**CyCon 2024: Over the Horizon**
**16th International Conference on Cyber Conflict**
C. Kwan, L. Lindström, D. Giovannelli, K. Podiņš, D. Štrucl (Eds.)
2024 © NATO CCDCOE Publications, Tallinn



# Enhancing the Cyber Resilience of Sea Drones

**Erwin Orye, Maj.**
Centre for Digital Forensics
and Cyber Security
Tallinn University of Technology
Tallinn, Estonia
erwin@orye.eu

**Gabor Visky**
Centre for Digital Forensics
and Cyber Security
Tallinn University of Technology
Tallinn, Estonia
gabor.visky@taltech.ee

**Alexander Rohl**
School of Computer
and Mathematical Sciences
Faculty of Sciences, Engineering and
Technology
University of Adelaide
Adelaide, Australia
alexander.rohl@adelaide.edu.au

**Olaf Maennel**
School of Computer
and Mathematical Sciences
Faculty of Sciences, Engineering and
Technology
University of Adelaide
Adelaide, Australia
olaf.maennel@adelaide.edu.au

**Abstract:** Sea drones are unmanned vessels that operate on or below the water's surface. During the military conflict between the Russian Federation and Ukraine, the latter has demonstrated how to use sea drones to attack Russian targets efficiently. However, as Russia's defences against drone attacks are continuously increasing, the cyber resilience of sea drones is becoming increasingly important. Technological developments in shipping have brought new cybersecurity challenges. This paper contributes to the knowledge on augmenting the cyber robustness of maritime autonomous surface-floating and subaqueous drones. Firstly, we aim to support manufacturers in building affordable sea drones that reduce the cyberattack surface of commercial drones. Secondly, we offer guidance for tactical military commanders on the potential cyber weaknesses in a sea drone's specific operational environments and its reliance on particular technologies. We propose eight distinctive threat categories for cyberattacks against autonomous vessels: attacks to disrupt radio frequency signals; attacks to deceive or degrade sensors; attacks to intercept or modify communications; attacks on operational technology systems; attacks on information technology systems; attacks on artificial intelligence (AI) used for autonomous operations; attacks through supply chains; and attacks through physical access. We use the STRIDE (spoofing,

tampering, repudiation, denial of service, elevation of privilege) [1] methodology in the context of each threat scenario, formulate mitigation measures to reduce the risk for each category, and link methods of cyberattack to each category.

**Keywords:** *cybersecurity, autonomous, threat modelling, unmanned, vessels, sea drones*

## 1. INTRODUCTION

Automation, and consequently limited human interaction, has created new vectors for cyberattacks. Cybersecurity is a critical issue for ships with some level of autonomy because of their increased dependence on information and communication technologies (ICT) for ship control, their advanced integration of control systems, their increased connectivity with shore control centres, and their accessibility to (and *from*) the Internet [2].

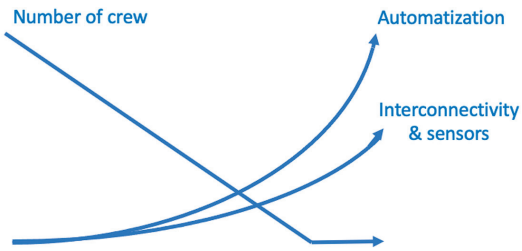
The coexistence of crewed and autonomous vessels (sea *drones*) necessitates the shared use of maritime, canal, and riverine domains. Ensuring the harmonious integration of these two naval transportation modes is vital to the sustainable and effective functioning of waterborne transportation systems.

Industry and academia have conducted extensive research and development in the field of autonomous vessels, such as Wärtsilä's IntelliTug [3], YARA Birkeland [4], L3Harris maritime autonomous systems [5], and Japan's fully autonomous ship program MEGURI2040 [6]. Research projects conducted in academia include, among many others, the University of Plymouth's Cetus Project [7], the Norwegian University of Science and Technology's Autoferry Project [8], and Heli by Tallinn University of Technology and the University of Tartu [9].

Sea drones rely entirely on digital systems with no physical crew to override them. Hence, the consequences of those digital systems being compromised can be more severe than would otherwise be the case.

Figure 1 depicts the evolution of growing automation. In particular, it shows how further automation is possible even when a vessel is already crewless, driven by the need for onshore supervision to become less involved.

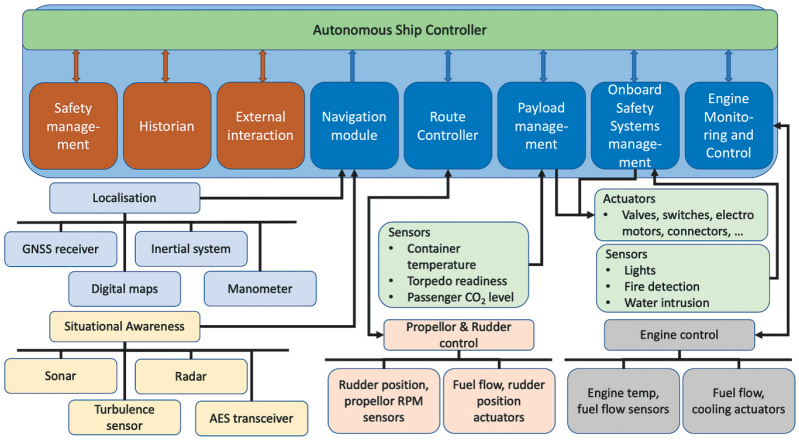
**FIGURE 1:** NUMBER OF CREW VERSUS THE LEVEL OF AUTONOMY AND RELIANCE ON AN INCREASED NUMBER OF INTERCONNECTED SENSORS




Sea drones come in many different configurations: surface and submarine, commercial and military, large and small, remote-controlled and auto-navigating, and many more [10]. Each configuration is suitable for a specific mission. Vessels can operate for days, weeks, and even longer without human intervention. For example, Saildrone's newest robotic ocean explorer sea drone draws its power from wind and can spend up to 12 months at a stretch out at sea [11]. The US Navy has recently received a prototype ship that can operate autonomously at sea for up to 30 days [12]. And, in 2022, the Nippon Yusen Kabushiki Kaisha (NYK Line) Designing the Future of Full Autonomous Ships (DFFAS) project achieved a 40-hour long autonomous trip across 790 kilometres (491 miles) at sea without human intervention for 99% of the journey [13].

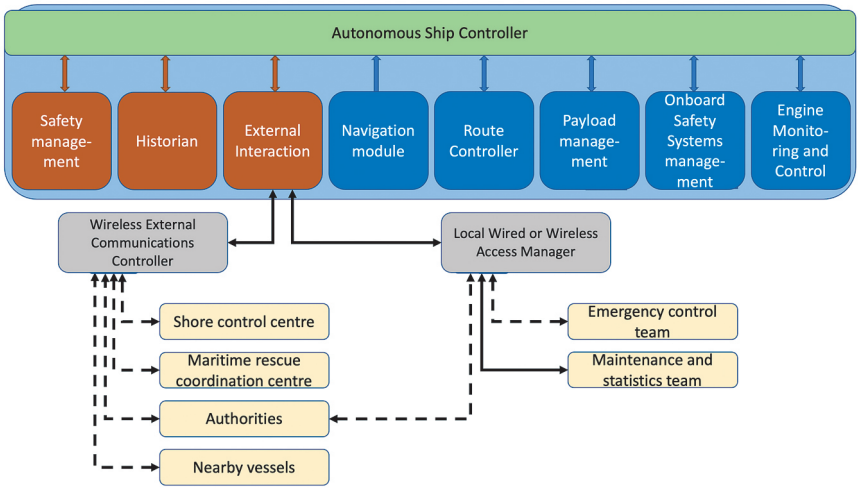
Although the configurations of sea drones might differ, their logical architecture often has the same functionalities. Figure 2 gives an overview of standard sea-drone functionalities.

**FIGURE 2:** SCHEMATIC OVERVIEW OF THE LOGICAL FUNCTIONS OF AN AUTONOMOUS SEA DRONE



Autonomous sea drones do, at some points, interact with humans, even if rarely or with only a minor impact on their functioning. Figure 3 shows the potential ways in which humans can interact with sea drones. Autonomous vessels have a command-and-control (C&C) channel to execute remote control commands, report sensor statuses, and receive mission instructions from the home base. This C&C channel is not necessarily always active, and the autonomous vessel might have to operate for long periods without supervision, potentially at a considerable physical distance from the control centre. As such, a sea drone needs to be equipped to operate in various uncontrolled environments and for different durations.

**FIGURE 3:** HUMAN INTERACTION WITH A SEA DRONE AND THE C&C LINKS FOR COMMUNICATIONS




## 2. RELATED WORK

To our knowledge, a combined study that jointly models the cyber threats, attacks, and defence methods regarding sea drones is not available in the literature (Section 2.B). It is this gap that motivated our research, in which we apply the STRIDE methodology (described in Section 2.A) to real scenarios to identify the adverse effects of cyber threats and the potential methods to defend against them.

### *A. Literature Review*

Silverajan et al. [14] identify seven main attack surfaces through which attackers can gain access to or disrupt operations on uncrewed ships: positioning systems, sensors, firmware, voyage data recorders, intra-vessel networks, vessel-to-land communication,

and remote operations systems. They also define six attack methods: code injection, tampering/modification, positional data spoofing, Automated Identification System (AIS) data spoofing, signal jamming, and link disruption/eavesdropping. However, their work does not cover contextual attack scenarios, possible consequences, or the mitigations required for defence.

Along similar lines, Agamy [15] proposes that the following three threats can affect the cybersecurity of autonomous ships: malicious components added to control systems during building or maintenance sessions, compromised communication links, and position data spoofing. Agamy also discusses a number of examples and regulatory frameworks, such as the International Safety Management Code (ISM), the International Ship and Port Facility Security Code (ISPS), the EU's General Data Protection Regulation (GDPR), and the Australian Cyber Security Center's Final Security Strategy. However, these frameworks do not offer any technical defence measures.

As for the cybersecurity risk assessment of autonomous ships, Tam and Jones [16] model risks relating to the systems and components of autonomous vessels – for example, AIS, Global Navigation Satellite Systems (GNSS), automated mooring systems, cargo management systems, radar, sensors, and voyage data recorders (VDR) – from the perspectives of theft, damage, denial of service, obfuscation, and misdirection. Their model-based framework for maritime cyber-risk assessment (MaCRA) risk model provides a comprehensive method for assessing risk, but the paper does not cover mitigation for the risks or defensive methods against them.

Kavallieratos et al. [17] analyse an autonomous ship into 14 systems: Engine Automation, Bridge Automation, Shore Control Centre, Autonomous Engine Monitoring and Control, Engine Efficiency, Maintenance Interaction, Navigation, Autonomous Ship Controller, Human-Machine Interface, Remote Manoeuvring Support, Emergency Handling, AIS, ECDIS, and Global Maritime Distress and Safety. They then identify threat scenarios for each system using the STRIDE framework. In subsequent research, Kavallieratos and Katskas [18] extend this approach by considering further components of the ship's systems, such as collision avoidance, RADAR, closed circuit television (CCTV), advanced sensor modules, and autopilot systems. These papers give an overview of the risk assessment of autonomous ships. However, they do not detail attack scenarios and defensive measures.

Sungbaek et al. [19] identify cyber threats against autonomous ships, but they do not structure this content into a framework.

## *B. Threat Model*

Threat modelling identifies and enumerates potential security threats and categorizes countermeasures by priority so as to reduce security risks to an acceptable level for the system owner. It includes several safety-focused risk management methodologies for Industrial Control Systems [20]. The CIA-triad (confidentiality, integrity and availability) has been used as a conceptual model in computer security for several decades [21]. The STRIDE methodology, as defined by Shostack [22], categorizes threats corresponding to cybersecurity goals by incorporating three more elements: authentication, non-repudiation, and authorization. The STRIDE threat categories are as follows [23]:

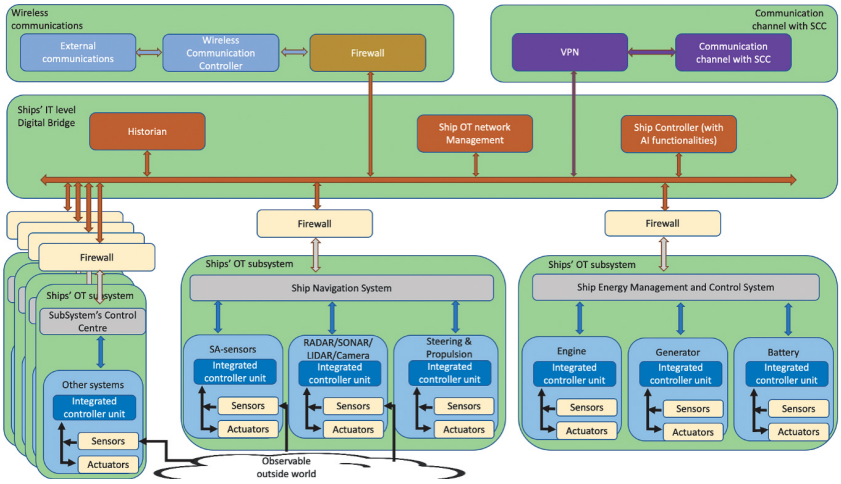
1) Spoofing is the ability of an adversary to masquerade as someone or something else.
2) Tampering refers to modifying or disrupting a system's disk, network, or memory.
3) Repudiation relates to threats where someone denies having taken specific actions that impact the system's operation or disclaims responsibility for the resulting outcomes.
4) Information disclosure involves exposing confidential information to unauthorized individuals.
5) Denial of service refers to compromises to the system's availability that work by consuming the necessary resources for its proper operation.
6) Elevation of privilege refers to situations in which an adversary can execute unauthorized actions.

According to Kim et al., the STRIDE methodology can be used for threat modelling against a distributed control system (DCS) [24]. Since our research focuses on sea drones, and since these are considered a system of DCSs [25], we adopt and use the STRIDE methodology. In that light, our research examines the different possible attacks so as to address the potential threats posed by malicious actors. Instead of focusing on a specific technology used in a particular ship, this paper employs general but transferrable abstractions. Thus, we offer a future-proof approach that can accommodate the broad functionalities of sea drones and cyberattack vectors.

# 3. RESULTS

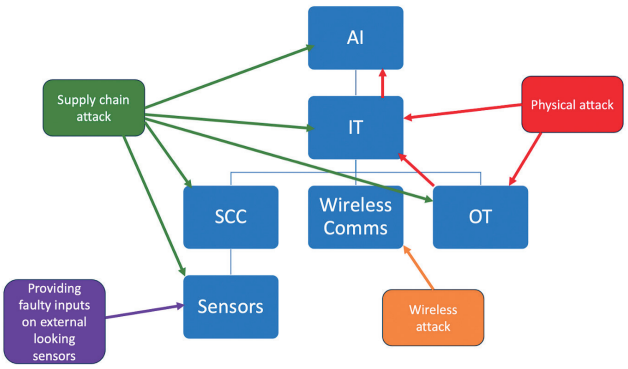
This section introduces the selected attack scenarios and their STRIDE analyses. To help motivate these scenarios, we must first consider the necessary functions of sea drones and their related subsystems. Figure 4 shows an abstract schematic overview, focusing only on the different types of equipment and how they relate to each other within an autonomous vessel.

**FIGURE 4:** SCHEMATIC OVERVIEW OF SUBSYSTEMS IN AN AUTONOMOUS VESSEL




To understand the attack surface of these subsystems, we must examine the lines for information flow. Figure 5 gives an overview of each sea-drone subsystem's possible attack vectors.

**FIGURE 5:** THE POSSIBLE ATTACKS ON A SEA DRONE'S SUBSYSTEMS



Taking these attacks and the interaction of the different subsystems as our starting point, we defined eight areas that we examine in more detail through the STRIDE methodology:

1) Attacks to intercept, modify or disrupt wireless communications
2) Attacks to deceive or degrade sensors
3) Attacks on operational technology (OT) systems
4) Attacks on information technology (IT) systems
5) Attacks on artificial intelligence (AI) for autonomous operations
6) Supply chain attacks (SCA)
7) Physical attacks to launch cybersecurity attacks and
8) Attacks against the shore control centre (SCC)

### *A. Attacks to Intercept, Modify, or Disrupt Wireless Communications*

**Description:** RF signals serve various purposes in relation to wireless communication, radar systems, and other wireless technologies. Disrupting RF signals involves actions taken to interfere with or disturb these signals. This can be accomplished through various means – for instance, jamming, interference, or deliberate manipulation of the signals – that degrade or turn off communication between devices or systems that rely on these signals.

**Possible scenario:** A design weakness, implementation, or design flaw in authentication or encryption can lead to signal manipulation.

**S:** Communication protocols such as AIS are easy to spoof in the maritime sector [26].
**T:** An attacker on the wireless C&C channel between the control station and the autonomous vessel could take over complete control of the ship.
**R:** There is often at lack of robust resilience against data modification within existing RF protocols. The absence of features to facilitate repudiation becomes apparent.
**I:** Autonomous vessels have sensors onboard. Some vessels provide some information on the fly through wireless channels to the home base. Access by third parties to sensitive information can lead to the disclosure of information.
**D:** Disruption of the C&C channel can lead to the vessel being made idle or execute fully automated actions, such as return to base. In any case, it is likely to lead to a denial of service for the operation of the vessel.
**E:** Accessing the C&C channel can allow deeper access to the system and overruling immutable parameters from a distance.

**Possible mitigations:**

- Using inertial systems or recognizing the environment with sensors and correlation with databases can mitigate incorrect GNSS input data or the unavailability of GNSS input data.
- There are multiple mitigations to protect against jamming, such as channel hopping, spectrum spreading, MIMO (multiple-input and multiple-output) based mitigation, channel coding, rate adaptation, and power control [27].
- A VPN solution or similar can potentially protect the C&C channels themselves and add additional authentication and integrity checks such as counters on messages, structure of messages, digital signatures, and so on.
- Communications that rely on interoperability – for instance, a communication channel between harbour and vessel, AIS, weather forecast broadcast, GNSS, or GDMSS – are vulnerable to attacks by design. However, there are possible countermeasures. For example, the autonomous vessel could try to filter out fake AIS messages by looking at the physical layer of the message and correlating this with previous messages to compensate. On the other hand, ignoring AIS messages too readily might decrease the vessel's situational awareness, which can increase the danger of collisions. Securing those channels would be the next level of security for autonomous ships.

### *B. Attacks to Deceive or Degrade Sensors*

**Description:** The sensors that capture information outside an autonomous ship offer a high-privilege way for attackers to influence the ship's operation because the attacker does not need physical access to the vessel to compromise these. In this regard, the location or proximity of the vessel is a condition to consider.

Another attack would be fooling internal sensors such as fire detection, engine failure, stability sensors, and so on. However, this would require first gaining physical access and initiating attacks on the sensors from there.

**Possible scenario:** A ship's sensors are prone to jamming and the injection of false echoes. The same applies to sensors designed for very short-distance situational awareness, such as cameras and illuminating LEDs on optical sensors.

**S:** An attack that changes the vessel's surroundings so that the sensors pick up a modified input. If an attacker knows a sensor's behaviour, they can modify the input so as not to trigger attention from the digital bridge.
**T:** Sensors need calibration before use. An attacker tampering with calibration (e.g., for a depth sensor) might cause severe havoc.

**R:** Most attacks that fool the sensors and provide erroneous information are challenging to repudiate.
**I:** Knowing how many sensors and what characteristics they have might indicate what type of vessel it is and how to attack it.
**D:** Ensuring that sensors cannot provide measurements in their everyday working range would constitute a denial of service for those sensors.
**E:** Attacks against sensors do not necessarily provide a means for privilege escalation.

**Possible mitigations:**

- The autonomous ship should have sufficient sensors based on entirely different technologies, compare the inputs from those sensors, and make decisions based on as complete information as possible. The greater the range of different technologies installed, the more difficult it becomes for the attacker to successfully provide all of the wrong inputs simultaneously. For example, using lidar, radar, and AIS systems to determine if the vessel is on a collision course with another ship is more reliable than using only AIS or only one radar sensor. In the former situation, hackers might need to intervene in close proximity to the targeted ship to influence its behaviour. Good situational awareness of the vessel's surroundings, above and under the sea level, is vital to detecting any signs of an intruder. The correlation of inputs from different sensors and specific sensors over time can reveal threats.
- Log files and histograms might help the digital bridge determine if any sensors are producing incorrect input data and take action to mitigate the problem. Such action can equally help with faulty sensors when there is no intervention from a malicious actor.

### *C. Attacks on Operational Technology Systems*

**Description:** Most of the digital components of an autonomous ship are operational technology (OT) systems. Traditionally, protocols used in OT systems are vulnerable to various cyberattacks since there is no standard encryption mechanism implemented in most communication protocols, and the authentication happens at the hardware level or not at all. For example, all major fieldbus protocols – such as Modbus, DNP3, Profinet and EtherCAT – lack authentication or encryption. Thus, if they manage to get access to the network, attackers can disrupt network operations or manipulate I/O messages to cause a failure in the control process [28].

**Possible scenario:** Different attacks are possible in this context, such as first hacking the C&C link and, with privilege escalation, getting into the core networks. Gaining

physical access to the system, such as through maintenance ports or even the physical wires, is another option.

**S:** It is straightforward to spoof an endpoint in an OT network since there is no authentication, and, therefore, it is easy to spoof an existing hardware address.
**T:** OT systems are prone to supply chain attacks and insider threats. For example, maintenance personnel could constitute an insider threat. An example of the former would be if a manufacturer or another actor in the supply chain of the OT endpoint or core element were to reveal undocumented functionalities that an attacker could use to launch an attack.
**R:** There are often no logfiles for OT networks since the total number of messages is substantial, even though each individual message might be small in size.
**I:** An attacker can read all the information passing on the bus. Depending on the size and type of endpoints, they can map the topology of the network and the functionalities of each endpoint.
**D:** By flooding the bus with messages, the denial of service of an endpoint becomes straightforward. If the endpoint is only sending information, this information is not reaching any destination. If the endpoint reads information from the bus, it will not receive any helpful input data.
**E:** The OT systems are often at the heart of the autonomous vessel. Protection focuses on threats from the outside. An attacker might try to go from the OT network (or bus) to get to a central controller and from there to the digital bridge.

**Possible mitigations:**

- By segregating networks, the amount of helpful information available on any one segment can be limited. Gateways, firewalls, and other security measures are essential to reduce the risk of an attacker gaining access to more segments, controllers, or even the digital bridge.
- Considerations should be made for implementing enhanced security for control systems, encrypting all volatile and non-volatile memory, securing bus protocols between different devices, and segregating/segmenting the networks with controls. Implementing these measures is challenging because of the number of OT devices on board and the need for common relevant standards.
- Another possible line of defence is to analyse all traffic in real time with anomaly-detector machine-learning algorithms that can identify abnormal behaviour.

### *D. Attacks on Information Technology Systems*

**Description:** Attacks on information technology (IT) systems modify the firmware of various components and devices on autonomous ships, operating systems, and software running on higher-level machines.

**Possible scenario:** With an attack on the IT systems, an attacker gains access to the digital bridge. Depending on the elevation of privilege on the IT system(s), this might allow them to gain complete control over the vessel.

**S:** Without firmware integrity verification and authorization for firmware updates, an attacker could perform an unauthorized firmware update. If the operator activates this option, the attacker could execute this via maintenance interfaces and over-the-air updates.
**T:** Malicious firmware updates can tamper with the functionalities of the autonomous vessel.
**R:** Without signed versions of software updates, it is nearly impossible to attribute an attack digitally.
**I:** Once an attacker is in the IT systems, they might have access to databases, (sensor) data, localization, the health status of the vessel, and other critical information.
**D:** When the central IT system is not responding as designed, the autonomous vessel is no longer executing its mission.
**E:** One of the most effective paths for an attacker of an IT system is an escalation of privilege. To gain complete control over the autonomous vessel, the attacker needs access to many functionalities in the IT system.

**Possible mitigations:**

- The first question that an operator of an autonomous vessel should decide upon is whether software or firmware updates are allowed over the air. Depending on the situation, one option will be better than the other. If operators at the SCC do not have access to the ship when they discover a significant software flaw, one option is to implement a patch immediately over the air. Still, enabling this access increases the attack surface for attackers. It is essential to know the status of the software and hardware and, therefore, use signed versions of firmware from trusted companies, define policies on who, when, and how to update the system, and, last but not least, test the software for functionality and security before installing it.
- Preferential redundancy is critical for making autonomous decisions. Use equipment and software from different vendors that provide the same functionality to install multiple independent calculation chains and, ultimately, use a voting system that decides what action to take.

### *E. Attacks on AI for Autonomous Operations*

**Description:** Machine learning code provides functions that can replace the human factor. This kind of software is, therefore, interesting from an attacker's point of view since it is directly engaged with the decision-making process. Attacks on machine learning software aim to cause misjudgement or malfunction.

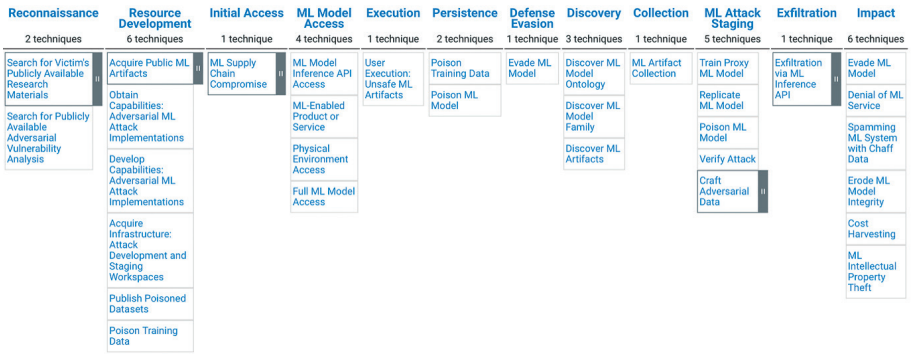
**Possible scenario:** Typical attacks on machine learning include evasion attacks (to fool a machine learning model by corrupting the query), model poisoning, and data pointing.

**S:** An attack on specific sensors might change the input for the AI coming from that sensor and fool the algorithms into changing the outcomes of decisions.
**T:** Modifying the behaviour of the AI software can result in different responses to sensor inputs. If the attacker has enough knowledge about the vessel, they might use this to execute actions on the ship.
**R:** Without digital signatures to allow changes in the AI software, other traces are required to achieve repudiation, which can be challenging.
**I:** Tampering with the AI system might lead to the full disclosure of all data available or generated on the vessel.
**D:** When altering the AI system, it is possible to achieve a complete denial of service of the autonomous vessel by spoofing input values to the AI that take unusually long to process.
**E:** Given that this attack targets the data of the AI system, it is important to note that it does not facilitate privilege escalation.

**Possible mitigations:**

- Select training datasets that focus on how to work effectively under sensor degradation or actuator failures. It is also crucial to consider what happens if the opponent knows the algorithms or the learning datasets and can create special conditions by fooling some sensors. Machine learning could help discover weaknesses in other machine learning software.
- Figure 6 shows all the attacks against deployed machine-learning systems according to the ATLAS framework.
- Extensive testing in extreme conditions should be conducted. The datasets for learning the system should include ways of responding to cyberattacks.

**FIGURE 6:** MITRE'S ADVERSARIAL THREAT LANDSCAPE FOR ARTIFICIAL INTELLIGENCE SYSTEMS [29]




## *F. Supply Chain Attacks*

**Description:** Attacks on the supply chain – which can have various sources, including third-party vendors, internal employees, and others – include disruption of operations, compromise of sensitive information, financial losses, reputational damage, legal and regulatory implications, and so on [30].

**Possible scenario:** A hacker steals a certificate used to vouch for the legitimacy or safety of a company's product, or a hacker leverages the tools for building software applications to introduce security weaknesses in the development process. Similarly, preinstalled malware can represent a valid threat scenario – for instance, if there is a malicious component in the firmware.

**S:** Implement faulty MAC addresses, ID numbers, or other mechanisms to receive information from the internal bus or networks.
**T:** Malicious code or components can be injected into the product through targeted attacks that initialize, for example, communication to a C&C server, thus creating a tampering backdoor into the system.
**R:** It is always difficult to tell which actor implemented a backdoor, a spy module, a modified firmware, and so on. Was it the chip manufacturer, the print board, the integrator, the shipping company, or other stakeholders?
**I:** When malicious actors trick individuals, a phishing attack can lead to information disclosure or compromised security, sometimes providing access with elevated rights.
**D:** A compromised component can cause a denial of service on an autonomous ship.
**E:** Malicious code running in a software component with elevated privileges can offer access to the IT systems with elevated rights.

**Possible mitigations:**

- Considering the multiple forms they can take, defending against SCA requires a range of different techniques, including auditing the IT (shadow) infrastructure, a highly secure build and update infrastructure, up-to-date software assets, application of client-side protection solutions, and so on [31].
- It is necessary to precisely follow up on all modifications made to a product, from designing to manufacturing integration to decommissioning.

### *G. Physical Attacks to Launch Cybersecurity Attacks*

**Description:** If an autonomous ship operates in the open sea, physical protection for the vessels can easily be weaker than otherwise.

**Possible scenario:** Various maintenance interfaces on autonomous ships, such as USB, Serial, JTAG and RJ45, could be exploited as initial attack vectors. Even if there are physical locks to prevent unauthorized physical access to these interfaces, there is a possibility that an attacker could compromise the locks and make unauthorized connections through these interfaces as the autonomous ship navigates in the open sea for an extended period of time.

**S:** With physical access to the vessel, an attacker gains an entry point to the digital systems without facing the difficulties of accessing interface points with the outside world. It makes sense that those interface points are the way in with the least privilege and the most extensive logging. Otherwise, determining the ease of spoofing the system depends on the exact location of the entry point.
**T:** There are many possible tampering actions, from swapping disks to plugging USB sticks with malware into maintenance. Different attacks are possible depending on the time available, size, computational power, design, and complexity.
**R:** Physical attacks are complicated to attribute digitally. Forensics might find some artefacts if, for example, malware leaves some digital traces.
**I:** Information disclosure is a risk for all internal communication that is not encrypted and where the attacker with physical access can extract the data. The same goes for databases that contain unencrypted data.
**D:** All physical destruction – for instance, unplugging a cable or flooding a data bus – will lead to denial of service of parts or the whole of the autonomous vessel.
**E:** An attacker still has to achieve elevation of privilege unless they can physically replace the IT system with their own.

**Possible mitigations:**

- There are many options to reduce the risk of physical access and the impact of such an attack: segregation and segmentation of the networks, cable fault sensors that detect anomalies, sensors that raise the alarm on intrusion, external sensors such as drones or satellites that surveil the neighbourhood of the vessel, physical protection measures such as locks to reduce the chances of obtaining physical access, firewalls between segments, time scheduled maintenance slots, and so on.
- Cost, the attacker's benefit, the vessel's value, available space, allowed weight, power consumption, and so on will probably determine the number and type of countermeasures that can and need to be put in place.

### *H. Attacks Against the Shore Control Centre to Launch a Cyberattack on a Sea Drone*

**Attack description:** Most autonomous ships have a C&C channel to receive input from the home base. This communication can be sporadic when tasking a mission to remote control with some automatic functions. The shore control centre (SCC) has a privileged entry point to the vessel from the outside. Access to the SCC might compromise one or more ships.

**Possible scenario:** Inappropriate segregation between the C&C network and the office network at the SCC or inappropriate control over removable media/mobile devices might compromise the C&C network, which can result in the transmission of unauthorized commands to autonomous ships or disruption of the C&C communication channel itself.

**S:** When instructions come from a hacker that spoofs the SCC – if the attacker has the encryption key for the VPN tunnel to the vessel, for example – the vessel will be unable to differentiate between legitimate and spoofed instructions.
**T:** The attacker can install malware through the C&C channel or modify the vessel's behaviour if remote updates are allowed.
**R:** If the attacker leaves traces in the SCC, it is possible to attribute an attack, but the traces of the login on the vessel will not help identify an attacker if the messages are well crafted.
**I:** The hacker will have access to all the data the SCC has access to. For example, if a vessel sends observations from its sensors directly to the SCC, the attacker will receive the same information.
**D:** An attack against the SCC does not necessarily lead to a denial of service for an autonomous vehicle. However, because of the level of automation, it still poses a danger.

**E:** Once the attacker can take over the C&C control channel, they might still need an elevation of privilege for the functionalities the SCC cannot execute from a distance. The SCC retains a large number of permissions to intervene when unexpected situations occur.

**Possible mitigations:**

- The SCC is a typical IT infrastructure with specific software to create instructions for the vessel and communicate this in a particular way. Therefore, the protection of the SCC is most similar to protection measures implemented by banks or for critical infrastructure. ISO27K series, National Institute of Standards and Technology (NIST), or similar guides the management of cybersecurity risks in this field.

## 4. DISCUSSION

Cybersecurity relates to risk assessment. Criminals attacking cargo vessels do not have the same profile as state actors who also show interest in specialized military, research, and governmental-operated vessels. Configurations of such specialized vessels can differ extensively in terms of the type and number of sensors, redundancy of subsystems, processing power, machine learning algorithms, and many other features. Thus, not all the subsystems previously mentioned need to be present, and the size and number of existing subsystems can differ significantly.

What actions a system owner takes to reduce the impact of cybersecurity attacks depends on the threat scenario, the residual risk an operator wants to assume, the threat level, the importance of the mission, their finances, and the time they have available to operationalize a vessel. Improving cybersecurity boils down to securing the complete software and hardware supply chain. Early levels of indicators of compromise (IOCs) and intelligence about advanced persistent threats (APTs) are a significant help when it comes to being informed about the threat scenario and level.

Complete autonomous ship operations have a larger cybersecurity attack surface. Still, depending on the setting, this can be acceptable since such ships have the advantage that there will be no loss of life and no way to demand ransoms when something happens to the vessel and non-existent crew.

Verification at different levels is essential to reducing the risk of the vessel being compromised:

1) Identification and authentication control: Who is allowed to access the system, and can you verify that this person is who they claim to be?
2) User control: Who is allowed to execute which commands?
3) Integrity control: Are you sure that the instructions have not been tampered with?
4) Data confidentiality control: Are you sure that adversaries cannot intercept information?
5) Restricted: Ensure everyone has access to information only on a need-to-know basis. This concept is very crucial with regard to insider threat issues.

Following our STRIDE analysis of the eight subsystems, a sea drone owner or manufacturer should take the relevant steps to improve the cyber resilience of their sea drone:

1) Analyse the system into its logical components according to Figure 4.
2) Define all the data fluxes between each system component and the external world.
3) Identify threats for each system component and function based on the operational use of the sea drone and the corresponding attackers' profiles.
4) Once the threats for each system component are identified, the STRIDE model indicates where vulnerabilities might arise. Software exists to support the technical process of finding specific vulnerabilities. For example, the Microsoft Threat Modelling Tool (MTMT) [32] implements the STRIDE framework at the software level. Open-source software, such as the open software templates building tool, inserts STRIDE threats in the generated template by searching common vulnerabilities and exposures (CVE) databases [33].
5) Take mitigation measures such as controlling information flows, adapting policies and installing control mechanisms. Implement effective mitigation strategies based on the specific discovered vulnerabilities.

## 5. CONCLUSIONS AND FUTURE WORK

Our research identified potential threats against autonomous maritime vehicles and provided a framework for their mitigation. Following that, we used the STRIDE attack model to highlight the cybersecurity aspects of sea drones and considerations

relevant to those, thus providing a solid background for manufacturers and end users willing to improve their sea drones.

We provided a framework and inventory of cyber risks for the engineers who develop sea drones and the users of sea drones. While we did not focus on the different components or parts of the sea drones, we grouped these into general but applicable subsystems to provide a foundational path towards developing detailed solutions for a specific sea drone. In our judgement, this approach fits the field best since each sea drone is a system of systems with its own individual specialized configuration.

Our research was limited to autonomous sea drones and crewed ships, depending on the level of automation. Although we focused only on technology-related measures, training people and improving processes are similarly crucial to cyber defence.

Many sea drones will soon serve as military [34] and merchant ships [35]. Our research aims to help industry and policymakers create a global ecosystem for safe and secure autonomous shipping.

## REFERENCES


[1] L. Kohnfelder and P. Garg, 'The threats to our products', Microsoft Security Development Blog, 1999. [Online]. Available: https://www.microsof t.com/security/blog/2009/08/27/the-threats-to-our-products/0Ahttps://adam.shostack.org/microsoft/The-Threats-To-Our-Products.docx

[2] S. K. Katsikas, 'Cyber security of the autonomous ship', in *CPSS 2017 – Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security, Co-located with ASIA CCS 2017*, pp. 55–56, 2017.

[3] 'Initial sea trials successfully completed by Wärtsilä & PSA Marine's ground-breaking "IntelliTug" project'. Wärtsilä. Accessed: Jan. 3, 2024. [Online]. Available: https://www.wartsila.com/media/news/13-03-2020-initial-sea-trials-successfully-completed-by-wartsila-psa-marine-s-ground-breaking-intellitug-project-3290931

[4] 'Yara Birkeland'. Yara. Accessed: Jan. 3, 2024. [Online]. Available: https://www.yara.com/news-and-media/media-library/press-kits/yara-birkeland-press-kit/

[5] 'Autonomous systems'. L3Harris. Accessed: Jan. 3, 2024. [Online]. Available: https://www.l3harris.com/all-capabilities/autonomous-systems

[6] 'The Nippon Foundation Meguri2040 fully autonomous ship program'. Nippon Foundation. Accessed: Jan. 3, 2024. [Online]. Available: https://www.nippon-foundation.or.jp/en/what/projects/meguri2040

[7] 'Uncrewed surface vessel (USV) Cetus'. University of Plymouth. Accessed: Jan. 3, 2024. [Online]. Available: https://www.plymouth.ac.uk/research/esif-funded-projects/usv-cetus

[8] 'Autoferry'. NTNU. Accessed: Jan. 3, 2024. [Online]. Available: https://www.ntnu.edu/autoferry

[9] 'Scientists launch Estonia's first autonomous maritime research vessel'. ERR. Accessed: Jan. 3, 2024. [Online]. Available: https://news.err.ee/1609117841/scientists-launch-estonia-s-first-autonomous-maritime-research-vessel

[10] N. Klein, D. Guilfoyle, M. S. Karim, and R. McLaughlin, 'Maritime autonomous vehicles: New frontiers in the law of the sea', *International and Comparative Law Quarterly*, vol. 69, no. 3, pp. 719–734, 2020.

[11] 'Saildrone launches a 72-foot autonomous seabed-mapping boat'. TechCrunch. Accessed: Jan. 11, 2024. [Online]. Available: https://techcrunch.com/2021/01/11/saildrone-launches-a-72-foot-autonomous-seabed-mapping-boat/?guccounter=2

[12] 'The navy's new autonomous ship can run by itself for 30 days'. Accessed: Jan. 11, 2024. [Online]. Available: https://www.popularmechanics.com/military/navy-ships/a43033206/navy-ship-can-operate-autonomously-for-30-days/

[13] ‘Autonomous cargo ship completes 500 mile voyage, avoiding hundreds of collisions’. Electrek. Accessed: Jan. 10, 2024. [Online]. Available: https://electrek.co/2022/05/13/autonomous-cargo-ship-completes-500-mile-voyage-avoiding-hundreds-of-collisions/
[14] B. Silverajan, M. Ocak, and B. Nagel, ‘Cybersecurity attacks and defences for un-manned smart ships’, in *Proceedings – IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, iThings/Gree*, pp. 15–20, 2018.
[15] K. S. M. Agamy, ‘The impact of cybersecurity on the future of autonomous ships’, *International Journal of Recent Research in Interdisciplinary Sciences*, vol. 6, no. 2, pp. 10–15, 2019.
[16] K. Tam and K. Jones, ‘Cyber-risk assessment for autonomous ships’, in *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*.
[17] G. Kavallieratos, S. Katsikas, and V. Gkioulos, ‘Cyber-attacks against the autonomous ship’, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 11387, pp. 20–36, 2019.
[18] G. Kavallieratos and S. Katsikas, ‘Managing cyber security risks of the cyber-enabled ship’, *Journal of Marine Science and Engineering*, vol. 8, no. 10, pp. 1–19, 2020.
[19] S. Cho, E. Orye, G. Visky, and V. Prates, *Cybersecurity Considerations in Autonomous Ships*. Tallinn: CCDCOE, 2022.
[20] H. Abdo, M. Kaouk, J.-M. Flaus, and F. Masse, ‘A safety/security risk analysis approach of industrial control systems: A cyber bowtie—combining new version of attack tree with bowtie analysis’, *Computers & Security*, vol. 72, pp. 175–195, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404817301931
[21] M. Whitman and H. Mattord, *Principles of Information Security*. Boston, MA: Cengage Learning, 2021. [Online]. Available: https://books.google.ee/books?id =Hwk1EAAAQBAJ
[22] A. Shostack, *Threat Modeling*. Nashville, TN: John Wiley & Sons, 2014.
[23] J. Meier, A. Mackman, S. Vasireddy, M. Dunner, R. Escamilla, and A. Murukan, *Improving Web Application Security*. Microsoft Corporation, 2003. [Online]. Available: https://www.microsoft.com/en-us/download/confirmation.aspx?id=1330
[24] K. H. Kim, K. Kim, and H. K. Kim, ‘STRIDE-based threat modeling and DREAD evaluation for the distributed control system in the oil refinery’, *ETRI Journal*, vol. 44, no. 6, pp. 991–1003, Nov. 2022, doi: 10.4218/etrij.2021-0181.
[25] K. Tam, K. Forshaw, and K. Jones, ‘Cyber-SHIP: Developing next generation maritime cyber research capabilities’, in *Conference Proceedings of ICMET Oman*, Muscat, Oman, Nov. 2019, doi: 10.24868/icmet.oman.2019.005.
[26] ‘Spoofed warship locations—automatic identification system (AIS)’. Popular Mechanics. Accessed: Jan. 7, 2024. [Online]. Available: https://www.popularmechanics.com/military/navy-ships/a37261561/ais-ship-location-data-spoofed/
[27] H. Pirayesh and H. Zeng, ‘Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey’, *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 767–809, 2022.
[28] E. D. Knapp and J. T. Langill, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, 2nd ed. Waltham, MA: Syngress, 2015.
[29] ‘ATLAS’. MITRE. 2021. [Online]. Available: https://atlas.mitre.org
[30] H. S. Berry, ‘The importance of cybersecurity in supply chain’, in *2023 11th International Symposium on Digital Forensics and Security (ISDFS)*, IEEE, May 2023, doi: 10.1109/ISDFS58141.2023.10131834.
[31] ‘What are supply chain attacks? Examples and countermeasures’. Fortinet. Accessed: Jan. 7, 2024. [Online]. Available: https: //www.fortinet.com/resources/cyberglossary/supply-chain-attacks
[32] ‘Microsoft threat modeling tool’. Microsoft. Accessed: Jan. 3, 2024. [Online]. Available: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool
[33] M. Da Silva, M. Puys, P. H. Thevenon, S. Mocanu, and N. Nkawa, *Automated ICS template for STRIDE Microsoft Threat Modeling Tool* (ACM International Conference Proceeding Series), 2023.
[34] ‘US Navy aims to field manned-unmanned fleet within 10 years’. Defense News. Accessed: Jan. 3, 2024. [Online]. Available: https://www.defensenews.com/naval/2023/04/12/us-navy-aims-to-field-manned-unmanned-fleet-within-10-years/
[35] Z. H. Munim and H. Haralambides, ‘Advances in maritime autonomous surface ships (MASS) in merchant shipping’, *Maritime Economics and Logistics*, vol. 24, no. 2, pp. 181–188, 2022, doi: 10.1057/s41278-022-00232-y.