council. (n.d.). Trade Statistics. Retrieved from http://www.worldshipping.org/about-the-industry/global-trade/trade-statistics