CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Cybersecurity Considerations in Autonomous Ships

Sungbaek CHO
NATO CCDCOE, Researcher

Erwin ORYE
Belgium Army, Major

Gabor VISKY
NATO CCDCOE, Researcher

Vasco PRATES
NATO CCDCOE, Researcher

Tallinn 2022

CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited knowledge hub offering a unique interdisciplinary approach to the most relevant issues in cyber defence. The heart of the CCDCOE is a diverse group of international experts from military, government, academia, and industry, currently representing 38 nations.

The CCDCOE maintains its position as an internationally recognised cyber defence hub, a premier source of subject-matter expertise and a fundamental resource in the strategic, legal, operational, and technical aspects of cyber defence. The Centre offers thought leadership on the cutting edge of all aspects of cyber defence and provides a 360-degree view of the sector. The Centre encourages and supports the process of mainstreaming cybersecurity into NATO and national governance and capability, within its closely connected focus areas of technology, strategy, operations, and law.

The CCDCOE produces the Tallinn Manual, the most comprehensive guide for policy advisers and legal experts on how international law applies to cyber operations carried out between and against states and non-state actors. Since 2010, the Centre has organised Locked Shields, the biggest and most complex technical live-fire cyber defence challenge in the world. Each year, Locked Shields gives cybersecurity experts the opportunity to enhance their skills in defending national IT systems and critical infrastructure under real-time attacks. The focus is on realistic scenarios, cutting-edge technologies, and simulating the entire complexity of a massive cyber incident, including strategic decision-making and legal and communication aspects.

The CCDCOE hosts the International Conference on Cyber Conflict, CyCon, a unique annual event in Tallinn, bringing together key experts and decision makers from the global cyber defence community. The conference, which has taken place in Tallinn since 2009, attracts more than 600 participants each spring. The CCDCOE is responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance. NATO-accredited centres of excellence are not part of the NATO Command Structure

www.ccdcoe.org
publications@ccdcoe.org

Disclaimer

This publication is a product of the NATO CCDCOE (the Centre). It does not necessarily reflect the policy or the opinion of the Centre or NATO. The Centre may not be held responsible for any loss or harm arising from the use of the information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

Digital or hard copies of this publication may be produced for internal use within NATO and personal or educational use when for non-profit and non-commercial purposes, provided that copies bear a full citation.

Abstract

Autonomous transportation will profoundly change maritime traffic. Human-crewed and autonomous vessels or ships will have to share the oceans, seas, rivers and canals. As autonomous vessels can operate at various levels of autonomy or control, cybersecurity on board will vary. Autonomous maritime vehicles, surface or submarine, commercial or military, provide advantages for specific missions. Being still under development, the effects of cyberattacks on autonomous vessels are not yet apparent. It is more efficient to consider security issues in the development phase since the security-by-design principle embraces the consideration of potential threats and countermeasures at an earlier stage. The insecurity of autonomous ships could lead to environmental disasters caused by collisions with other ships and port facilities, vessel hijacking, theft or blackmail. However, relatively little attention has been paid so far to the security of autonomous vessels compared to other similar applications such as autonomous cars, drones and aircraft.

This paper provides an overview of a general framework and components of autonomous vessels and related work on their security. Then, it provides nine distinctive threat categories with explanations of scenarios and applicable countermeasures at a high level: attacks to disrupt radio frequency (RF) signals; attacks to deceive or degrade sensors; Attacks to intercept/modify communications; Attacks on Operational Technology systems; Attacks on Information Technology systems; Attacks on Artificial Intelligence used for autonomous operations; Attacks through supply chains; Attacks through physical access; and Attacks on the Shore Control Centre. As the concept and technology related to autonomous vessels are still evolving, identification and determination of detailed specific countermeasures at this stage are not feasible. Moreover, detailed countermeasures will be different by application and the targeted level of autonomy. Nevertheless, potential threat scenarios and high-level considerations of countermeasures would help ship engineers, owners and operators identify and implement security functionalities essential for autonomous vessels.

1. Introduction

Autonomous vessels are highly automated, using state-of-art Information Technology (IT) and data analysis techniques and onshore monitoring and control bases connected through telecommunications. They automatically carry out part of or all of the on board tasks associated with ship operations, including observing its surroundings, monitoring equipment status, manoeuvring, engine control, cargo management and loading, docking and undocking.[1] There are many initiatives to develop autonomous vessels around the globe, some examples being Mayflower,[2] YARA Birkeland,[3] AAWA[4] and KASS.[5] Autonomous vessels provide certain advantages over conventional vessels. Their crewlessness can save operational costs, reduce pollution and reduce accidents resulting from human errors or mistakes. It can also enable vessels to be dispatched for dangerous missions.

Technological progress has changed the way of human operations in the maritime sector. Owing to the integration of more comprehensive situational awareness capabilities inside and outside the ship, smaller crews may carry out the same missions which previously required more people. Linking its position, navigation and timing (PNT) services by Global Navigation Satellite System (GNSS) signals, being aware of other vessels through Automatic Identification Systems (AIS) and plotting the collected information on the Electronic Chart Display and Information Systems (ECDIS) are typical examples of such progress. On top of these technologies, autonomous vessels will have better capabilities to navigate autonomously by using artificial intelligence and machine learning (AI/ML) and real-time maritime situational awareness through sensors to recognise current ship position, status and surroundings. AI/ML could also be used to detect, mitigate and compensate for the partial degradation of sensors by comparing and integrating sensor inputs while purging unreliable or suspect inputs intelligently to continue to operate reliably even under adverse conditions.

Most autonomous vessels will have communication capabilities to communicate with a home base, allowing a Shore Control Centre (SCC) to receive status data and send control instructions. This Command and Control (C2) communication link will be necessary for the SCC to remotely monitor vessel status and take control by overruling the autonomous functions in the event of an emergency or significant functional failure. In addition, some vessels may have a data link to send telemetric or image data collected by the vessels back to the SCC. They may also have an internet connection to collect and download open-source information such as global marine traffic status and climate forecasts. The C2 and data links would be implemented by combinations of technologies such as cellular, satellite, VHF, UHF and Wi-Fi depending on communication distances and data transfer rates. For example, navigation in a harbour area needs more and faster communications with the SCC to monitor traffic and avoid collisions. In specific applications such as military autonomous submarines and operations in communication blind spots, the C2 communication may not be continuously available for fully

[1] Koji Wariishi, 'Maritime Autonomous Surface Ships Development Trends and Prospects,' Mitsui Global Strategic Studies Institute Monthly Report, September 2019, https://www.mitsui.com/mgssi/en/report/detail/__icsFiles/afieldfile/2020/01/09/1909t_wariishi_e.pdf.

[2] 'Mayflower Autonomous Ship - Transatlantic Mission Overview and Status Update,' IBM, https://newsroom.ibm.com/Mayflower-Autonomous-Ship-Transatlantic-Mission-Overview-and-Status-Update, [Accessed 24 January 2022].

[3] 'Autonomous Ship Project, Key Facts about Yara Birkeland,' Kongsberg, https://www.kongsberg.com/maritime/support/themes/autonomous-ship-project-key-facts-about-yara-birkeland, [Accessed 24 January 2022].

[4] 'Remote and Autonomous Ships - The Next Step,' Rolls-Royce, 21 June 2016, https://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/aawa-whitepaper-210616.pdf.

[5] 'Korea Autonomous Surface Ship Project – Project Detail,' Korea Research Institute of Ships & Ocean Engineering, https://kassproject.org/en/info/projectdetail.php, [Accessed 24 January 2022].

autonomous vessels because they would be designed to operate without any human intervention in radio silence to avoid detection.

However, heavy dependency on technology inevitably increases the vessel's presence in cyberspace, increasing its attack surface and the chances of being targeted and offering new vectors for such attacks.[6] The cyberattack surface of autonomous vessels will be closely related to the level of autonomy of the vessel since the attack surface varies with the complexity of and dependency on the number of systems and human interfaces to control, monitor and overrule the vessels. On levels of autonomy, International Maritime Organisation (IMO) has proposed four levels for the scoping exercise:[7]

- Degree 1 (Ship with automated processes and decision support): Seafarers are on board to operate and control shipboard systems and functions. Some operations may be automated but with seafarers on board ready to take control.
- Degree 2 (Remotely controlled ship with seafarers onboard): The ship is controlled and operated from another location. Seafarers are available onboard to take control and operate the shipboard systems and functions.
- Degree 3 (Remotely controlled ship without seafarers onboard): The ship is controlled and operated from another location. There are no seafarers on board.
- Degree 4 (Fully autonomous ship): The ship operating system can make decisions and determine actions by itself.

The commercialisation of unmanned (Degree 3) or fully autonomous (Degree 4) vessels is not expected until the 2030s and 2040s, respectively.[8] However, security risks associated with the operation of these vessels should be considered from the conceptualisation and design phases to enable security-by-design principles with a full grasp of potential security implications and possible countermeasures. Cybersecurity is also important, even with the Degree 1 and Degree 2 ships since some functionalities of these vessels will also be heavily dependent on IT and onboard seafarers are unlikely to be IT or security specialists.

[6] Kevin Jones, Kimberly Tam and Maria Papadaki, 'Threats and Impacts in Maritime Cyber Security,' Engineering & Technology Reference, 22 April 2016, doi:10.1049/etr.2015.0123.
[7] 'MSC 100/20/Add.1 Annex 2: Framework for the Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (MASS),' International Maritime Organization, June 2019, https://maiif.org/wp-content/uploads/2019/06/MSC-100_20-Annex-20-1.pdf.
[8] Koji Wariishi, 'Maritime Autonomous Surface Ships Development Trends and Prospects.'

2. Architecture and Use Cases

The concept of autonomous vessels is still new and it is difficult to be certain what security risks may exist in the vessels. Therefore, it is worth looking at the technological architecture and use of autonomous vessels to help identify and discuss potential threats and countermeasures. This section provides an overview of technologies for autonomous vessels and how the vessels could be used for commercial and military purposes.

2.1 Major Components and Core Technologies

The project 'Maritime Unmanned Navigation through Intelligence in Networks' (MUNIN), a collaborative research project by eight organisations from 2012 to 2015 co-funded by the European Commission, identified the main modules/components of an autonomous ship as follows.[9,10]

- Advanced Sensor Module (ASM): This comprises radar, video and other systems for lookout, object detection and generally sensing the ship's environment.
- Integrated Bridge System (IBS): This comprises all bridge systems and equipment related to the navigation of the ship. The name 'bridge' implies that its basic functionality is somehow equivalent to a physical bridge found on ships today.
- Engine/Automation Systems (EAS): It comprises all systems related to power generation and propulsion. The MUNIN project also assumed that it would also include automation related to safety systems, life support, ballast and cargo control, etc.
- Autonomous Ship Controller (ASC) is the additional control and monitoring functions to enable autonomous operation. It includes an 'Autonomous Engine Monitoring and Control' (AEMC) function and the 'Autonomous Navigation System' (ANS) modules. It also includes communication management functions for all communication between the vessel and the SCC through the Communications Controller.
- The Dedicated Line-of-Sight Communication Systems communicates with other ships and shore facilities including Vessel Traffic Management Information System (VTMIS), and Maritime Rescue Coordination Centres (MRCC). It comprises AIS, VDES (VHF Data Exchange System, the 2nd generation of AIS using satellite communications) and GMDSS (Global Maritime Distress and Safety System, the mandatory emergency signal communication system).
- The Rendezvous Control Unit is a system that allows an Onboard Control Team to take control of the ship temporarily or an Emergency Control Team to recover the vessel during a breakdown.
- The SCC contains all onshore functions to handle an autonomous ship. It also includes remote bridge and engine control modules that can be used to directly control the ship. Initial voyage planning would be performed from the SCC.

[9] 'D4.5: Architecture Specification,' The MUNIN Project Deliverable, 8 February 2014, http://www.unmanned-ship.org/munin/wp-content/uploads/2014/02/d4-5-architecture-v11.pdf.

[10] 'D8.6: Final Report: Autonomous Bridge,' The MUNIN Project Deliverable, 6 August 2015, http://www.unmanned-ship.org/munin/wp-content/uploads/2015/09/MUNIN-D8-6-Final-Report-Autonomous-Bridge-CML-final.pdf.

Figure 1 shows an overview of high-level modules comprising an autonomous ship.[11]

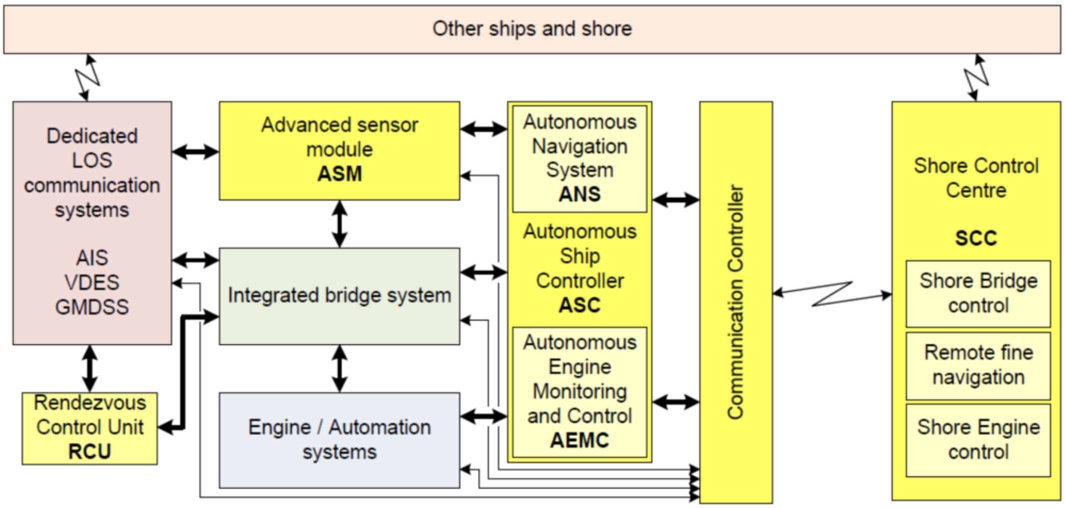

FIGURE 1. OVERVIEW OF HIGH-LEVEL MODULES

Wang et al. (2020) identified a list of core technologies required for an autonomous ship, as shown in Table 1.[12]

TABLE 1. CORE TECHNOLOGIES FOR AUTONOMOUS VESSELS

Core Technologies	Description
Gyroscope	Senses the ship’s movements, indicating average and peak movement around three axes, and also vibrations.
Intelligent Awareness	Relies on advanced sensors on board that monitor for hazard detection and avoidance and situational awareness, such as automated surveillance cameras and accelerator sensors.
Sensor Fusion	Monitors, evaluates and processes individual sensor data to improve sensors' output.
Route Planning	Global route planning relies on static obstacle information of the sea area. Local route planning is based on sensor information to determine the optimal route.
Collision Avoidance	Includes obstacle detection, tracking and motion estimation to ensure safe navigation.
Communications	Includes LF, HF, VHF/UHF, satellite, Celular3G/4G/5G.
Autonomous Navigation	Different technologies such as satellite navigation (based on GNSS and Differential GNSS), dead reckoning (a method to obtain the track and position of a vessel based on speed, heading, water current, etc.), inertial system (a way to determine speed and position using accelerometers) and multi-sensor navigation (using radar information in addition to other sensor information) may be employed for autonomous navigation.
Energy Control	Uses energy control algorithms to optimise efficiency.
Status Monitoring System	Monitors the status of a crewless ship.
Fault Diagnosis System	Diagnoses faults quickly and effectively to prevent and reduce accidents.
Cargo Supervision System	Identifies the positioning and management of the cargo. Cargo can be a sensor, a weapon system, people, containers, etc.

[11] Ibid.
[12] Jia Wang, Yang Xiao, Tieshan Li and C. L. Philip Chen, ‘A Survey of Technologies for Unmanned Merchant Ships,’ IEEE Access, Vol. 8, pp. 224461-224486, 2020, doi: 10.1109/ACCESS.2020.3044040.

Emergency Response System	Transmits the situation of a ship in real-time when in danger for response action from the SCC.
LiDAR System	Detects targets by emitting laser waves and receiving the reflected echo for collision avoidance, location and navigation.
Radar System	Detects targets by emitting electromagnetic waves and receiving the reflected echo for collision avoidance, location and navigation.
Dynamic Positioning	Provides data to maintain the position of the vessel using the propellers without anchoring.
Strain Gauge	Measures and monitors the strain of a ship and equipment.
ECDIS	Provides digital layered charts fused with ship positions to assist decision-making for navigation.
Iceberg Tracking	Icebergs can be detected by radar and sonar.
AIS Transponder	Gives situational awareness of other vessels in the vicinity, but it is a collaborative system.
Remote Human Vision	Monitors and intervenes from the SCC in crewless ships.
AI/ML	Path tracking and planning using a set of sensor inputs.
Edge Computing	Autonomous ships need to perform a complex set of calculations on a real-time basis with low latency.

2.2 Network Architecture

Studies on the detailed network architecture of autonomous vessels have yet to be published. However, in the field of general unmanned ships, Rødseth and Tjora (2014)[13] presented a detailed network architecture decomposed into several layers, as shown in Figure 2. Although 'autonomous' and 'unmanned' are different concepts, their study can provide some insight into the network architecture of autonomous ships.

In Figure 2, the Instrument Layer at the bottom consists of navigational sensors such as the gyro, AIS and GNSS required for navigational awareness, internal automation sensors such as those for pressure, temperature, torque and vibration, and associated actuators for machinery operations of the ship. These various sensors and actuators will then be grouped by their roles at the Process Layer and connected to system components in the Integrated Ship Control Layer, where essential operations of the ship take place. The General Ship Layer on the top of the Integrated Ship Control Layer is where additional administrative activities such as reporting and record-keeping are performed. At the top of the architecture is the Off Ship Layer, which provides capabilities for communications with external parties, including the SCC. This architectural view is similar to the Purdue reference model[14] which has been widely used to represent generic Industrial Control Systems (ICS), except that there are no human-machine interfaces.

[13] Ørnulf J. Rødseth and Åsmund Tjora, 'A System Architecture for an Unmanned Ship,' The 13th International Conference on Computer and IT Applications in the Maritime Industries (COMPIT 2014), pp. 291-302, May 2014.
[14] Theodore J. Williams, 'The Purdue Enterprise Reference Architecture,' Computers in Industry, Vol. 24, No. 2, pp. 141-158, 1994.

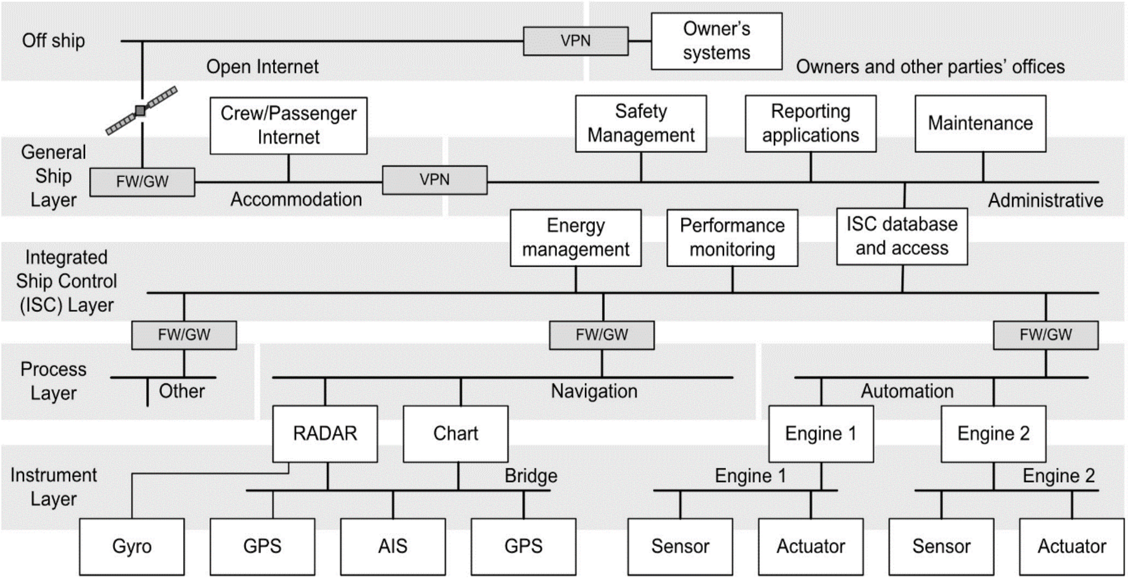

FIGURE 2. ARCHITECTURAL OVERVIEW OF UNMANNED SHIPS

The architecture yields four distinctive types of network as follows.[15]

- Navigational Network: In principle, it should be based on communication protocols standardised by the International Electro-technical Commission (IEC), the standard body for navigation devices. Conventional IEC 61162-1/2 (based on RS422) or IEC 61162-3 (based on Controller Area Network buses) standards may not be appropriate for navigational networks of an autonomous vessel due to limitations in speed, connectivity and security. The ethernet-based IEC 61162-450, more advanced 61162-460 and their successors will be used instead.
- Automation and Safety Network: It is connected to sensors and actuators to control and monitor the vessel and therefore constitute the Operational Technology (OT) network. There are so far no mandatory communication protocols for OT parts of vessels such as engine control. Communication protocols often used in ICS such as Modbus and OPC Unified Architecture may be used for the automation and safety networks. It will be able to interface with IEC 61162-460-compliant components at the application level.
- Line-of-Sight Network: This network is to control and monitor the vessel near the coast. It may be primarily based on VHF channels. High-speed mobile communications may also be considered for some operations requiring intensive communication with the SCC such as berthing and manoeuvring around ports. However, mobile communications have limitations in range and therefore may not be sufficient to control the vessels from a long distance.
- Ship-to-Shore Network: For communications far beyond the line-of-sight, typical transmission means between vessel and SCC will be based on satellite communications such as Inmarsat, Iridium and Very Small Aperture Terminal (VSAT).

In addition to these specific networks, other networks may exist depending on the purpose and use of the autonomous vessel. For example, environmental monitoring and military surveillance missions would require additional data transmission capabilities in addition to C2 communications. This data link typically requires a higher rate and lower latency than traditional C2 links. In missions using unmanned submarines and buoys, additional means of communication may exist. Submarines may use unique communication means such as acoustic modems, optical fibre spools and laser devices to communicate with buoys or ships on the surface. Relay points such as buoys and ships may use a variety of communication options such as UHF, VHF, MF, HF and satellite communications to communicate with the SCC or other relay points. Underwater or surface sensor networks may also be used to monitor and control autonomous vessels. Typical applications of sensor networks are also used with marine environmental monitoring such as water quality, coral reef monitoring and fish farm management.[16]

[15] Rødseth and Tjora, 'A System Architecture for an Unmanned Ship.'
[16] Guobao Xu, Weiming Shen and Xianbin Wang, 'Applications of Wireless Sensor Networks in Marine Environment Monitoring: A survey,' Sensors, Vol. 14, No. 9, pp. 16932-16954, 2014, doi: 10.3390/s140916932.

Future sensor networks may also be used to receive positional and status data of vessels and transmit commands as a backup means for mission or safety-critical operations such as manoeuvring in harbour areas. Internal systems of autonomous vessels could also be configured to use wireless networks rather than a wired bus network or ethernet as wireless networks have several advantages such as low implementation cost and flexible layout.[17]

2.3 Uses

The use of autonomous vessels will be dependent on a variety of factors related to cost and safety.[18] There are several costs associated with operating a vessel of any sort, including the capital cost of vessels and control centres, operating costs for repairs and maintenance, voyage cost for fuel and port fees and revenue to be expected from the operation of vessels. Safety factors consider the well-being of the crew and passengers, the value of the vessel and assets onboard, the well-being of people outside the vessel, the value of assets external to the vessel and environmental impact. As there are no clear estimates for the costs related to the procurement and operation of autonomous vessels, it is difficult to predict which use cases will be realised in the future.

Although Degree 3 or Degree 4 unmanned autonomous cargo ships and passenger ships will undoubtedly be technically feasible in the future, these uses may not be commercially viable, and the unmanned operation of cargo or passenger ships may not be permitted by IMO or national maritime regulatory bodies which may require a certain number of crew members on board for safety reasons. However, this does not invalidate the usefulness or value of autonomous vessels since they can still reduce the size of the crew and potential human error. The onboard crews will be in charge of safety and take control in emergencies, while voyage and manoeuvring will be mainly based on autonomous capabilities.

Autonomous vessels could also be actively engaged in dangerous tasks that could result in human casualties, such as ocean environmental surveys in adverse climate conditions and a variety of military operations. For military use, Savitz et al. (2013)[19] considered ten main mission categories: C4ISR;[20] military deception, information operations and electronic warfare; surface warfare; mine warfare; anti-submarine warfare (ASW); logistics; ground attack; air and missile defence (AMD); supportive functions; and other not missions currently being performed (see Table 2).

Humanitarian operations such as the delivery of supplies and the rescue and evacuation of civilians can also be carried out by autonomous vessels. However, there is a lack of clarity over whether government or military-owned and operated autonomous vessels would be regarded as warships and other government ships for non-commercial purposes under the UN Convention on the Law of the Sea (UNCLOS) that gives sovereign immunity to such vessels, preventing their seizure by other states.[21]

[17] Wang et al., 'A Survey of Technologies for Unmanned Merchant Ships.'

[18] Bjørn J. Vartdal, Rolf Skjong and Asun L, St. Clair, 'Remote-Controlled and Autonomous Ships in the Maritime Industry,' DNV, 2018, https://www.dnv.com/maritime/publications/remote-controlled-autonomous-ships-paper-download.html.

[19] Scott Savitz, Irv Blickstein, Peter Buryk, Robert W. Button, Paul DeLuca, James Dryden, Jason Mastbaum, Jan Osburg, Phillip Padilla and Amy Potter, 'U.S. Navy Employment Options for Unmanned Surface Vehicles (USVs),' RAND Corporation, 2013, https://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR384/RAND_RR384.pdf.

[20] Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance.

[21] Natalie Klein, Douglas Guilfoyle, Saiful Karim and Rob McLaughlin, 'Maritime Autonomous Vehicles: New Frontiers in The Law of The Sea,' International & Comparative Law Quarterly, Vol. 69, No. 3, pp. 719-734, 2020, doi: 10.1017/S0020589320000226.

TABLE 2. POTENTIAL NAVAL MISSIONS FOR AUTONOMOUS VESSELS

Category	Detailed Applications
C4ISR	Persistent ISR in permissive environments; Environmental collection in permissive environments; ISR in hostile environments; Unmanned surface vehicles with tethered unmanned undersea vehicles to deploy sensors or networks; Environmental collection in hostile environments; Processing, exploitation and dissemination; Communications relay; Deploy individual sensors; Deploy independent sensor network.
Military Deception /Information Operations/ Electronic Warfare	Disposition/intentions deception; Communications/signals deception; Radar/ signals deception; Acoustic/signals deception; Decoy/countermeasures; Military information support operations; Tactical jamming; Disguised mission; Info systems (cyber/tech); Computer network attack; Diversion.
Surface Warfare	Armed escort; Counter fast attack craft (fully autonomous); Counter fast attack craft (remote control); Presence patrol; Open-water ship-vs.-ship conflict; Countering swarms.
Mine Warfare	Mine countermeasures intelligence preparation of the battlespace; Re-acquisition mine hunting and neutralisation; Autonomous in-stride mine hunting and neutralisation; Mechanical mine sweeping and mine harvesting; Influence mine sweeping; Minefield proofing; Mine laying support.
ASW	Unarmed ASW area sanitation; Act as an ASW sensor node; Cued overt ASW tracking; Armed wartime ASW area sanitation; Uncued covert ASW tracking; Cued covert ASW tracking; Cued/uncued ASW engagement.
Logistics	Unmanned vehicle support; Autonomous ship-to-shore connector; Opposed amphibious landing resupply; Covert/clandestine special operations forces (SOF) cargo delivery; Unmanned Vehicle refuelling; Resupply for manned ships; Military interdiction operations support.
Ground Attack	Short/medium-range ground attack; Long-range ground attack (arsenal ship, optionally manned).
AMD	Sensing and warning - unit level; Sensing and warning - force level; Non-kinetic unit defence; and, AMD kinetic force defence (using projectiles or directed energy).
Supportive Functions	Search and rescue of conscious victims; Complex search and rescue; Test platform; Training support.
Not Currently Performed Missions	Blockship operations/port detonations; Deliberately allowing capture; Impairing adversary sensors; Provocative high-risk presence; Vehicle as a surface weapon.

3. Related Work in Maritime Cybersecurity

In 2016, the IMO officially recognised the importance of cybersecurity in that security breaches have the potential to do considerable harm to the safety and security of ships, ports and marine facilities. It issued a temporary risk management guideline (MSC.1/Circ.1526), which was superseded by a formal guideline MSC-FAL.1/Circ.3[22] the next year. In 2017, it adopted Resolution MSC.428(98)[23] requiring member states to apply a cybersecurity risk management approach to the safety management systems of ships. These documents only provide high-level principles without detailed information on securing and protecting ships but they are significant progress towards achieving and improving cybersecurity in the marine sector.

In Europe, EU Directive 2016/1148 on the security of network and information systems (the NIS Directive) recognised the importance of maritime cybersecurity and identified maritime operators, including passenger and freight water transport companies, and the managing bodies of ports and operators of vessel traffic services as 'Operators of Essential Services' (OES) and invited them to beef up the level of their cybersecurity.[24] Several cybersecurity reports and guidelines have also been published by the European Union Agency for Cybersecurity (ENISA) for maritime security. In 2011, it published the first EU report on cybersecurity challenges in the maritime sector[25] and, in 2019, a second focusing on security for port authorities and terminal operators with a list of potential threats and security recommendations,[26] followed by a more detailed risk management guideline for port security in 2020.[27]

Regarding the risk management of ship onboard systems, the Baltic and International Maritime Council (BIMCO), together with other leading shipping organisations, published detailed cybersecurity guidelines in 2016, and the latest version was published in 2020.[28] UK Department for Transport also published the Code of Practice for Cyber Security for Ships, which is similar to the BIMCO guidelines but described at a little more general level.[29] The BIMCO guidelines provide explanations of critical onboard systems and associated risks:

- Cargo and loading management systems: These systems are used to load, manage and control cargo. They may interface with various systems ashore and include shipment tracking tools available to shippers via the internet. Such interfaces make the systems and data vulnerable.
- Bridge systems: The increasing use of digital navigation systems with an interface to shoreside networks for the updating and provision of services makes such systems vulnerable. Stand-alone systems not connected to other networks may be equally vulnerable as removable media are often used for updates.
- Propulsion and machinery management and power control systems: These systems are used to monitor and control onboard machinery, propulsion and steering. The vulnerability of these

[22] 'MSC-FAL.1/Circ.3: Guidelines on Maritime Cyber Risk Management,' International Maritime Organization, 4 July 2017, https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.

[23] 'Resolution MSC.428(98): Maritime Cyber Risk Management in Safety Management Systems,' International Maritime Organization, 16 June 2017, https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.

[24] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union, 19 July 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148.

[25] 'Cyber Security Aspects in the Maritime Sector,' European Union Agency for Cybersecurity, 19 December 2011, https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1.

[26] 'Port Cybersecurity - Good Practices for Cybersecurity in the Maritime Sector,' European Union Agency for Cybersecurity, 26 November 2019, https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector.

[27] 'Guidelines - Cyber Risk Management for Ports,' European Union Agency for Cybersecurity, 17 December 2020, https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports.

[28] 'The Guidelines on Cyber Security Onboard Ships - Version 4,' Baltic and International Maritime Council, 23 December 2020, https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships.

[29] 'Code of Practice: Cyber Security for Ships,' UK Department for Transport, 13 September 2017, https://www.gov.uk/government/publications/ship-security-cyber-security-code-of-practice.

systems increases when used in conjunction with remote monitoring and integration with navigation and communications equipment on ships for integrated bridge systems.

- Access control systems: These systems support access control to ensure the physical security and safety of a ship and its cargo, including surveillance, security alarms and personnel-on board tracking systems. They can be vulnerable to cyberattack.
- Passenger servicing and management systems: These systems may hold valuable passenger-related data. Intelligent devices. Devices used for passenger services such as tablets can be an attack vector.
- Passenger-facing public networks: Fixed or wireless networks connected to the internet installed on board for the benefit of passengers should not be connected to any safety-critical system on board.
- Administrative and crew welfare systems: Onboard computer networks used for administration of the ship or the crew's welfare are vulnerable when providing internet access and email.
- Communication systems: Availability of internet connectivity via satellite and other wireless communication increases the vulnerability of ships and VSAT signals are vulnerable to exploitation.

The IMO and BIMCO guidelines aim to provide a general understanding of cybersecurity and risk management to ship owners and operators. There is little detail on risks and mitigation measures specific to onboard systems, although the BIMCO guidelines include an annex listing onboard systems, equipment and technologies that should be considered for risk management. Cybersecurity is much more critical for autonomous vessels considering the levels and forms of autonomy directly related to their heavy reliance on ICT for ship control, the increased integration of control systems, the increased connectivity with the SCC at any time anywhere and the possible accessibility of such systems to the internet.[30] However, little attention has so far been paid to the cybersecurity of autonomous vessels.

Research by Silverajan et al. (2018)[31] was probably the first work to consider various types of potential cybersecurity threats to autonomous vessels. The authors identified seven attack vectors that attackers could exploit: positioning systems; sensors; firmware upgrades; voyage data recorders (devices similar to the black box on aeroplanes); intra-vessel networks; vessel-to-land communications including satellite and cellular; and remote systems on the vessel accessible from the SCC. They also identified attack types applicable to these surfaces: malicious code injection by network infiltration, removable devices or firmware update; tampering or modification of intra-vessel network packets; GNSS spoofing; AIS spoofing; signal jamming against GNSS and various sensors; and eavesdropping and disruption of the communication link between the vessel and SCC. Agamy (2019)[32] argued that typical threat scenarios to autonomous ships would be: removable devices inserted into the onboard system; taking control of the vessel through a communication link; GNSS jamming; blocking communications between the vessel and the SCC; and GNSS spoofing. However, these works did not cover the full spectrum of threats to autonomous vessels and how to mitigate them. Regarding administrative and technical security requirements for autonomous or unmanned ships, Kavallieratos et al.[33] proposed a broad range of security controls similar to ISO/IEC 27001 in 13 categories: human resource security, asset management, access control, cryptography, physical and environmental security, operations security,

[30] Sokratis K. Katsikas, 'Cyber Security of the Autonomous Ship,' The 3rd ACM Workshop on Cyber-Physical System Security, pp. 55-56, 2017, doi: 10.1145/3055186.3055191.

[31] Bilhanan Silverajan, Mert Ocak and Benjamin Nagel, 'Cybersecurity Attacks and Defences for Unmanned Smart Ships,' 2018 IEEE International Conference on Internet of Things/IEEE Green Computing and Communications/IEEE Cyber, Physical and Social Computing/IEEE Smart Data, pp. 15-20, 2018, doi: 10.1109/Cybermatics_2018.2018.00037.

[32] Kazem. 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.

[33] Georgios Kavallieratos, Vasiliki Diamantopoulou and Sokratis K. Katsikas, 'Shipping 4.0: Security Requirements for the Cyber-Enabled Ship,' IEEE Transactions on Industrial Informatics, Vol. 16, No. 10, pp. 6617-6625, 2020, doi: 10.1109/TII.2020.2976840.

communication security, system acquisition, development and maintenance, supplier relationships, incident management, business continuity management and compliance.

For risk assessment and management of autonomous vessels, Tam and Jones (2018)[34] proposed a high-level risk assessment approach to measure the risks associated with seven onboard systems or components of an autonomous vessel. These were AIS, GNSS, automated mooring systems, cargo management systems, radar, sensors and voyage data recorders and the threats were theft, damage, denial of service, obfuscation and misdirection. Similarly, Kavallieratos et al. (2018)[35] deconstructed an autonomous vessel into fourteen systems: engine automation; bridge automation; SCC; AEMC; engine efficiency; maintenance interaction; navigation; ASC; human-machine interface; remote manoeuvring support; emergency handling system; AIS; ECDIS; and GMDSS. They identified threat scenarios for each system: spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege (STRIDE). They later[36] extended the STRIDE concept by adding components such as collision avoidance, radar, CCTV, advanced sensor modules and autopilot systems. These works, along with the list in the BIMCO guidelines, help identify systems and components of an autonomous vessel that should be considered for risk management. However, the risk assessments were performed at a high level and did not provide detailed scenarios on how systems or components could be compromised.

While functional failures of sensors and equipment are not the same as cyberattacks, the reliability issue is of paramount importance for unmanned vessels since a single fault could lead to the inability to manoeuvre or the complete loss of communications on the high seas. Therefore, autonomous vessels must be fault-tolerant enough to minimise the effect of faults. Blanke et al. (2017)[37] defined six levels of redundancy from Level 0 to Level 5: Level 0 is no redundancy, whereas Level 5 is when all main functions are double- or triple-redundant so that no single fault prevents navigation, safe monitoring or complete standard propulsion.

4. Threats and Countermeasures

Autonomous vessels have advantages including reduced operating costs such as labour and eliminating human casualties in dangerous missions such as minesweeping, or the performance of tasks that are not possible with humans on board. However, the nature of autonomous operations increases the attack surface for cyber and physical attacks. In particular, taking control of autonomous ships could result in disaster. Adversaries may hack into autonomous ships, alter the ship's route and launch a 'suicide' attack, steal the cargo, capture the vessel for financial extortion, or capture autonomous ships to steal the ship's technologies or weapon systems.

In this paper, significant threats surrounding the autonomous vessels are classified into nine categories. They are attacks to disrupt RF signals; deceive or degrade sensors; intercept or modify communications;

[34] Kimberly Tam and Kevin Jones, 'Cyber-Risk Assessment for Autonomous Ships,' 2018 International Conference on Cyber Security and Protection of Digital Services, pp. 1-8, 2018, doi: 10.1109/CyberSecPODS.2018.8560690.
[35] Georgios Kavallieratos, Sokratis Katsikas and Vasileios Gkioulos, 'Cyber-Attacks against the Autonomous Ship,' 2018 International Workshop on the Security of Industrial Control Systems and Cyber-Physical Systems, pp. 20-36, 2018, doi: 10.1007/978-3-030-12786-2_2.
[36] Georgios Kavallieratos and Sokratis Katsikas, 'Managing Cyber Security Risks of the Cyber-Enabled Ship,' Journal of Marine Science and Engineering, Vol. 8, No. 10, pp. 1-19, 2020, doi: 10.3390/jmse8100768.
[37] Mogens Blanke, Michael Henrique and Jakob Bang, 'A Pre-Analysis on Autonomous Ships,' Technical University of Denmark Technical Report, 2017, https://www.dma.dk/Documents/Publikationer/Autonome%20skibe_DTU_rapport_UK.pdf.

OT systems; damage IT systems; damage AI used for autonomous operations; compromise supply chains; give physical access; and damage the SCC.

Attacks to Disrupt RF Signals

Jamming of RF signals can disrupt communications. Most autonomous vessels have a communication channel with their SCC. When the distance between the vessel and the SCC is relatively small, direct communication using VHF/UHF, cellular or Wi-Fi can be possible. For greater distances, it is necessary to relay it through satellites, buoys, other ships, aircraft or submarines. Each frequency band and communication protocol has its own strengths and weaknesses, but they are all prone to denial of service attacks. There has been much study of jamming and anti-jamming techniques against RF signals.[38] Jamming RF signals by sending out more powerful signals than the communication channel's signal strength is not new. Specialists often catalogue this under electronic warfare (EW) instead of cybersecurity. With digitalised autonomous transportation, jamming could be used in a way that would confuse an initial assessment of its vector, EW or cyberattack. For aerial drones, there are already jammer devices or services commercially available as anti-drone equipment. It will be only a matter of time before the same is available for autonomous vessels.

Satellite signal jamming is relatively easy if the transmitter is in the antenna coverage of the satellite. As most communication satellites simply receive an incoming signal, amplify it and send it back to the earth on a different frequency, there is no filtering of the content of the information on the satellite.[39] GNSS signals are also vulnerable to jamming attacks. So far, there have been many GNSS jamming incidents around the globe, including the significant GPS interference at the eastern and central Mediterranean Sea, the Persian Gulf and multiple Chinese ports in September 2020.[40] Those attacks can have severe consequences, especially when the vessel relies completely on GNSS for determining its position.

Various techniques offer some level of mitigation against RF jamming attacks. These include channel hopping, spectrum spreading, multiple-input multiple-output (MIMO) based mitigation, channel coding, rate adaptation and power control.[41] The use of adaptive antenna arrays, algorithms to detect or prohibit immediate jumps in location and time, inertial navigation systems, algorithms to filter out interfered frequency bands and the use of eLoran (a low-frequency radio navigation system) receivers as a backup can help overcome the interference.[42] Using multiple constellations including GPS (US), QZSS (Japan), BEIDOU (China), GALILEO (EU), GLONASS (Russia) and IRNSS/NAVIC (India) may also provide a better defence against GNSS jamming or spoofing than using a single one. However, it does not provide complete protection because attackers who can jam or spoof one of the constellations successfully will be able to do the same for the others. Autonomous vessels need to have a self-recovery capability in case of loss of communications or position sensing. These may vary depending on the type and circumstances of the disruption, but one option could be to continue sailing using a gyrocompass and accumulated voyage logs. Another could be to return to a predefined location using the same means if the disruption lasts longer than a certain period. When the vessel is in a hazardous area and its position cannot be ascertained, stopping the vessel could be considered the best option.

[38] Kanika Grover, Alvin Lim and Qing Yang, 'Jamming and Anti-jamming Techniques in Wireless Networks: A Survey,' International Journal of Ad Hoc and Ubiquitous Computing, Vol. 17, No. 4, pp 197-215, 2014, doi: 10.1504/IJAHUC.2014.066419.

[39] Pavel Velkovsky, Janani Mohan and Maxwell Simon, 'Satellite Jamming,' Project on Nuclear Issues by the Center for Strategic and International Studies, 3 April 2019, https://ontheradar.csis.org/issue-briefs/satellite-jamming.

[40] 'MSCI Advisory 2020-016-Various-GPS Interference,' U.S. Department of Transportation, 22 September 2020, https://www.maritime.dot.gov/msci/2020-016-various-gps-interference.

[41] Grover et al., 'Jamming and Anti-jamming Techniques in Wireless Networks: A Survey.'

[42] 'Jamming and Spoofing of Global Navigation Satellite Systems (GNSS),' INTERTANKO, 2019, https://www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf.

Attacks to Deceive or Degrade Sensors

Attack to deceive or degrade sensor data can also occur to the sensors used for identifying ship locations and obstacles such as GNSS, radar, optic sensors, ultrasonic and acoustic sensors. GNSS spoofing is about sending a counterfeit signal to a receiver antenna from a radio transmitter. While GNSS jamming appears to be the more significant threat, GNSS spoofing delivers a sucker punch to various applications since the fake GNSS feeds cause drivers, ship captains and other operators to go off course without any coercion.[43] After demonstrating drone hijacking with GNSS spoofing in 2012, the University of Texas showed a yacht hijacking after a year. More recently there was a hijacking demonstration of the Tesla Model 3's Navigate on Autopilot (NOA) system by an Israeli security company.[44] Although military-grade GNSS signals are protected by encryption against manipulation, signals used for commercial applications are not encrypted yet and therefore manipulation can remain undetected.

Sensors located outside an autonomous vessel can be attractive targets for attackers since they do not need physical access inside the vessel. If sensors use wireless signals to transmit the sensory data, they can directly be victims of RF jamming. Attackers also can launch attacks to degrade the sensors that deliver inputs for autonomous functionalities. A straightforward example is blocking a camera from taking pictures by using a projector that emits a narrow beam of white light directly at a charge-coupled device (CCD) of the camera, making the camera's electronics constantly adjust and ultimately producing large white splotches.[45] Acoustic signals for underwater communications and sonar images for underwater scanning are also prone to attacks that use acoustic sounds to make noises. Navies widely use acoustic countermeasure devices (ADCs) to confuse torpedoes.[46] These devices are examples of ways to interfere with acoustic signals. Like RF jamming, radar jamming or deception can degrade the effectiveness of radar systems by emitting noise or false information with the same frequency.[47]

AIS is one of the sources of maritime situational awareness and traffic monitoring. It suffers from a problem of trustworthiness of messages because a shutdown or misinformation about the vessel's current status or a faulty installation or configuration is possible.[48] Besides these human-related risks, the VHF communications used by AIS can also be spoofed and hijacked, allowing a man-in-the-middle attack. Examples of spoofing attacks on AIS include faking a possible collision with a ship and by doing so deviating the autonomous vessel into a direction the attackers want, generating false distress beacons, and crafting fake information to lure target ships into making wrong manoeuvres.[49]

To minimise the effect of attacks on a specific sensor, autonomous vessels should be equipped with enough sensors based on different technologies to compare various inputs from these sensors and make decisions based on all available information. For example, data from cameras, LiDAR and laser sensors can collectively identify obstacles in front of vessels. By doing this, autonomous vessels can

[43] 'What is GPS Spoofing?' McAfee, 25 August 2020, https://www.mcafee.com/blogs/internet-security/what-is-gps-spoofing.

[44] Roi Mit, 'Top 10 GPS Spoofing Events in History,' Threat Technology, https://threat.technology/top-10-gps-spoofing-events-in-history, [Accessed 24 January 2022].

[45] Kate Greenearchive, 'Lights, Camera - Jamming,' MIT Technology Review, 22 June 2006, https://www.technologyreview.com/2006/06/22/228938/lights-camera-jamming.

[46] Aaron Amick, 'The Shadowy World of Submarine and Ship-Launched Torpedo Countermeasures,' The Drive, 12 May 2020, https://www.thedrive.com/the-war-zone/33467/the-shadowy-world-of-submarine-and-ship-launched-torpedo-countermeasures-an-explainer.

[47] 'How Radar Jamming & Deception Changed Warfare FOREVER (Plus Future Trends),' Bliley Technologies, 16 January 2018, https://blog.bliley.com/radar-jamming-deception-electronic-warfare.

[48] Cyril Ray, Clément Iphar, Aldo Napoli, Romain Gallen and Alain Bouju, 'DeAIS Project: Detection of AIS Spoofing and Resulting Risks,' OCEANS 2015, pp. 1-6, 2015, doi: 10.1109/OCEANS-Genova.2015.7271729.

[49] Marco Balduzzi, Kyle Wilhoit and Alessandro Pasta, 'A Security Evaluation of AIS,' Trend Micro, 2014, https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-security-evaluation-of-ais.pdf.

achieve robustness to partial degradation or disruption of sensory data. Moreover, the usage of different technologies makes it more difficult for an attacker to be successful in deceiving all sensor data simultaneously.

Placing redundant sensors, preferably on a different vessel location, can also ward against sabotage attacks on a specific sensor and its subsequent failure. Another countermeasure is to use sensors that are not onboard the vessel. For example, satellite images can determine the vessel's position or drones launched from a ship near the autonomous vessel might fly around the vessel to act as remote image sensors. Sabotage attacks can also be possible for sensors inside the vessel. However, this type of attack first requires physical or logical access to ship networks. Therefore, these attacks are relevant to the security of OT systems. Regarding spoofed AIS messages, the autonomous vessel needs to have the capability to filter them out. Several techniques are available to detect spoofed AIS messages, such as determining the validity against legitimate historical messages[50] and using the radar sensor as a complement.[51] With GNSS spoofing, the same countermeasures as those against GNSS jamming can be considered.[52] However, encrypting GNSS signals will be the best solution to combat a spoofing attack.

Attacks to Intercept or Modify Communications

Unauthorised disclosure or manipulation of transmission data between the vessel and the SCC/other relay points can have a considerable impact. Examples of transmission data include C2 instructions from the SCC, acknowledgements of received instructions from the vessel, various pieces of information regarding the vessel status, images or videos and other observation and reconnaissance data taken by the vessel. Interception of RF signals is possible if attackers are in the proper place to receive the signals and listen to the right frequency.[53]

With the advent of software-defined radio (SDR) technology, the cost of intercepting RF signals has decreased dramatically. There are several low-cost interception devices designed for various frequency bands, including satellite signals.[54] Therefore, eavesdropping, replay and manipulation of transmitted data or, in the worst case, the entire occupation of the C2 and data links could be possible if data transmission is not adequately protected. In aerial drones, the hijacking of RF signals that modulates DSMx packets was first demonstrated using an SDR device in 2016.[55] DSMx is one of the prevalent protocols used to control low-end drones and radio-controlled cars and it does not have a secure authentication process. Manipulation of C2 instructions used for autonomous vessels, for example, could result in changing the vessel's direction and final destination. In the case of armed military ships, a missile could be launched at the wrong target. In the same way, the transmission of false information could lead to faulty intelligence if an autonomous surveillance submarine sends altered data back to its home base.

To prevent compromising security in data transmission, strong cryptographic mechanisms should be in place to provide authentication, confidentiality, integrity and non-repudiation. Any pre-installed shared

[50] Ray et al., 'DeAIS Project: Detection of AIS Spoofing and Resulting Risks.'

[51] Fotios Katsilieris, Paolo Braca and Stefano Coraluppi, 'Detection of Malicious AIS Position Spoofing by Exploiting Radar Information,' The 16th International Conference on Information Fusion, pp. 1196-1203, 2013.

[52] 'Jamming and Spoofing of Global Navigation Satellite Systems (GNSS),' INTERTANKO.

[53] Bruce R Wilkins, 'Common Misconceptions About Radio Waves, Radio Frequency and Wireless Communication,' ISACA Newsletters, Vol. 22, 30 October 2019, https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2019/volume-22/common-misconceptions-about-radio-waves.

[54] 'Software Defined Radio (SDR) for Hackers: Choosing the Best Hardware for SDR,' Hackers-Arise, 20 August 2021, https://www.hackers-arise.com/post/software-defined-radio-sdr-for-hackers-hardware-comparison-for-sdr.

[55] Jonathan Andersson, 'Attacking DSMx with Software Defined Radio (Presentation Slides),' PacSec 2016, 26 October 2016,
https://pacsec.jp/psj16/PSJ2016_Andersson_Hacking_DSMx_with_SDR_PacSec_2016_English.pdf.

secret between communicating parties should be securely injected during the provisioning process and the device used for provisioning should also be securely maintained to prevent it from being used in an unauthorised manner. Appropriate physical layer security mechanisms should also be in place. The same or similar techniques used for anti-jamming can be used to reduce the signal interception capability of attackers.[56] Besides these security mechanisms, having multiple communication channels with different technologies would also improve robustness against unauthorised manipulation. The main purpose of redundancy is to provide an alternative means when one technology is damaged, but it may also be used to verify that none of the channels is compromised by comparing data received separately from multiple channels.

Attacks on OT Systems

These attacks cause malfunctions or denial of service through penetration of the OT systems of autonomous vessels. Conventional industrial protocols that have been used in OT systems for years are vulnerable to cyberattack because security was not sufficiently considered when they were designed. For example, all major Fieldbus protocols such as Modbus, DNP3, Profinet and EtherCAT lack authentication and encryption and as a result, attackers can disrupt network operations or manipulate IO messages to cause a failure of the control process if they can access the OT network.[57] These security concerns may continue even if protocols with added security features such as Secure Modbus and Secure DNP, or even a new generation of secure protocols, are used in autonomous vessels. This is because sensors and actuators may still have limited computational power and memory that hinders the implementation of security functionalities. Even legacy protocols may still be in use. Another concern with OT systems is that some security solutions that could introduce unacceptable delay and jitter may not be deployed as timeliness and performance are essential.[58] The NMEA 0183 and 2000 protocols, the founding protocols for IEC 61162 specified by National Marine Electronic Association (NMEA), do not have native security features. Their successor, NMEA OneNet, is still vulnerable to spoofing and man-in-the-middle attacks, although some security improvements have been made.[59]

Infiltration into the OT system can be made indirectly via the ship network or directly via physical access to OT components. Attack vectors could include: manipulating the C2 instructions to enable over-the-air updates for installation of malicious codes; infiltrating the remote access point used for maintenance; infiltrating the external IT component and then laterally moving to the OT network by exploiting configuration errors in network segregation; and having physical access to a maintenance port such as USB, RJ45, UART and JTAG or even the physical wires used by OT systems. Several threat scenarios for general types of ICS not specific to autonomous vessels can be found in various ICS security guidelines such as BSI-CS 005E,[60] which considers malware infiltration via removable media and external hardware as the most severe threat.

To protect OT systems against cyberattack, security hardening practices such as using strong passwords, disabling unused services and ports and keeping all components up-to-date should be in

[56] Yi-Sheng Shiu, Shih Yu Chang, Hsiao-Chun Wu, Scott C.-H. Huang and Hsiao-Hwa Chen, 'Physical Layer Security in Wireless Networks: A Tutorial,' IEEE Wireless Communications, Vol. 18, No. 2, pp. 66-74, 2011, doi: 10.1109/MWC.2011.5751298.

[57] Eric D. Knapp and Joel Langill, Industrial Network Security, 2nd Edition, Syngress, 2015.

[58] 'NIST Special Publication 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security,' U.S. National Institute of Standards and Technology, May 2015, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

[59] Ky Tran, Sid Keene, Erik Fretheim and Michail Tsikerdekis, 'Marine Network Protocols and Security Risks,' Journal of Cybersecurity and Privacy, Vol. 1, pp. 239–251, 2021, doi: 10.3390/jcp1020013.

[60] 'BSI-CS 005E: Industrial Control System Security Top 10 Threats and Countermeasures 2019 (Version 1.30),' German Federal Office for Information Security, 6 June 2019, https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005E.pdf.

place, as they should in any IT system. Additional security measures specific to OT systems should also be identified and implemented. Separation of the OT network into smaller logical enclaves (virtual LANs), segregation of the OT network from the IT network, the use of a unilateral network device (preferably a hardware-based data diode) to allow data flow only in one way and applying physical protection measures to all maintenance ports are the examples of security measures specific to OT systems. There are many security guidelines for OT systems published by cybersecurity agencies around the globe, including US DHS's Recommended Practices for ICS[61] and EU ENISA's Recommendations on Protecting ICS.[62] These guidelines, along with IEC 62443 form a series of international standards for ICS security and provide valuable insights into building the cyber resilience of OT systems. In the future, security technologies for OT systems will be much more mature. Secure industrial protocols and security awareness capabilities that can fully understand the protocols and monitor and protect OT systems should be actively used wherever possible. Update processes for firmware and control logic should also be protected to prevent unauthorised updates.

Attacks on IT Systems

Autonomous vessels may also have IT systems which, in this context, means the systems and components that are not directly related to the manoeuvring of the vessel and include network components that are used to communicate with external parties such as the SCC and relay points. Besides the network components, typical examples of IT systems are administrative and supportive computers used by the crew. Unmanned vessels may also have some IT systems. For example, there may be a file server to store images, videos, sounds and other types of data collected as part of a surveillance and monitoring mission. Another example is a data historian that collects and stores time-series data regarding the vessel's status. It can be placed outside the OT network to allow remote access for engineers for troubleshooting. Likewise, various network configurations for IT systems may exist by implementing demilitarised zones using firewalls and unilateral network devices wherever applicable.

Attacks on IT systems could result in disruption of the systems and disclosure, deletion or modification of data in the systems. One may think the effect of attacks on the IT systems would be marginal on the assumption that the core OT system is adequately protected by network segregation and other security measures. However, there could be configuration errors in the network segregation and some IT systems may possess important data from business or military perspectives depending on the application. Therefore, the security of IT systems should not be overlooked. To protect IT systems against attack, security hardening practices should be established as it is for OT systems. In general, IT systems have more computing power and memory than OT systems and there is more room to use security solutions such as a security information and event management (SIEM) system or an intrusion prevention system (IPS). The deployment of security solutions should be actively considered for monitoring and protecting all resources within the network. Network segmentation and segregation using VLANs, firewalls and software-defined networks (SDNs) should be applied to the network to minimise the lateral movement when a particular system is compromised.

Attacks on AI used for Autonomous Operations

AI technologies employed by autonomous vessels are also vulnerable to cyberattack. Many current AI systems are powered by ML that extracts knowledge by learning many examples in a dataset. As the

[61] 'Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies,' U.S. Department of Homeland Security, September 2016, https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

[62] 'Protecting Industrial Control Systems,' European Union Agency for Cybersecurity, 9 December 2011, https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states.

ML is dependent on the dataset, it will be compromised if the dataset is corrupted or poisoned by an attacker.[63] In autonomous vessels, attackers will aim to attack the AI to cause misjudgement or malfunction in autonomous operations. The security, particularly the integrity, of AI in autonomous vessels is key when communication with the SCC is unavailable and manoeuvring is reliant on AI. With growing concerns about AI attacks on various real-world applications, the MITRE Corporation initiated the Adversarial Threat Landscape for Artificial Intelligence Systems (ATLAS) project in 2020 to enable researchers to navigate the landscape of threats to ML systems.[64] It provides an overview of security incidents related to ML and attackers' tactics and techniques applied to each incident. Typical attacks identified by ATLAS include model evasion to modify an ML model by malicious inputs that cause the attacker's desired effect in the model, model poisoning by training it with poisoned data and data poisoning of datasets. Other types of attacks that target input values used for fusion and computation are possible. Sensor values could be altered by attackers before they are used by AI if the communication interfaces are not adequately protected. Likewise, predefined voyage settings such as destination, route, alternative routes and restricted areas could also be altered if there is a lack of authentication when injection or alteration of these values is made.

To protect against AI attacks, it is essential to secure all interfaces including communications with the SCC and computational resources used for AI operations. Any intrusion into these resources could result in malfunction or disruption of AI operations. Appropriate security measures should also be in place when the ML model is being built at a vendor's or vessel owner's laboratory before its deployment to an autonomous vessel. Secure development practices such as removable device control, segregation of the development network from the internet and adequate configuration management should be applied to the development and learning environments. An attacker's initial access to the ML model and datasets can also be made through supply chain attacks by compromising hardware, software and data used for learning, including Graphics Processing Units (GPUs), training datasets, ML software stacks and the model itself.[65] When predefined ML models, training datasets and ML software stacks uploaded in open-source repositories are used, their integrity and authenticity should be thoroughly examined before using them for learning.

Attacks Through Supply Chains

Supply chain attacks have been identified for years among security practitioners and policy-makers since they can happen at any time and anywhere during the entire life cycle of all IT and OT hardware and software components in any application. Autonomous vessels can also be the victim of supply chain attacks. When they operate on the high seas far from the SCC, security incidents will not be handled promptly. In the worst case, the entire vessel may be damaged, resulting in a sinking or hijacking. Supply chain attacks occur not only through penetration into the vendor's development environment or update server but also through manipulating third-party modules and open-source libraries used in development. Thousands of malicious libraries uploaded onto Python Package Index, the open-source Python repository, are typical examples of such an attack.[66]

The supply chain of all hardware and software components used for autonomous vessels should be protected against intentional and accidental modification that could be incurred throughout its life cycle as any lack of physical and cybersecurity by a vendor or service provider may result in a breach in OT

[63] Marcus Comiter, 'Attacking Artificial Intelligence,' Belfer Center, 2019, https://www.belfercenter.org/sites/default/files/2019-08/AttackingAI/AttackingAI.pdf.
[64] 'ATLAS,' https://atlas.mitre.org, [Accessed 24 January 2022].

[65] 'ML Supply Chain Compromise,' https://atlas.mitre.org/techniques/AML.T0010, [Accessed 24 January 2022].
[66] Thomas Claburn, 'Python Package Index Nukes 3,653 Malicious Libraries Uploaded Soon after Security Shortcoming Highlighted,' The Register, 2 March 2021, https://www.theregister.com/2021/03/02/python_pypi_purges.

or IT systems. The vessel's owner should require suppliers, vendors and service providers to meet a certain level of security.[67] For example, they may request vendors obtain a third-party security certification such as ISO 27001 or set additional requirements for added security. However, asking vendors to implement security at a general level may not be sufficient to accomplish the security of all components because there is always a risk of attackers infiltrating manufacturers' development environments to modify products. Vendors may also produce insecure products due to mistakes or lack of security skills and awareness. Third-party security certification schemes such as Common Criteria, European Cybersecurity Certification and IEC 62443 certification could help. Although they do not guarantee the complete discovery of malicious codes and security flaws, these schemes examine the vendor's security practices related to development and delivery and check the security functionalities of the product. The vessel owner must also check the hash values and physical protection seals of products before installation or deployment to ensure that the products are authentic and not altered during delivery. In addition, maintaining a software bill of materials (SBOM), an inventory of software components and dependencies, and information about those components and their hierarchical relationships for software used in autonomous vessels may help vendors and owners identify and cope with supply chains risks.

Attacks Through Physical Access

The vulnerability of autonomous vessels to physical attack may inevitably increase when it operates on the high seas because anyone could have unauthorised physical access to the vessel. For example, pirates, criminals or adversaries may board the vessel and cause harm to the system, such as changing routes or destinations and stopping the engine for hijacking. The hijacking of autonomous vessels could happen due to the economic value of the vessel itself and the cargo it carries and the technical value from the perspective of industrial espionage. Adversaries can obtain information related to military operations and technologies applied to autonomous naval vessels through reverse engineering. There are also concerns that if pirates or terrorists hijack armed military vessels, they will obtain weapons from the vessel and abuse them for terrorism. Pirates could divert the vessel to a different location and take the vessel itself 'hostage', threatening to blow up or sink it to cause massive environmental pollution.

Although there is no clear answer to this problem, all efforts should be made to increase the cost of such attacks. Power and communication cables should not be exposed outside the vessel and the entrance door to the inside should be firmly locked. Inside the vessel, network ports or other maintenance ports of system components should be sealed and cables should not be exposed, placing them under the floor or inside the wall. Alarm systems that transmit security alarms to the SCC when identifying intrusion and cable fault sensors that detect disconnection of cables should be installed. Tamper-resistant mechanisms that erase important business or military data following intrusion may also be considered for critical data that should not be disclosed to other parties. Likewise, there are physical protection measures that make vessels more robust against physical attacks. However, nothing can protect the vessel entirely on the high seas and, therefore, the vessel's value, the likelihood of physical attack and the cost of countermeasures should be considered together to find the most cost-effective setup.

Attacks on the Shore Control Centre

Inadequate segregation between the C2 network and the office network at the SCC or inappropriate control over removable media within the C2 network may cause compromise which can cause the transmission of unauthorised commands to autonomous vessels or disruption of communication links between the SCC and vessels. Like the OT and IT systems of autonomous vessels, security best practices should be implemented to protect C2 and office networks at the SCC, including the deployment

[67] 'Port Cybersecurity - Good Practices for Cybersecurity in the Maritime Sector,' European Union Agency for Cybersecurity.

of the SIEM capability. The physical perimeter controls for the building and the physical access control for the control room should also be implemented at the SCC.

5. Concluding Remarks

The scope of security in autonomous vessels can be broader than in other ICSs. In general, the main focus of security in other ICSs is the availability and integrity of systems. However, autonomous vessels may have additional security requirements for confidentiality and integrity of the data and information they produce, collect or possess, depending on their missions which might include surveillance or combat operations. The scope of protection may also extend to various IT processing and computation systems which communicate with external parties by wireless means. These characteristics make the security problem more complicated.

When operating on the high seas far from SCCs or home bases, autonomous vessels will be less monitored due to the limited bandwidth in communications. If seafarers are on board, they can override the system to manual control or simply stop the ship if any unpredicted event happens. However, when a crewless vessel is under attack and its C2 channel is disrupted, it will take a long time for a team of engineers to board the vessel to regain control. During this period, attackers might be already successful in their objectives. Autonomous military intelligence submarines that have no communications with base for months and go into foreign territorial waters will have a much higher level of risk, requiring more intensive security considerations to provide resilience. However, autonomous vessels continuously travelling between two endpoints on a route may have a lower level of risk because they can be closely monitored and a team of engineers can physically access the vessel quickly.

A risk management approach should be applied when designing, developing and operating autonomous vessels to identify and implement appropriate countermeasures commensurate with the risk. It is still unclear when fully automated autonomous vessels will be available for practical commercial or military operations. However, it is crucial to ensure that security considerations are applied from the planning and design phase because considering security in the early stages of development will enable security measures to be implemented in an efficient/effective manner while saving costs, compared to adding them after development.

6. References

1. Koji Wariishi, ‘Maritime Autonomous Surface Ships Development Trends and Prospects,’ Mitsui Global Strategic Studies Institute Monthly Report, September 2019, https://www.mitsui.com/mgssi/en/report/detail/__icsFiles/afieldfile/2020/01/09/1909t_wariishi_e.pdf.
2. ‘Mayflower Autonomous Ship - Transatlantic Mission Overview and Status Update,’ IBM, https://newsroom.ibm.com/Mayflower-Autonomous-Ship-Transatlantic-Mission-Overview-and-Status-Update, [Accessed 24 January 2022].
3. ‘Autonomous Ship Project, Key Facts about Yara Birkeland,’ Kongsberg, https://www.kongsberg.com/maritime/support/themes/autonomous-ship-project-key-facts-about-yara-birkeland, [Accessed 24 January 2022].
4. ‘Remote and Autonomous Ships - The Next Step,’ Rolls-Royce, 21 June 2016, https://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/aawa-whitepaper-210616.pdf.
5. ‘Korea Autonomous Surface Ship Project – Project Detail,’ Korea Research Institute of Ships & Ocean Engineering, https://kassproject.org/en/info/projectdetail.php, [Accessed 24 January 2022].
6. Kevin Jones, Kimberly Tam and Maria Papadaki, ‘Threats and Impacts in Maritime Cyber Security,’ Engineering & Technology Reference, 22 April 2016, doi:10.1049/etr.2015.0123.
7. ‘MSC 100/20/Add.1 Annex 2: Framework for the Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (MASS),’ International Maritime Organization, June 2019, https://maiif.org/wp-content/uploads/2019/06/MSC-100_20-Annex-20-1.pdf.
8. ‘D4.5: Architecture Specification,’ The MUNIN Project Deliverable, 8 February 2014, http://www.unmanned-ship.org/munin/wp-content/uploads/2014/02/d4-5-architecture-v11.pdf.
9. ‘D8.6: Final Report: Autonomous Bridge,’ The MUNIN Project Deliverable, 6 August 2015, http://www.unmanned-ship.org/munin/wp-content/uploads/2015/09/MUNIN-D8-6-Final-Report-Autonomous-Bridge-CML-final.pdf.
10. Jia Wang, Yang Xiao, Tieshan Li and C. L. Philip Chen, ‘A Survey of Technologies for Unmanned Merchant Ships,’ IEEE Access, Vol. 8, pp. 224461-224486, 2020, doi: 10.1109/ACCESS.2020.3044040.
11. Ørnulf J. Rødseth and Åsmund Tjora, ‘A System Architecture for an Unmanned Ship,’ The 13th International Conference on Computer and IT Applications in the Maritime Industries (COMPIT 2014), pp. 291-302, May 2014.
12. Theodore J. Williams, ‘The Purdue Enterprise Reference Architecture,’ Computers in Industry, Vol. 24, No. 2, pp. 141-158, 1994.
13. Guobao Xu, Weiming Shen and Xianbin Wang, ‘Applications of Wireless Sensor Networks in Marine Environment Monitoring: A survey,’ Sensors, Vol. 14, No. 9, pp. 16932-16954, 2014, doi: 10.3390/s140916932.
14. Bjørn J. Vartdal, Rolf Skjong and Asun L, St. Clair, ‘Remote-Controlled and Autonomous Ships in the Maritime Industry,’ DNV, 2018, https://www.dnv.com/maritime/publications/remote-controlled-autonomous-ships-paper-download.html.
15. Scott Savitz, Irv Blickstein, Peter Buryk, Robert W. Button, Paul DeLuca, James Dryden, Jason Mastbaum, Jan Osburg, Phillip Padilla and Amy Potter, ‘U.S. Navy Employment Options for Unmanned Surface Vehicles (USVs),’ RAND Corporation, 2013, https://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR384/RAND_RR384.pdf.
16. Natalie Klein, Douglas Guilfoyle, Saiful Karim and Rob McLaughlin, ‘Maritime Autonomous Vehicles: New Frontiers in The Law of The Sea,’ International & Comparative Law Quarterly, Vol. 69, No. 3, pp. 719-734, 2020, doi: 10.1017/S0020589320000226.
17. ‘MSC-FAL.1/Circ.3: Guidelines on Maritime Cyber Risk Management,’ International Maritime Organization, 4 July 2017, https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.
18. ‘Resolution MSC.428(98): Maritime Cyber Risk Management in Safety Management Systems,’ International Maritime Organization, 16 June 2017, https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx.
19. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union, 19 July 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148.
20. ‘Cyber Security Aspects in the Maritime Sector,’ European Union Agency for Cybersecurity, 19 December 2011, https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1.

21. 'Port Cybersecurity - Good Practices for Cybersecurity in the Maritime Sector,' European Union Agency for Cybersecurity, 26 November 2019, https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector.
22. 'Guidelines - Cyber Risk Management for Ports,' European Union Agency for Cybersecurity, 17 December 2020, https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports.
23. 'The Guidelines on Cyber Security Onboard Ships - Version 4,' Baltic and International Maritime Council, 23 December 2020, https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships.
24. 'Code of Practice: Cyber Security for Ships,' UK Department for Transport, 13 September 2017, https://www.gov.uk/government/publications/ship-security-cyber-security-code-of-practice.
25. Sokratis K. Katsikas, 'Cyber Security of the Autonomous Ship,' The 3rd ACM Workshop on Cyber-Physical System Security, pp. 55-56, 2017, doi: 10.1145/3055186.3055191.
26. Bilhanan Silverajan, Mert Ocak and Benjamin Nagel, 'Cybersecurity Attacks and Defences for Unmanned Smart Ships,' 2018 IEEE International Conference on Internet of Things/IEEE Green Computing and Communications/IEEE Cyber, Physical and Social Computing/IEEE Smart Data, pp. 15-20, 2018, doi: 10.1109/Cybermatics_2018.2018.00037.
27. Kazem. 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.
28. Georgios Kavallieratos, Vasiliki Diamantopoulou and Sokratis K. Katsikas, 'Shipping 4.0: Security Requirements for the Cyber-Enabled Ship,' IEEE Transactions on Industrial Informatics, Vol. 16, No. 10, pp. 6617-6625, 2020, doi: 10.1109/TII.2020.2976840.
29. Kimberly Tam and Kevin Jones, 'Cyber-Risk Assessment for Autonomous Ships,' 2018 International Conference on Cyber Security and Protection of Digital Services, pp. 1-8, 2018, doi: 10.1109/CyberSecPODS.2018.8560690.
30. Georgios Kavallieratos, Sokratis Katsikas and Vasileios Gkioulos, 'Cyber-Attacks against the Autonomous Ship,' 2018 International Workshop on the Security of Industrial Control Systems and Cyber-Physical Systems, pp. 20-36, 2018, doi: 10.1007/978-3-030-12786-2_2.
31. Georgios Kavallieratos and Sokratis Katsikas, 'Managing Cyber Security Risks of the Cyber-Enabled Ship,' Journal of Marine Science and Engineering, Vol. 8, No. 10, pp. 1-19, 2020, doi: 10.3390/jmse8100768,
32. Mogens Blanke, Michael Henrique and Jakob Bang, 'A Pre-Analysis on Autonomous Ships,' Technical University of Denmark Technical Report, 2017, https://www.dma.dk/Documents/Publikationer/Autonome%20skibe_DTU_rapport_UK.pdf.
33. Kanika Grover, Alvin Lim and Qing Yang, 'Jamming and Anti-jamming Techniques in Wireless Networks: A Survey,' International Journal of Ad Hoc and Ubiquitous Computing, Vol. 17, No. 4, pp 197-215, 2014, doi: 10.1504/IJAHUC.2014.066419.
34. Pavel Velkovsky, Janani Mohan and Maxwell Simon, 'Satellite Jamming,' Project on Nuclear Issues by the Center for Strategic and International Studies, 3 April 2019, https://ontheradar.csis.org/issue-briefs/satellite-jamming.
35. 'MSCI Advisory 2020-016-Various-GPS Interference,' U.S. Department of Transportation, 22 September 2020, https://www.maritime.dot.gov/msci/2020-016-various-gps-interference.
36. 'Jamming and Spoofing of Global Navigation Satellite Systems (GNSS),' INTERTANKO, 2019, https://www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf.
37. 'What is GPS Spoofing?' McAfee, 25 August 2020, https://www.mcafee.com/blogs/internet-security/what-is-gps-spoofing.
38. Roi Mit, 'Top 10 GPS Spoofing Events in History,' Threat Technology, https://threat.technology/top-10-gps-spoofing-events-in-history, [Accessed 24 January 2022].
39. Kate Greenearchive, 'Lights, Camera - Jamming,' MIT Technology Review, 22 June 2006, https://www.technologyreview.com/2006/06/22/228938/lights-camera-jamming.
40. Aaron Amick, 'The Shadowy World of Submarine and Ship-Launched Torpedo Countermeasures,' The Drive, 12 May 2020, https://www.thedrive.com/the-war-zone/33467/the-shadowy-world-of-submarine-and-ship-launched-torpedo-countermeasures-an-explainer.
41. 'How Radar Jamming & Deception Changed Warfare FOREVER (Plus Future Trends),' Bliley Technologies, 16 January 2018, https://blog.bliley.com/radar-jamming-deception-electronic-warfare.
42. Cyril Ray, Clément Iphar, Aldo Napoli, Romain Gallen and Alain Bouju, 'DeAIS Project: Detection of AIS Spoofing and Resulting Risks,' OCEANS 2015, pp. 1-6, 2015, doi: 10.1109/OCEANS-Genova.2015.7271729.
43. Marco Balduzzi, Kyle Wilhoit and Alessandro Pasta, 'A Security Evaluation of AIS,' Trend Micro, 2014, https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-security-evaluation-of-ais.pdf.
44. Fotios Katsilieris, Paolo Braca and Stefano Coraluppi, 'Detection of Malicious AIS Position Spoofing by Exploiting Radar Information,' The 16th International Conference on Information Fusion, pp. 1196-1203, 2013.
45. Bruce R Wilkins, 'Common Misconceptions About Radio Waves, Radio Frequency and Wireless Communication,' ISACA Newsletters, Vol. 22, 30 October 2019,

https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2019/volume-22/common-misconceptions-about-radio-waves.

46. ‘Software Defined Radio (SDR) for Hackers: Choosing the Best Hardware for SDR,’ Hackers-Arise, 20 August 2021, https://www.hackers-arise.com/post/software-defined-radio-sdr-for-hackers-hardware-comparison-for-sdr.
47. Jonathan Andersson, ‘Attacking DSMx with Software Defined Radio (Presentation Slides),’ PacSec 2016, 26 October 2016, https://pacsec.jp/psj16/PSJ2016_Andersson_Hacking_DSMx_with_SDR_PacSec_2016_English.pdf.
48. Yi-Sheng Shiu, Shih Yu Chang, Hsiao-Chun Wu, Scott C.-H. Huang and Hsiao-Hwa Chen, ‘Physical Layer Security in Wireless Networks: A Tutorial,’ IEEE Wireless Communications, Vol. 18, No. 2, pp. 66-74, 2011, doi: 10.1109/MWC.2011.5751298.
49. Eric D. Knapp and Joel Langill, Industrial Network Security, 2nd Edition, Syngress, 2015.
50. ‘NIST Special Publication 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security,’ U.S. National Institute of Standards and Technology, May 2015, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.
51. Ky Tran, Sid Keene, Erik Fretheim and Michail Tsikerdekis, ‘Marine Network Protocols and Security Risks,’ Journal of Cybersecurity and Privacy, Vol. 1, pp. 239–251, 2021, doi: 10.3390/jcp1020013.
52. ‘BSI-CS 005E: Industrial Control System Security Top 10 Threats and Countermeasures 2019 (Version 1.30),’ German Federal Office for Information Security, 6 June 2019, https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005E.pdf.
53. ‘Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies,’ U.S. Department of Homeland Security, September 2016, https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.
54. ‘Protecting Industrial Control Systems,’ European Union Agency for Cybersecurity, 9 December 2011, https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states.
55. Marcus Comiter, ‘Attacking Artificial Intelligence,’ Belfer Center, 2019, https://www.belfercenter.org/sites/default/files/2019-08/AttackingAI/AttackingAI.pdf.
56. ‘ATLAS,’ https://atlas.mitre.org, [Accessed 24 January 2022].
57. ‘ML Supply Chain Compromise,’ https://atlas.mitre.org/techniques/AML.T0010, [Accessed 24 January 2022].
58. Thomas Claburn, ‘Python Package Index Nukes 3,653 Malicious Libraries Uploaded Soon after Security Shortcoming Highlighted,’ The Register, 2 March 2021, https://www.theregister.com/2021/03/02/python_pypi_purges.