From Click To Sink: utilizing AIS for command and control in maritime cyber attacks

Ahmed Amro[0000−0002−3390−0772] and Vasileios Gkioulos

Norwegian University of Science and Technology, Gjøvik, Norway
ahmed.amro@ntnu.no and vasileios.gkioulos@ntnu.no

Abstract. The maritime domain is among the critical sectors of our way of life. It is undergoing a major digital transformation introducing changes to its operations and technology. The International Maritime Organization urged the maritime community to introduce cyber risk management into their systems. This includes the continuous identification and analysis of the threat landscape. This paper investigates a novel threat against the maritime infrastructure that utilizes a prominent maritime system that is the Automatic Identification System (AIS) for establishing covert channels. We provide empirical evidence regarding its feasibility and applicability to existing and future maritime systems as well as discuss mitigation measures against it. Additionally, we demonstrate the utility of the covert channels by introducing two realistic cyber attacks against an Autonomous Passenger Ship (APS) emulated in a testing environment. Our findings confirm that AIS can be utilized for establishing covert channels for communicating Command & Control (C&C) messages and transferring small files for updating the cyber arsenal without internet access. Also, the establishment and utilization of the covert channels have been found to be possible using existing attack vectors and technologies related to a wide range of maritime systems. We hope that our findings further motivate the maritime community to increase their efforts for integrating cyber security practices into their systems.

Keywords: maritime · cybersecurity · Automatic Identification System (AIS) · cover channel · *ATT&CK*

1 Introduction

We live in a highly connected world that depends on various means of transportation for the delivery of goods, services, and the transportation of people all around the globe. Thus, the transportation sector is regarded internationally as a critical infrastructure. In the European Union, five modes of transport have been recognized: air, road, rail, maritime, and inland waterways [4]. Among these sectors, this paper targets the maritime domain. The maritime domain is linked to the well-being, prosperity, and security of the citizens of Europe [1]. It is also involved in 90% of the global trade of goods [3] making it a domain worthy of increased attention in the research community.

Maritime systems include a variety of cyber systems including Information Technology (IT) and Operational Technology (OT) which are distributed across port facilities, ships, and other components within the maritime infrastructure. These systems are applied in specific applications in navigation, propulsion and steering, cargo handling, and others. These applications rely on a group of maritime-specific systems such as the Automatic Identification System (AIS), and the Electronic Chart Display and Information System (ECDIS). Additionally, such systems rely on maritime-specific protocols and standards including among others, the National Marine Electronics Association (NMEA) standard, and the AIS protocol. NMEA standard is utilized in the communication between marine systems including the communication of sensor data through message-based protocol [49]. AIS is a special message-based protocol based on the NMEA standard which is utilized in many maritime services including; among others, traffic management, search and rescue, and collision avoidance [41].

Disruptive attacks against the maritime domain can have devastating effects as witnessed in the cyber attack against Mærsk shipping company, which lead to weeks of interrupted operations and losses beyond 300 million US dollars [36]. Also, insufficient security in the maritime systems and protocols has been demonstrated in the literature. To mention a few examples, Balduzzi et al [25] have demonstrated a wide range of attacks against AIS including spoofing, jamming, and other sorts of misuse while Tran et al [60] discussed the limited authentication, encryption, and validation in one of the NMEA protocols. Positively, there are demands for the consideration of cyber threats and cyber risk management in the current state of affairs in the maritime domain. The International Maritime Organization (IMO) has adopted Resolution MSC.428(98) [32] encouraging the maritime industry stakeholders to include cyber risk management into their safety management systems. The resolution provides guidelines and requirements for cyber risk management [31]. The guidelines suggest the continuous analysis and assessment of the threat landscape against the maritime infrastructure.

In this direction, this paper investigates attacks in the maritime industry in order to identify novel attacks that can surface into reality in the future. We have identified a limitation in the literature when discussing Command and Control (C&C) activities. Then, we investigate the utility of the Automatic Identification System (AIS) as a covert channel for conducting C&C activities during the development of cyber attacks against maritime infrastructure. In our investigation, we initially developed a threat model of the covert channel focusing on the threat requirements, scope, objectives, and techniques. Afterward, we developed and evaluated a proof of concept of the covert channel. Moreover, we demonstrated the utility and application of the covert channel in two realistic attack scenarios against a modern maritime use case which is an Autonomous Passenger Ship (APS). We aspire to motivate the maritime community to further adopt cybersecurity into their operations and system development practices.

2 Background and Related Work

2.1 Autonomous Passenger Ship

This paper is part of an ongoing research project titled "Autoferry"[50]. The project targets the development of an APS prototype which is named milliAmpere2; an autonomous ferry with the capacity to carry 12 passengers and their luggage across the Trondheim city canal as an alternative for a high-cost bridge [38]. MilliAmpere2 is designed to be fully autonomous with the ability to be supervised and controlled from a Remote Control Center (RCC). The ferry includes an Autonomous Navigation System (ANS) which utilizes data from various sensors for establishing situational awareness and safe navigation. The sensors include lidar, radar, Automatic Identification System (AIS), Global Positioning System (GPS), and others. The ANS forwards sensor data to a Remote Navigation System (RNS) at the RCC through a ship-shore communication link. More details can be found in our earlier article [22]. In this paper, we utilize this APS as a use case for demonstrating two cyber kill chains (i.e attack scenarios) to showcase the application and utility of the discussed covert channel.

2.2 ATT&CK Framework

Recently, wide adoption is observed for the Adversarial Tactics, Techniques, and Common Knowledge from MITRE, shortly known as the *ATT&CK* framework [57]. *ATT&CK* captures adversarial behavior in enterprise environments, industrial control systems, and other technology domains making it suitable for modeling cyber attacks in a wide range of use cases. The European Union Agency for Cybersecurity (ENISA) utilizes *ATT&CK* terminologies for mapping adversarial activities in their annual threat landscape report [11]. Also, Security Incidents and Event Management (SIEM) systems utilize *ATT&CK* terminologies for detecting adversarial activities [2, 10].

The recent adoption of *ATT&CK* as a threat model is observed for modeling threats against maritime systems. Kovanen et al [45] utilized *ATT&CK* for mapping threat actors' objectives to a remote pilotage system for improved risk assessment and design. Also, Jo et al [43] proposed a cyber attack analysis method based on *ATT&CK*. The authors described four documented cyber attacks in the maritime domain using *ATT&CK* tactics and techniques. Moreover, in our earlier work [23] we utilized *ATT&CK* as a threat model for describing attacks against navigational functions. In this paper, we will also utilize *ATT&CK* for modeling cyber attacks and provide a proof of concept of some of the *ATT&CK* techniques in common maritime systems.

The *ATT&CK* threat model provides useful terminologies for describing the different elements of threats. In this paper, we rely heavily on both, namely tactics and techniques. Tactics describe the adversarial objectives also referred to as stages of cyber attacks. Techniques on the other hand describe the adversarial method for realizing an objective [57].

2.3 Maritime Kill Chains, Threats and Attacks

In this paper we investigate and aim to answer the following question; what are the adversarial tactics (i.e. objectives) and techniques that are discussed in the literature in the maritime domain and do they cover the current threat landscape. In our research, we rely on the *ATT&CK* framework due to its comprehensive threat model and increased adoption as a new standard for adversarial tactics, techniques, and procedures. We have conducted a comprehensive literature review to identify relevant works that have discussed adversarial techniques across the different stages of cyber attacks (i.e. tactics). This allows for a clearer understanding of the current threat landscape in the maritime domain.

Starting with the reconnaissance stage, Enoch et al [33] briefly discussed the utility of OpenVAS and NMAP for conducting reconnaissance-related activities in a vessel system. Also, Standard et al [54] discussed the teaching of network reconnaissance for naval officers during a cybersecurity course for capacity development. Additionally, Lund et al [47] mentioned that activities at the reconnaissance stage were conducted through physical access to the vessel and access to the network, and ECDIS software. Moreover, Amro [20] has demonstrated the utility of AIS and NMEA communicated messages for gaining both cyber and physical attributes of possible maritime targets.

For gaining access to maritime components and networks; also known as attack delivery, Lund et al [47] discussed the utilization of a USB flash drive to deliver a malicious payload into the ECDIS machine and execute it. Also, Papastergiou et al [51] referred to the possibility of gaining access to maritime infrastructure through compromising the supply chain. Additionally, Pavur et al [52] demonstrated the feasibility of VSAT TCP session hijacking for reaching and controlling maritime VSAT communication. Moreover, Tam and Jones[58] argued that users can be tricked into downloading and executing malicious software or guided into malicious websites.

After gaining access to systems and networks attackers aim to achieve a group of objectives including discovery, credential access, and collection. Hemminghaus et al [39] target the network for discovery through sniffing and collection of network traffic including navigation data. Jo et al [43] categorized vulnerability scanning of ship systems, eavesdropping on Voice over Internet Protocol (VoIP), and Wi-Fi communication in the discovery stage of cyber attacks. Pavur et al [52] demonstrated the ability to collect credit card information, visa, passport, ship manifest, and non-encrypted REST API credentials communicated through eavesdropping on VSAT connections.

In certain cases, attackers desire to perform privilege escalation to execute commands and programs with higher privilege. Lund et al [47] mentioned that the operator station utilized as the pivot point of their attack demonstration was running already within administrator privilege and therefore doesn't require escalation. However, they referred to hijacking execution flow through a malicious Windows socket dynamic-link library (Winsock DLL), this is among the techniques utilized to achieve privilege escalation, persistence in the target system, and evade defensive measures [13].

Many works have discussed attacks that aim to impact maritime operations. Lund et al [47] and Hemminghaus et al [39] discussed the manipulation of sensor messages for impacting the operation of navigation systems. Amro et al [23] formalized manipulation and denial of view based on navigational data as attacks that can impact navigational functions. Moreover, Hemminghaus et al [39] referred to alarm suppression for inhibiting response functions as well as spoof reporting messages to impair process control.

Many stages of cyber attacks in the maritime domain are demonstrated and discussed in the literature in sufficient detail. Still, a limited discussion is observed regarding Command and Control (C&C) activities. Hooper [40] has investigated the potential of covert communications in pulsed or continuous-wave radar and discussed the cyber implications of that in the maritime domain. The authors argued that communication links utilizing spectrum-sharing may pave the way for unintended channels (i.e covert channels); an inclination which we agree with. Hareide et al. [37] bypassed the need for the C&C channel by implementing a specific condition for an attack to be launched when arriving at a certain position. Jo et al [43] described three maritime cyber incidents including C&C stages with a limited description of the implementation. Enoch et al [33] have briefly mentioned C&C in the attack model but without details of the implementation. Leite et al [46] proposed a triggering mechanism for cyber attacks based on radar and AIS messages. The authors proposed and demonstrated a pattern matching technique that can identify false plots depicted on the ECDIS which can be used for triggering cyber attacks. Other than that, to the best of our knowledge, no other work has discussed C&C in the maritime domain in more detail. Therefore, a contribution of this paper is an investigation of the utilization of AIS as a covert channel for C&C attack techniques using real maritime systems. This is intended to raise awareness of yet another possible attack utilizing the AIS protocol and hopefully drive the maritime community to consider cybersecurity more seriously and deeply within their systems.

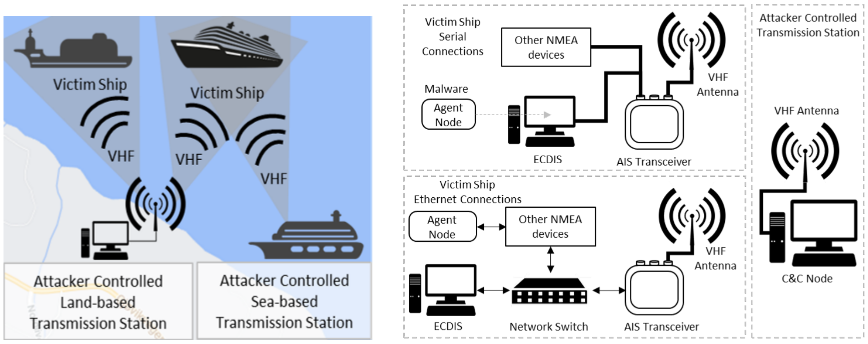
The concept of a kill chain; a multi-staged cyber attack scenario, is observed in the maritime domain. Hareide et al.[37] have discussed a maritime kill chain for demonstrating the feasibility of cyber attacks in order to increase awareness. The authors relied on a previously developed attack by Lund et al [47] which also discusses the development of the attack through a kill chain. Also, Jo et al [43] utilized consequent tactics from *ATT&CK* for describing cyber attacks against maritime systems. In this paper, we will also utilize the concept of kill chains for discussing complete scenarios for cyber attacks that implement our novel Command and Control (C&C) covert channel.

3 AIS as a Covert Channel

In this section, we discuss our analysis of the utility of the AIS as a covert channel supporting adversarial activities throughout different phases of cyber attacks. The analysis considers both the AIS protocol itself as well as AIS devices. This section also describes the threat model with details from different viewpoints. Context (i.e. physical and cyber architecture), Objectives (i.e. tactics), and techniques. Additionally, a proof of concept of the attack is developed and demonstrated in this section in addition to a discussion of relevant countermeasures.

3.1 Context view

Following a top-down approach, the context of utilizing AIS as a covert channel is discussed in this section. A physical view of the context is demonstrated in Figure 1a. A threat actor needs to be located in physical proximity to the victim ships either at land or sea. The range is limited by the VHF range of the attacker station and the placement of the antennas on both sides; the range can reach up to 60 nautical miles [19]. The VHF radio frequencies for AIS belong to the licensed portion of the radio spectrum and require a proper license to operate in most countries. Therefore, an attacker without a proper license can be detected and addressed. However, an attacker with a proper license such as an industrial competitor or a maritime entity belonging to a nation-state might operate undetected at this level.


Victim Ship
VHF
Victim Ship
VHF
VHF
Attacker Controlled Land-based Transmission Station
Attacker Controlled Sea-based Transmission Station
Victim Ship Serial Connections
Other NMEA devices
Malware
Agent Node
VHF Antenna
ECDIS
AIS Transceiver
Victim Ship Ethernet Connections
Agent Node
Other NMEA devices
VHF Antenna
ECDIS
Network Switch
AIS Transceiver
Attacker Controlled Transmission Station
VHF Antenna
C&C Node

(a) Physical view of the context of utilizing AIS as a covert channel

(b) Component view of the context of utilizing AIS as a covert channel

Fig. 1. Physical and component view for utilizing AIS as a covert channel

A component view of the context is depicted in Figure 1b. The attacker station consists of a Command and Control (C&C) node that is able to transmit AIS traffic over VHF. On the other hand, the victim ships network might have either serial [29, 55, 56] or Ethernet connections [30] from the AIS device to internal components. An internal agent node to be controlled by the attacker is needed to receive and execute the (C&C) commands. The agent node is assumed to either be a machine infected with an attacker's controllable malware or a standalone malicious machine. In a ship network consisting of serial connections, malware is expected to infect an existing machine. On the other hand, in an

Ethernet network, a standalone machine is a possible alternative. Different attack techniques are needed to establish a covert channel in each network (More details in Section 4).

3.2 Tactics and Techniques

The threat model is developed considering variant attacker capabilities and communicated as tactics and techniques using the *ATT&CK* terminology. The objectives (i.e tactics) of the attackers are assumed to be the following:

- Command and Control: send unidirectional C&C messages from an attacker to victims (1 to many). The messages can carry either simple commands or files (e.g. malware). This is assumed to be achievable through properly encoding commands and files into AIS messages. More advanced threat actors are expected to pursue secure C&C communication. They might aim to secure the communication from being revealed, or tampered with. Even if their activities are detected, the executed commands or transferred files are aimed to be kept a secret. This is assumed to be established through hiding command messages into AIS messages with additional obfuscation, steganography, or cryptography.
  A bi-directional channel is expected to require additional components, tactics, and techniques which are items for future work.
- Defense Evasion: this includes avoiding raising the operators' attention or other detection measures. This means that limited impact on legitimate operations is pursued. This is assumed to be achievable through careful selection of AIS message types and fields.

To achieve the C&C objective the attacker can establish the covert channel using a combination of Alternate Network Medium (i.e. VHF) [5] and Protocol Tunneling [17] command and control attack techniques. This combination entails the utilizing of VHF radio communication as a medium for the C&C communication which is tunneled through the AIS protocol. Based on the attacker capabilities to secure it, attackers can apply Data Encoding [7], Data Obfuscation [8] or Encrypted Channel [9]. According to ATT&CK, data encoding can be achieved using standard or non-standard encoding (e.g. Base32), Data obfuscation can be achieved using stenography, protocol impersonation, or junk data, and Encrypted channel can use asymmetric or symmetric cryptography [15]. On the other hand, to avoid detection, the different types of AIS messages and fields are considered to best serve the objectives. The criteria for choosing the most suitable message type and field is that they should provide the largest capacity of transfer and limited impact on operations. The rationale for choosing the largest capacity is to reduce the amount of AIS messages needed to encode C&C messages.

We have considered all possible 27 AIS message types using the description provided By Rayomon[53]. As shown in Table 1, messages 8 and 14 were found to provide the largest capacity while at the same time having a common appearance, unlike message type 26. Moreover, the messages types; if carefully configured, do not provide navigational data that will influence the navigational functions and therefore are expected to have no impact on operations. Message 14 can be utilized in managing distress signals and might invoke a response from a nearby rescue unit [48]. Therefore, we will restrict our discussion in this paper in the utility of message type 8 for C&C. Furthermore, the structure of message 8 content itself is controlled. We analyzed the different content categories to identify the category that allows for the largest capacity and flexible field format. We relied on IMO circulation SN.1/Circ.289 [28] in our analysis. We have identified that a text description message is the best candidate as it includes a text string field with a maximum limit of 161 ASCII characters. Although there is a standard format for this field, it is only recommended and not mandatory to follow.

Table 1. The top 5 AIS message types with the largest fields

Message Type	Field	Max Size (bits)	Rational
Type 26: Multiple Slot Binary Message	Data	1004	Extremely rare
Type 14: Safety-Related Broadcast Message	Text	968	Suitable.
Type 8: Binary Broadcast Message	Data	966	Suitable.
Type 12: Addressed Safety-Related Message	Text	936	Addressed to a specific target. Reduced C&C channels
Type 6: Binary Addressed Message	Data	920	Addressed to a specific target. Reduced C&C channels

3.3 Proof of Concept

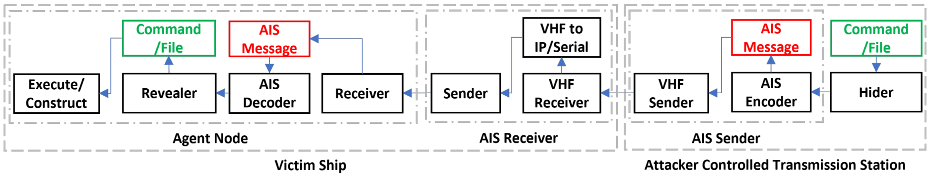


Fig. 2. A logical view of the components of the AIS covert Channel

In this section, we present the development of the proof of concept for utilizing AIS as a covert channel. Figure 2 depicts the required logical components to achieve the attackers' objectives. First, the C&C message or file is input into a hider function to evade detection and the output is then encoded into an AIS message. Then, the message is transmitted over VHF using an AIS transmitter. Should it be received and accepted at the AIS on the victim ship, protocol conversion is expected to forward the AIS messages through a serial link or IP protocol to the ship network; this is traditionally performed by AIS receivers. The agent node then eavesdrops on the AIS message stream, decodes the messages to identify C&C messages (e.g. based on the MMSI or other signal) reveals the hidden message, and executes it, or reconstructs it if its part of a file. Through this channel, attackers gain the capabilities to remotely and covertly update their cyber attack arsenal and techniques.

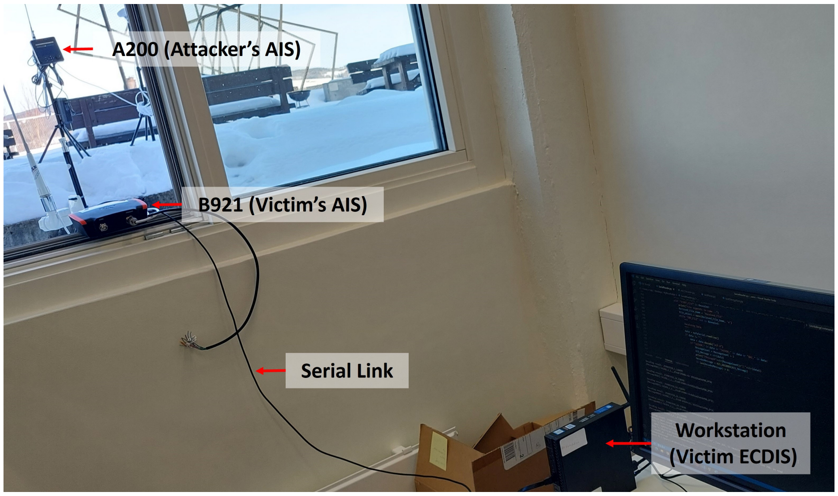
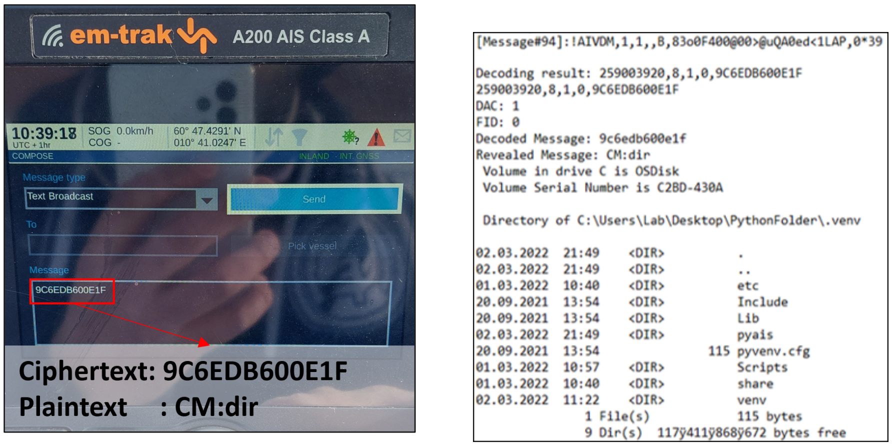


Fig. 3. Setup for the proof of concept of AIS as a covert channel

Figure 3 depicts the setup for the proof of concept. It is implemented using two AIS transceivers, namely, em-trak A200 and em-trak B921. A200 is used as the attacker-controlled transmission station. B921 is used as the AIS receiver and is connected through a serial link to a workstation simulating the victim ECDIS. The workstation is equipped with a script that simulates the agent node or malware that is monitoring the AIS messages over the serial link. The script decodes AIS messages and when a C&C message is identified it executes the encoded command or reconstructs the transmitted file.

We conducted several experiments to test if the implementation works. We attempted to send and execute commands as well as construct files at the victim ECDIS. Due to space restrictions, we will present one of these experiments. First, the ciphertext which includes the hidden C&C message is prepared using a python script. In this example, the attacker will send a directory listing command, the plaintext of the hidden message "CM:dir" is encrypted using Advanced Encryption Standard (AES), the ciphertext is "9C6ED8600E1F" and then encoded into an AIS message "!AIVDM,1,1,,B,83o0F400@00¿@uQA0ed¡1LA P,0*39". The "CM:" string is used to identify a command execution message at the agent node while the "dir" string is the directory listing command in Windows.



```
[Message#94]:!AIVDM,1,1,,B,83o0F400@00>@uQA0ed<1LAP,0*39

Decoding result: 259003920,8,1,0,9C6EDB600E1F
259003920,8,1,0,9C6EDB600E1F
DAC: 1
FID: 0
Decoded Message: 9c6edb600e1f
Revealed Message: CM:dir
 Volume in drive C is OSDisk
 Volume Serial Number is C2BD-430A

 Directory of C:\Users\Lab\Desktop\PythonFolder\.venv

02.03.2022  21:49    <DIR>          .
02.03.2022  21:49    <DIR>          ..
01.03.2022  10:40    <DIR>          etc
20.09.2021  13:54    <DIR>          Include
20.09.2021  13:54    <DIR>          Lib
02.03.2022  21:49    <DIR>          pyais
20.09.2021  13:54               115 pyvenv.cfg
01.03.2022  10:57    <DIR>          Scripts
01.03.2022  10:40    <DIR>          share
02.03.2022  11:22    <DIR>          venv
               1 File(s)            115 bytes
               9 Dir(s)  117ÿ411ÿ868ÿ672 bytes free
```

(a) Sending from A200

(b) Receiving at the agent node

Fig. 4. Demonstration for sending and receiving covert C&C message over AIS

Figure 4(a) depicts a photo of the message composer at the A200 AIS transceiver with the ciphertext as the content of the message. After the message was sent, Figure 4(b) depicts a screenshot of the agent node receiving and executing the command.

3.4 Evaluation of the Covert Channel

In this section, we will evaluate the utility of the covert channel to attackers to better analyze the associated risk. The evaluation is discussed based on their type, throughput, and robustness to detection and countermeasures. Then, suggesting suitable improvement for the detection and prevention is provided.

Our analysis considers two hider functions and two settings for the covert channel. The hider functions are Base32 encoding and AES-CFB encryption; with a 16-byte key and a 16 bytes Initialization Vector (IV). The settings are either based on the protocol specifications or the em-track A200 commercial AIS device. The type of the channel is a unidirectional covert channel. The C&C node can transmit messages that the agent node can receive, however, the agent node; on its own, cannot establish an outbound channel through the AIS device. This limits the attackers' capabilities in managing the agent node in the targeted environments. Regarding the throughput, the maximum capacity for the text string field is 966 or 480 bits in the protocol specifications or the A200, respectively. The implementation of encoding or encryption further restricts the capacity. Table 2 depicts the maximum size of the field that can hold the clear segment of a command or a file as well as the corresponding throughput considering the two hider functions, two settings, and two transmission rates (TR).

From the attacker's perspective, using AES as a hider function is a reasonable option since it provides secure communication with only a relatively less

Table 2. Covert Channel Throughput Evaluation

Hider Function	Based on	Max Field Capacity (bit)	Throughput (bit/sec) 2 sec TR	10 min TR
Base32	Protocol specs	600	300	1
	AIS200 em-trak	276	138	0,46
AES	Protocol specs	480	240	0,8
	AIS200 em-trak	240	120	0,4

TR: Transmission Rate

throughput than the Base32. Still, secure key establishment and handling is an additional burden the attacker needs to consider. While the Base32 encoding is simpler to implement and provides slightly better throughput, it doesn't provide secure communication and can expose the content of the covert channel. We have also evaluated the utility of this channel for delivering malware to the victim ship and allowing threat actors to update their adversarial cyber arsenal at sea. With such a transmission rate, transporting a 338 Kb malware; the average malware size in 2010 [14] at a 2-sec transmission rate would take 3 hours considering the protocol specifications. However, transporting the NotPetya malware which is 1,5 Gb [6] would take 29826 hours at the same transmission rate. Therefore, the utility of this covert channel is limited to commands and small malware. Regarding robustness to detection and countermeasures, several works have discussed countermeasures for securing AIS communication using encryption for authentication and integrity [44, 35, 24, 25]. Although a wide adoption of such countermeasures is not observed we argue that encryption doesn't eliminate the threat of covert channels against AIS. In the case of utilizing a public key infrastructure (PKI) for authenticating the different entities participating in the AIS communication, threat actors with legitimate credentials such as boat and ship owners, competitors, and nation-states would still be able to utilize the channel. Moreover, there is a discussion regarding anomaly detection algorithms for AIS such as the work of Iphar et. al [42], Blauwkamp et. al [27] and Balduzzi et. al[25]. However, there is no discussion regarding anomalies associated with AIS message type 8. Additionally, if the attacker maintained a reduced transmission rate, the likelihood of detecting anomalies is expected to be reduced. Real maritime infrastructure is required for formal evaluation of the robustness of this covert channel against detection. Therefore, we argue that such channels constitute a threat to the maritime infrastructure that is utilizing AIS communication and countermeasures should be tuned to detect them. Future efforts are advised for investigating the utility of anomaly detection in detecting the covert channel.

4 Adversary Emulation against an Auto-remote Vessel

To demonstrate the utility of the proposed covert channel for attackers, and its technical application in realistic attack scenarios, we will apply an adversary emulation process; a security assessment process applying realistic attack scenarios which emulate the capabilities of real threat actors [57]. This enables the elicitation and evaluation of relevant security control.

In this section, we present two cyber kill chains emulating two attack scenarios against an Autonomous Passenger Ship (APS) use case which is discussed in Section 2.1. The kill chains are constructed based on the observed adversarial techniques in the maritime industry across the different kill chain phases which are discussed in Section 2.3. Additionally, we improve the kill chains by utilizing the proposed C&C channel discussed in Section 3 to demonstrate its application. We argue that the kill chains are also relevant for other maritime use cases encompassing similar technologies.

We utilize our previously proposed maritime-themed testbed [21] for the development of the adversarial techniques. The utilization of the testbed with regards to this paper is system replication and system analysis. During system replication, we developed a replica of the target system using real and simulated components, and then target the developed replica with a group of attack techniques emulating an adversarial behavior.

4.1 Target Environment

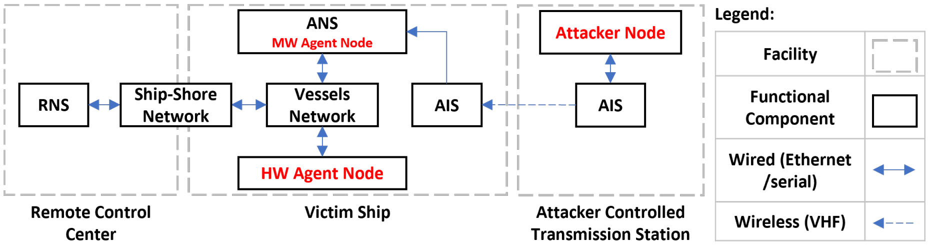


Fig. 5. A model of the target environment for the development of the kill chains

A model of the target environment is depicted in Figure 5. It emulates three facilities, namely, an attacker-controlled transmission station, a victim ship, and a remote control center. The attacker station consists of capabilities to create and transmit command and control traffic encapsulated within AIS messages over VHF. The A200 AIS is utilized at this station. The victim ship consists of an AIS transceiver; in this setup, the B921 is utilized. The receiver AIS receives AIS messages and forwards them over a serial link to the Autonomous Navigation System (ANS) which in turn forwards it to the Remote Navigation System (RNS) over a ship-shore network. The ANS and RNS are emulated using virtual machines while the vessel and ship-shore networks are emulated using virtual networking using Virtualbox. Due to the lack of available ANS and RNS software, both components are simulated as chart plotters using the OpenCPN software. The difference between them is that the ANS is not intended to be monitored by a human operator while the RNS is. The autonomous and remote navigation functions are simulated only through rendering the AIS and companion NMEA messages in the chart plotter. No control functions are simulated in this environment. Additionally, another virtual machine with Kali Linux is added to simulate a hardware agent node. This environment will be utilized in the demonstration of the later kill chains and is added as part of our testbed for further research.

4.2 Cyber Kill Chains

In this section, we present and discuss two attack scenarios. We will utilize the *ATT&CK* terminologies to facilitate the communication of a threat. In this paper, we utilized the abstract concept of the tactics and techniques and positioned them in a maritime context. We utilized attack trees for the description of the kill chain as it has been observed to be a common approach in the literature [33, 34]. These kill chains can later be used as adversary emulation exercises for the evaluation of cybersecurity controls in maritime systems with technologies similar to the ones in the testing environment.

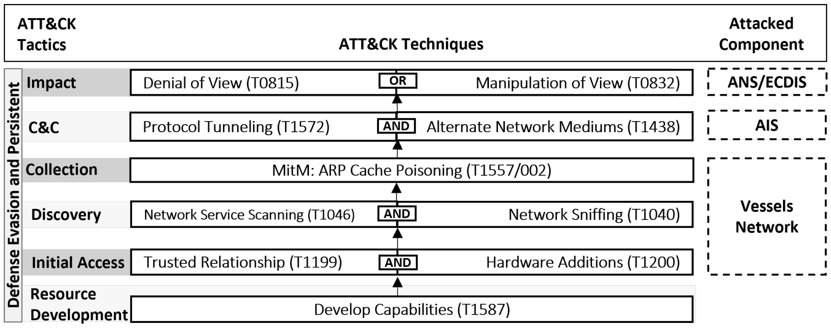

ATT&CK Tactics
ATT&CK Techniques
Attacked Component
Defense Evasion and Persistent
Impact
Denial of View (T0815)
OR
Manipulation of View (T0832)
ANS/ECDIS
C&C
Protocol Tunneling (T1572)
AND
Alternate Network Mediums (T1438)
AIS
Collection
MitM: ARP Cache Poisoning (T1557/002)
Discovery
Network Service Scanning (T1046)
AND
Network Sniffing (T1040)
Vessels Network
Initial Access
Trusted Relationship (T1199)
AND
Hardware Additions (T1200)
Resource Development
Develop Capabilities (T1587)

Fig. 6. Remotely and covertly controlling a malicious hardware agent node

Kill Chain 1: Impact through malicious hardware agent node The first kill chain depicted in Figure 6 describes the following scenario. A motivated threat actor invests in the development of attacking capabilities into the attacker agent node to be boarded on the vessel and remotely controlled from a place within range by utilizing the covert channel described in Section 3. The capabilities include a hardware component with Ethernet and software to receive and execute commands from the C&C node. In our environment, this is achieved through the Kali Linux virtual machine which can later be shipped into a Raspberry Pi or small hardware. The node is also equipped with scripts that are needed to conduct the later attack techniques. First, the developed capability needs to be connected to the ship network. Considering the lack of crew on the autonomous vessels, an attacker may attempt to access the vessel and locate the network and insert the agent node (Hardware Additions [12] or Transient Cyber Asset [18]). The success of this depends on the imposed physical security controls. In the case that physical controls exist, threat actors could exploit trusted relations and gain access to the network for several reasons (e.g. maintenance) and insert the node. This is a communicated concern in the maritime community. BIMCO; a global organization for shipowners, charterers, shipbrokers, and agents, discussed the issue of the lack of control of the onboard systems during ship visits in their latest guidelines [26]. They argued that knowing whether malicious software has been left in the systems onboard vessels is difficult. After the insertion of the node, assuming it received valid network configurations (e.g. through DHCP), the node is developed to conduct network service scanning using a scanning tool (e.g. NMAP) and sniffing using a network sniffer (e.g. tshark) to identify other components in the network. Later, target components with specific criteria are identified; certain operating system versions, or certain network services. The chosen targets are then targeted by a MitM attack in the form of ARP spoofing using a MitM tool (e.g. Ettercap). If that is successful, the node should be capable of eavesdropping on network traffic passing to and from the attacked components in the vessel network including AIS messages. When reaching this vantage point, the node stays dormant and only monitors the AIS messages to identify commands from the C&C node. On the other side, the threat group utilizes an alternate network medium that is the VHF radio used in the AIS to send C&C messages. The attacker node can send either command to be executed by the agent node upon reception or send files including malware. This capability allows attackers to bypass traditional network defenses if the AIS link is not monitored. In traditional vessels, the ECDIS which is usually connected to the AIS is considered air-gapped and not connected to the internet [37]. However, this attack would remove the gap and provide attackers with an offensive capability not possible before. At this stage, the threat group has a tactical advantage of observing the physical operational environment and launching an attack under certain conditions (e.g. difficult weather conditions in which visibility is limited). Their next step is targeting the NEMA messages in a combination of denial of view and manipulation of view attacks. The options for the attackers are a lot, only limited by the number of NMEA messages utilized in the vessels and their criticality to the navigation functions. In our earlier work, we formalized and demonstrated a group of such attacks [23]. One instance could be that the attackers choose to drop radar messages (TTM messages) going to the ANS denying it from establishing accurate rendering of the vessels in the physical environment. Also, attackers can manipulate the actual Speed Over Ground (SoG) estimated from the GPS to impact the speed of the vessel. According to a previously conducted Preliminary Hazard Analysis for an autonomous ferry use case, manipulation of sensor data could lead to collisions or ship sinking [59]. This concludes the first kill chain which can; in the lack of proper defenses, cause few clicks to sink a vessel.

Throughout the kill chain, several evasion and persistence techniques can be employed to challenge the detection and countermeasures and maintain a foothold in the network. This can include the utilization of the hider functions in the covert channel (Section 3), applying slight modification to the sensor data, and others.

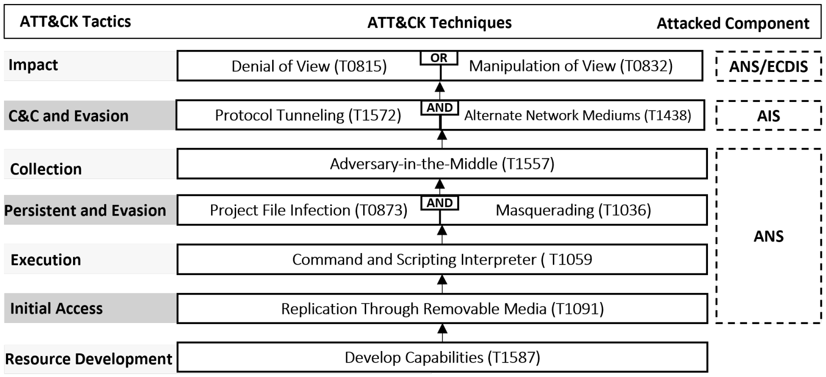

ATT&CK Tactics
ATT&CK Techniques
Attacked Component
Impact
Denial of View (T0815)
OR
Manipulation of View (T0832)
ANS/ECDIS
C&C and Evasion
Protocol Tunneling (T1572)
AND
Alternate Network Mediums (T1438)
AIS
Collection
Adversary-in-the-Middle (T1557)
Persistent and Evasion
Project File Infection (T0873)
AND
Masquerading (T1036)
ANS
Execution
Command and Scripting Interpreter (T1059
Initial Access
Replication Through Removable Media (T1091)
Resource Development
Develop Capabilities (T1587)

Fig. 7. Remotely and covertly controlling a malware agent node

Kill Chain 2: Impact through malware The second kill chain depicted in Figure 7 describes the following scenario. A motivated threat actor targets the APS through the maintenance personnel boarding the APS. It is assumed that the malware is loaded into the ANS through a USB stick. The malware relies on commands and scripting for executing its tasks. Upon execution, the malware aims to eavesdrop on the AIS messages communicated over the serial link at the ANS. However, serial interfaces allow only a single listener. In principle, there are several options to bypass this constraint. One option is discussed by Lund et al [47] through malicious Winsock DLL (Section 2.3). This direction, however, would require escalating privilege. Another option, which is explored in this paper, is to modify the configuration file of the ANS regarding the sources of AIS messages. A similar technique suggested in *ATT&CK* is called Project File Infection [16]. This option, in principle, doesn't require escalated privileges under the assumption that the permissions to modify the configuration files are granted to normal users. This is the case for the OpenCPN software. Therefore, the malware is programmed to first close the OpenCPN software to release the serial interface and update the data source configuration to receive AIS and NMEA messages from the malware over UDP and then reopen the software quickly. In this manner, the malware masquerades as a legitimate data source. However, during testing, it was observed that this activity can be detected by the local firewall. A message is shown on the monitor requesting acceptance for the creation of a new connection. Assuming that a local firewall is activated at the ECDIS, the attacker needs to implement techniques to bypass it. Now the malware is actually in the middle between the AIS and the OpenCPN software. It has access to the serial link, can collect the messages, and forwards them to the OpenCPN software to avoid disrupting the operations. At this vantage point, the malware keeps monitoring the messages waiting for a C&C message. When one arrives the malware can distinguish if it's a command to be executed or file segments to be reconstructed. From this point forward, similar to the previous kill chain, the range of possible activities the malware can perform is wide open and relies on the C&C messages sent from the attacker-controlled transmission station. Among the options are also manipulating or denying the view and possibly causing a collision and sink. The malware is developed using python and is compiled as an executable for windows.

This scenario relies on a group of assumptions regarding the knowledge needed by the threat group while developing the malware. First, the name and path of the ANS or ECDIS executable, as well as the name, path, and structure of the configuration file, are all assumed to be known. This is likely possible for commonly deployed software such as OpenCPN. Also, altering the configuration without causing operation disruption is not trivial if there are multiple AIS data sources and destinations. In our proof of concept, the modification is done using a simple rule which is to remove a serial data source and replace it with a UDP data source. These kill chain conditions render it a targeted attack that requires a sufficient level of the domain and system knowledge in addition to a moderate level of complexity.

5 Conclusion

Recent efforts are undergoing to introduce cyber risk management into the maritime community. This includes the continuous identification and analysis of the threat landscape. In this direction, this paper presents an overview of the maritime cyber threat landscape and presents the results of an investigation of a novel cyber attack against maritime systems. The attack is in the form of a covert channel utilizing the prominent Automatic Identification System (AIS) for sending Command & Control messages and delivering malware. We have investigated the feasibility of this attack by developing a threat model utilizing the *ATT&CK* framework, developing a proof of concept of the attack, as well as presenting two cyber attack scenarios (i.e. kill chains) that can utilize this attack. The feasibility of the attack has been demonstrated using existing technology that is relevant to a wide range of traditional and future maritime systems including autonomous vessels. The findings are hoped to urge the maritime community to increase their integration of cybersecurity practices. Future work can be dedicated to the investigation and development of mitigation solutions against the proposed covert channel. Additionally, the proposed kill chains can be utilized as adversary emulation plans for the evaluation of cybersecurity of maritime systems.

References

1. European defence agency, maritime domain. https://eda.europa.eu/docs/default-source/eda-factsheets/2017-09-27-factsheet-maritime (2017)
2. How mitre attck alignment supercharges your siem. https://www.securonix.com/how-mitre-attack-alignment-supercharges-your-siem/ (2019)
3. Ocean shipping and shipbuilding. https://www.oecd.org/ocean/topics/ocean-shipping/ (2019)
4. Transport modes. https://ec.europa.eu/transport/modes_en (Jan 2019)
5. Alternate network mediums. https://attack.mitre.org/techniques/T1438/ (2021), accessed on 30.01.2022
6. Backdoor built in to widely used tax app seeded last week's notpetya outbreak. https://arstechnica.com/information-technology/2017/07/heavily-armed-police-raid-company-that-seeded-last-weeks-notpetya-outbreak/ (2021), accessed on 20.12.2021
7. Data encoding. https://attack.mitre.org/techniques/T1132/ (2021), accessed on 30.01.2022
8. Data obfuscation. https://attack.mitre.org/techniques/T1001/ (2021), accessed on 30.01.2022
9. Encrypted channel. https://attack.mitre.org/techniques/T1573/ (2021), accessed on 30.01.2022
10. Enhancing with mitre. https://documentation.wazuh.com/current/user-manual/ruleset/mitre.html (2021)
11. Enisa threat landscape 2021. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 (2021)
12. Hardware additions. https://attack.mitre.org/techniques/T1200/ (2021)
13. Hijack execution flow: Dll search order hijacking. https://attack.mitre.org/techniques/T1574/001/ (2021), accessed on 14.03.2022
14. How large is a piece of malware? https://nakedsecurity.sophos.com/2010/07/27/large-piece-malware/ (2021), accessed on 20.12.2021
15. Mitre attck. https://attack.mitre.org/ (2021), accessed on 14.12.2021
16. Project file infection. https://collaborate.mitre.org/attackics/index.php/Technique/T0873 (2021)
17. Protocol tunneling. https://attack.mitre.org/techniques/T1572/ (2021), accessed on 30.01.2022
18. Transient cyber asset. https://collaborate.mitre.org/attackics/index.php/Technique/T0864 (2021)
19. Two-way radio range, the facts about distance. https://quality2wayradios.com/store/radio-range-distance (2021), accessed on 14.12.2021
20. Amro, A.: Cyber-physical tracking of iot devices: A maritime use case. In: Norsk IKT-konferanse for forskning og utdanning. No. 3 (2021)
21. Amro, A., Gkioulos, V.: Communication and cybersecurity testbed for autonomous passenger ship. In: European Symposium on Research in Computer Security. pp. 5–22. Springer (2021)
22. Amro, A., Gkioulos, V., Katsikas, S.: Communication architecture for autonomous passenger ship. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability p. 1748006X211002546 (2021)

23. Amro, A., Oruc, A., Gkioulos, V., Katsikas, S.: Navigation data anomaly analysis and detection. Information **13**(3) (2022). https://doi.org/10.3390/info13030104, https://www.mdpi.com/2078-2489/13/3/104
24. Aziz, A., Tedeschi, P., Sciancalepore, S., Di Pietro, R.: Secureais-securing pairwise vessels communications. In: 2020 IEEE Conference on Communications and Network Security (CNS). pp. 1–9. IEEE (2020)
25. Balduzzi, M., Pasta, A., Wilhoit, K.: A security evaluation of ais automated identification system. In: Proceedings of the 30th annual computer security applications conference. pp. 436–445 (2014)
26. BIMCO: The Guidelines on Cyber Security Onboard Ships. BIMCO (2016)
27. Blauwkamp, D., Nguyen, T.D., Xie, G.G.: Toward a deep learning approach to behavior-based ais traffic anomaly detection. In: Dynamic and Novel Advances in Machine Learning and Intelligent Cyber Security (DYNAMICS) Workshop, San Juan, PR. Retrieved from http://faculty. nps. edu/Xie/papers/ais_analysis_18. pdf (2018)
28. Circular, I.D.S.: Guidance on the use of ais application-specific messages‖. IMO NAV55/21/Add **1**
29. Commission, I.I.E., et al.: Iec 61162-1 (2010)
30. Commission, I.I.E., et al.: Iec 61162-450 (2016)
31. Committee, T.M.S.: Interim guidelines on maritime cyber risk management (msc-fal.1/circ.3/rev.1). https://cutt.ly/6R8wqjN
32. Committee, T.M.S.: International maritime organization (imo) (2017) guidelines on maritime cyber risk management. https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx
33. Enoch, S.Y., Lee, J.S., Kim, D.S.: Novel security models, metrics and security assessment for maritime vessel networks. Computer Networks **189**, 107934 (2021)
34. Glomsrud, J., Xie, J.: A structured stpa safety and security co-analysis framework for autonomous ships. In: European Safety and Reliability conference, Germany, Hannover (2019)
35. Goudosis, A., Katsikas, S.: Secure ais with identity-based authentication and encryption. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation **14**(2) (2020)
36. Greenberg, A.: The untold story of notpetya, the most devastating cyberattack in history, https://bit.ly/MaerskAttack
37. Hareide, O.S., Jøsok, Ø., Lund, M.S., Ostnes, R., Helkala, K.: Enhancing navigator competence by demonstrating maritime cyber security. The Journal of Navigation **71**(5), 1025–1039 (2018)
38. Havdal, G., Heggelund, C.T., Larssen, C.H.: Design of a Small Autonomous Passenger Ferry. Master's thesis, NTNU (2017)
39. Hemminghaus, C., Bauer, J., Padilla, E.: Brat: A bridge attack tool for cyber security assessments of maritime systems (2021)
40. Hooper, J.L.: Considerations for operationalizing capabilities for embedded communications signals in maritime radar. Tech. rep., NAVAL POSTGRADUATE SCHOOL MONTEREY CA (2018)
41. IMO: Resolution a.1106(29) revised guidelines for the onboard operational use of shipborne automatic identification systems (ais) (2015)
42. Iphar, C., Ray, C., Napoli, A.: Data integrity assessment for maritime anomaly detection. Expert Systems with Applications **147**, 113219 (2020)
43. Jo, Y., Choi, O., You, J., Cha, Y., Lee, D.H.: Cyberattack models for ship equipment based on the mitre att&ck framework. Sensors **22**(5), 1860 (2022)

44. Kessler, G.: Protected ais: a demonstration of capability scheme to provide authentication and message integrity. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation **14**(2) (2020)
45. Kovanen, T., Pöyhönen, J., Lehto, M.: epilotage system of systems' cyber threat impact evaluation. In: ICCWS 2021 16th International Conference on Cyber Warfare and Security. p. 144. Academic Conferences Limited (2021)
46. Leite Junior, W.C., de Moraes, C.C., de Albuquerque, C.E., Machado, R.C.S., de Sá, A.O.: A triggering mechanism for cyber-attacks in naval sensors and systems. Sensors **21**(9), 3195 (2021)
47. Lund, M.S., Hareide, O.S., Jøsok, Ø.: An attack on an integrated navigation system (2018)
48. Maritime, N.R.F.N. 46 ais safety-related messaging. https://puc.overheid.nl/nsi/doc/PUC_2045_14/1/
49. NMEA: National marine electronics association - nmea0183 standard (2002)
50. NTNU Autoferry: Autoferry - Autonomous all-electric passenger ferries for urban water transport. https://www.ntnu.edu/autoferry (2018)
51. Papastergiou, S., Kalogeraki, E.M., Polemi, N., Douligeris, C.: Challenges and issues in risk assessment in modern maritime systems. In: Advances in Core Computer Science-Based Technologies, pp. 129–156. Springer (2021)
52. Pavur, J., Moser, D., Strohmeier, M., Lenders, V., Martinovic, I.: A tale of sea and sky on the security of maritime vsat communications. In: 2020 IEEE Symposium on Security and Privacy (SP). pp. 1384–1400. IEEE (2020)
53. Raymond, E.S.: Aivdm/aivdo protocol decoding, https://gpsd.gitlab.io/gpsd/AIVDM.html
54. Standard, S., Greenlaw, R., Phillips, A., Stahl, D., Schultz, J.: Network reconnaissance, attack, and defense laboratories for an introductory cyber-security course. ACM Inroads **4**(3), 52–64 (2013)
55. Std, I.: 61162-2. Maritime Navigation and radiocommunication equipment and systems–Digital interfaces–Part2: Single talker and multiple listeners, high-speed transmission (1998)
56. Std, I.: 61162-3. Maritime Navigation and radiocommunication equipment and systems–Digital interfaces–Part3: Serial data instrument network (2008)
57. Strom, B.E., Applebaum, A., Miller, D.P., Nickels, K.C., Pennington, A.G., Thomas, C.B.: Mitre att&ck: Design and philosophy. Technical report (2018)
58. Tam, K., Jones, K.: Macra: a model-based framework for maritime cyber-risk assessment. WMU Journal of Maritime Affairs **18**(1), 129–163 (2019)
59. Thieme, C.A., Guo, C., Utne, I.B., Haugen, S.: Preliminary hazard analysis of a small harbor passenger ferry–results, challenges and further work. In: Journal of Physics: Conference Series. vol. 1357, p. 012024. IOP Publishing (2019)
60. Tran, K., Keene, S., Fretheim, E., Tsikerdekis, M.: Marine network protocols and security risks. Journal of Cybersecurity and Privacy **1**(2), 239–251 (2021)