TRANSNAV
http://www.transnav.eu

the International Journal
on Marine Navigation
and Safety of Sea Transportation

Volume 17
Number 2
June 2023

DOI: 10.12716/1001.17.02.01

Cyber Threats for Present and Future Commercial Shipping

J. Pawelski
Gdynia Maritime University, Gdynia, Poland

ABSTRACT: Cyber-attacks are extremely dangerous for all operations relaying upon it-technologies. Today shipping businesses cannot operated without processing large amounts of information. Four biggest shipping companies suffered break-down in their operations after they were struck by malware. International Maritime Organization also was struck by cyber-attack which took its website down. Maritime community noticed rise in cyber-attacks on virtually all computer-based systems on board of vessels. For manned vessels risks to safety of navigation are mitigated by presence of crew on board but remain financial and reputational losses. Introduction of remotely controlled and fully autonomous unmanned vessels will increase seriousness of threats. Cyber-attack may severely hamper ship's operability or even lead to complete loss of control. International community is developing several countermeasures to protect commercial shipping presently and in future.

1 INTRODUCTION

Number of cyber-attacks against maritime industry is growing each year. Such attacks were directed for shipping companies and as well against individual vessels. Within three years, from 2017 to 2020, shipping industry had experienced tenfold rise in cyberattacks as shown on graphic below:

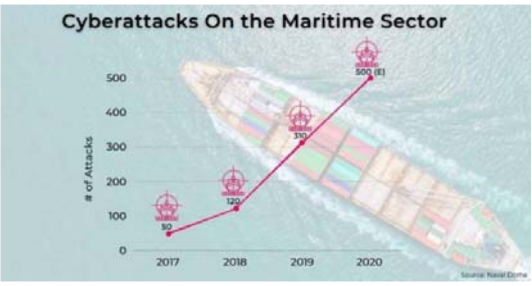


Figure 1. Cyber-attacks rise on maritime industry [32].

Targeted were shipping companies and individual vessels. Maritime security experts reported for the same period number of cyber-attacks against vessels arose for 900% [18]. Most significant attacks were aimed against major shipping lines and International Maritime Organization. In June 2017 Danish Maersk was hit with NotPetya wiper malware. Most of Maersk data was lost with 49,000 laptops and 4,000 servers. Total losses exceeded $300 million [14]. A year later, in July 2018, another shipping giant COSCO fell prey of SamSam ransomware. Company worldwide network collapsed and remained shut down for several days. COSCOS's global fleet was not affected by attack. Financial losses remain unknown as company never disclosed them [14]. Hackers did not spare even international organization working on cyber security regulations for maritime sector. Two months later, on September 30, 2020, some International Maritime Organization (IMO) website services were taken down for few days by cyber-attack, however e-mail and communication continued to work [24].

This web site is under maintenance. We are sorry for any inconvenience caused.

GISIS | IMODOCS | Virtual Publications | eRoster

Figure 2. IMO website taken down due to cyber-attack [24].

Increasing dependency of vessels on computer technologies makes them more vulnerable to attack by existing and future malware. Problem becomes more acute with introduction of autonomous vessels. Cyber-attacks pose real barriers for safe operations of such vessels until effective solution has been found [11]. Baltic and International Maritime Council (BIMCO) issued in 2019 Cyber Security Clause 2019 obliging all parties involved in security incident inform each other with 12 hours and poses security plans and procedures [15]. Maritime insurance companies concerned with growing number cyber-attacks on shipping industry published warnings for their customers [1]. Insurers now are limiting claims by application two clauses published by International Underwriters Association (IUA). Clause IUA 09-081 CYBER LOSS ABSOLUTE EXCLUSION CLAUSE and clause IUA 09-0812 CYBER LOSS LIMITED EXCLUSION CLAUSE are excluding any cyber loss from insurance cover [29]. Cyber-attack targeting vessel's navigational systems, steering and propulsion may have very serious consequences including event denial of port entry by authorities due to her unseaworthiness. Without possibility to return ship's vital equipment to its working condition, vessel could be left adrift, remaining at anchor at roads or towed to port as a hulk. It is not an imaginary scenario. In 2017 hackers took control over container vessel in Mediterranean Sea. They gained full control to ship's navigational systems with purpose to steer vessel to convenient place for boarding her. Crew regained control of vessel after ten hours and bringing IT team on board [13]. Analysis of shipboard networks and equipment shows their growing vulnerability to cyber-attacks due to implementation of more complex systems for communication and vessel control. Introduction of remotely controlled and fully autonomous vessels may have negative impact on overall safety of navigation.

2 VESSEL'S SHIPBOARD NETWORK

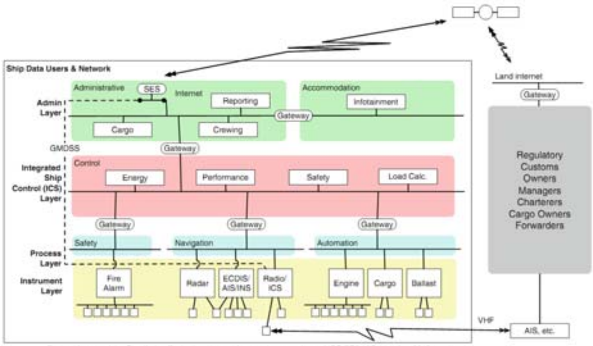
Until middle of last century ship's communication and control of equipment were domain of analogue technology. Digital revolution first revolutionized land-based information transmission methods and ways of industrial processes control with introduction of network. Implementation of Global Maritime Distress Safety System (GMDSS) began era of maritime communication networks for digital information transfer. Digitalization also found its way into systems controlling vessel's equipment. Analogue mechanical and electronic controllers were replaced with fully digitalized interconnected systems forming shipboard network. Digitalized systems onboard vessels are divided into two distinctive kinds: Information Technology (IT) and Operational Technology (OT). IT systems are designed for data management and typically they handle GMDSS, Automatic Ship Identification (AIS), Long Range Identification and Tracking (LRIT), corporate communication (owners, management, charterers, suppliers, local authorities). Systems termed as OT are industrial control systems. They consist of Programmable Logic Controllers (PLC), Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition systems (SCADA). Most significant differences among IT and OT systems are given in table 1.

Table 1. Main differences between IT and OT systems. Modified from [10]

Category	Information Technology	Operational Technology
Performance	Non-real time. Response must be consistent. Response to emergency less critical. Access can be restricted to the required degree.	Real time. Real time response critical. Response to emergency critical. Access strictly restricted.
Availability	Rebooting acceptable. Temporary lack of availability acceptable.	Rebooting not acceptable. Uninterrupted availability may require redundant system
Risk Management	Manage data. Data confidentiality and integrity is paramount Fault tolerance is less important. Major risk impact is delay of business operation	Control physical world. Human safety is paramount, followed by protection of the process. Major risk impacts are regulatory non-compliance, environmental impacts, loss of life, equipment, or production
System Operations	Systems are designed for use with typical operating systems. Upgrades are straightforward with the availability of automated deployment tools.	Proprietary system for industrial process. Mostly without safety capabilities built in. Upgraded by authorized service.
Resource Constrains	Systems with enough resources to support the addition of third-party applications such as security solutions.	System with limited computing and memory resources to support only particular process.
Communi-cations	Standard communications protocols Primarily wired networks with some localized wireless capabilities. Typical IT networking Practices.	Many proprietary and standard communication protocols Several types of communications media used including dedicated wire and wireless (radio and satellite). Networks are complex and

		sometimes require the expertise of control engineers.
Component Lifetime	3 to 5 years	10 to 15 years
Components Locations	Components locally and easily accessible.	Components can be isolated, remote, and require extensive physical effort to gain access to them.

Another major difference between IT ant OT is CIA Triad. It is model of security policy of IT systems in organization. CIA stand for Confidentiality, Integrity, and Availability of information in hierarchical order. OT systems represent different model security policy. It is CAIC which means Control, Availability, Integrity, and Confidentiality [31]. For long time both systems were separated on board of vessels and so-called 'air gap' was acting as very efficient barrier protecting OT systems from malicious attacks. Situation has changed when development of internet-based technologies evolved into Internet of Things (IoT) linking consumer devices with Internet and other devices [27]. Digitalization of industrial systems eventually led to the creation of Industrial Internet of Things (IIoT) for managing and controlling processes and data acquisition via global network [34]. New industrial technology opened the way for Internet based maritime services and created Internet of Ships (IoS) for management and monitoring of smart vessels [20]. Figure 3 shows shipboard networks for existing and future vessels [9]. IoS technology is necessary for introduction of remotely controlled and fully autonomous vessels. Future development of IoS needs to address security issues and uninterrupted availability of transferred information, alternative systems of data transfer and widening bandwidth to accommodate much larger volume of information being transferred at high speed. Connecting OT systems to networks outside ship makes them vulnerable to cyber-attacks which may lead to injury, loss of life, large scale damage to assets and have serious environmental impact.



Derived from work by Ørnulf Jan Rødseth with input from various members of ISO TC8 at September 2019 meetings

Figure 3. Present and future shipboard networks [9]

More advanced autonomy of vessels will require all shipboard equipment conjoined into the single local network connected to shore-based services by satellite or radio link. Merging ship's environment with global network opens the gateway for cyber-attack unless effective preventive measures are introduced.

3 VESSEL'S INFRASTRUCTURE TARGETED BY CYBER ATTACKS

Dependency of shipping industry on digital technologies and networks is growing each year. Shipping lines are extensively using IT for managing their businesses and for communication with their business partners. Some of them suffered heavy losses when their IT systems were attacked [14]. It happened despite of having their systems protected and supervised by IT specialists. Digitalization of ship's communication and control systems made them prone to malicious cyber-attacks. Due to increased dependency of ship's IT and OT systems on networks and Internet theoretically all shipboard systems are vulnerable. Internal protocols used by internal networks are not encrypted are officially known and published industry standards. Attacker can easily inject false information in data exchange stream to fool equipment. Equipment requiring more computing power often uses commercial operating systems including these which are no longer supported. Obsolete and unpatched systems are easy prey for hackers.

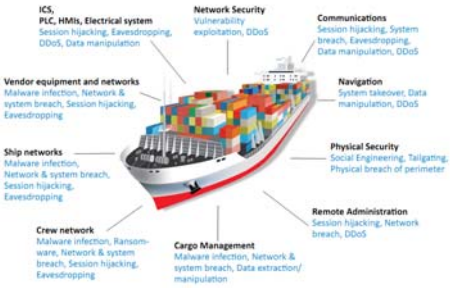

ICS,
PLC, HMIs, Electrical system
Session hijacking, Eavesdropping, DDoS, Data manipulation
Network Security
Vulnerability exploitation, DDoS
Communications
Session hijacking, System breach, Eavesdropping, Data manipulation, DDoS
Vendor equipment and networks
Malware infection, Network & system breach, Session hijacking, Eavesdropping
Navigation
System takeover, Data manipulation, DDoS
Ship networks
Malware infection, Network & system breach, Session hijacking, Eavesdropping
Physical Security
Social Engineering, Tailgating, Physical breach of perimeter
Remote Administration
Session hijacking, Network breach, DDoS
Crew network
Malware infection, Ransom-ware, Network & system breach, Session hijacking, Eavesdropping
Cargo Management
Malware infection, Network & system breach, Data extraction/ manipulation

Figure 4. Potential targets of cyber-attack against vessel [4].

It is difficult to analyse all hypothetical cyber-attacks against vessel's systems but security and resilience against cyber-attack is paramount for safety of navigation. With more developed ship's network more equipment is exposed to attacks. Shipboard network consists of several components like:

- communication network including satellite and radio links. Composed of GMDSS equipment with mandatory emergency satellite and radio communication means, Very Small Aperture Terminals (VSAT) for official and crew communication including Internet other communication systems provided for communication and global network access.
- integrated navigation system as network of navigational equipment linked together. Introduction of e-Navigation concept resulted necessity of data interchange between Global Navigational Satellite System (GNSS) receivers and Electronic Chart Display and Information Centre (ECDIS), radars with Automatic Radar Plotting Aid (ARPA), Automatic Ships Identification (AIS) transponders, Voyage Data Recorders (VDR) and adaptive autopilots.
- industrial control systems (ICS) as networks made up of OT equipment managing ship's propulsion, power generation and steering, such as SCADA, DCS, PLC and HMI (Human-Machine Interface).
- loading and stability network including cargo management and cargo handling, ballast management systems.

- shipboard safety systems for fire and smoke detection, water ingress alarm, fire, and watertight doors management.
- shipboard security system, as such internal communication, Closed Circuit TV (CCTV) with video recording, firewalls, network segmentation devices, Ship Security Alert System (SSAS), Ship Security Reporting System (SSRT)

First generations of malware targeting OT were aimed at Windows-based SCADA systems. Prime example of it is Stuxnet worm created for attacking Iranian uranium centrifuges PLC controllers through Windows applications controlling PLC's and controllers embedded software. Today Stuxnet is the history, and zero-day vulnerabilities are patched long ago but after attack on Iranian Natanz facility it quickly spread into numerous locations in the world [17]. Low level systems like PLCs for long time were considered as safe from cyber-attacks when protected by "air gap" and lack of PLC specific malware. Manufacturers did not bother to provide them even with rudimentary security features. Within last few years researchers worked out PLC hack which gathers sensitive data and sends it out by radio link created by PLC itself generating frequency modulated transmission. Data is decoded by Software Defined Radio (SDR) and personal computer (PC) with antenna. Range of transmission is limited due to low signal level but low flying drone or placed nearby PC with SDR are capable to pick up signal [20]. Another unpleasant information for OT engineers is development of undetectable PLC rootkits for research purposes. Rootkits residing in dynamic memory can manipulate PLC input-output devices (I/O) and directly affect control of industrial processes [19]. Researchers also proved feasibility of cyber-attack on PLC networks due to meagre security features provided by makers [21]. All shipboard systems are important for universally understood safety of navigation, but overall command of vessel is exercised by navigation systems.

4 NAVIGATION SYSTEMS

Development of Global Navigational Satellite Systems (GNSS) paved way to rise of Integrated Navigation Systems (INS) requiring continuous updating of ship's position. IMO determined equipment and its functions INS [7].

Table 2. Integrated Navigation System. Modified from [7].

INS subsystem	Tasks and functions
Radar	Collision avoidance
ECDIS	Route planning Route monitoring
Heading control	Navigation control data Navigation status and data display
Track control	Navigation control data and track control
AIS	Collision avoidance Navigation control data
Echosounder	Route monitoring
GNSS	Navigation control data Navigation status and data display
Log (speed and distance)	Navigation control data Navigation status and data display

Today GNSS is the backbone of all integrated navigational systems providing continuous position of vessel necessary for appropriate work of ECDIS, radar, ARPA, AIS, and track control. Most of vessels are using Global Positioning System (GPS) as main source of position however alternative system Globalnaya Sputnikovaya Systema (GLONASS) is often used in high latitudes due to its higher orbital inclination. Differential version of GPS allows to navigate confined waters with much higher accuracy than traditional methods of navigation. Cyber- attack on GPS disrupts work of most INS components and seriously jeopardize safety of navigation. As a source of position GPS is the most important part of any INS. ECDIS plays no less significant role in safe navigation as means of planning and monitoring of vessel's safe route. Loss of GPS position limits ECDIS route monitoring abilities to terrestrial navigation with position obtained from radar or terrestrial bearings. Digital radars in use today are based on data processing software which can be targeted by malicious attack leaving ECDIS without position input from radar and denying vessel protection against collision. AIS is design to supplement ship's navigation and collision avoidance, but its unsecured communication protocols made it vulnerable to spoofing attacks with purpose to provide false information. All these technologies are playing especially vital role in development of autonomous vessels of the future.

4.1 *GPS*

Satellite navigation system is the most crucial part of today's INS, and its role will rise with development of remotely controlled and fully autonomous vessels. Manned vessels even with reduced crew can still navigate in confined waters when GPS position is not available using more traditional ways of navigation. Vessels relying solely upon remote control or autonomous navigation must always have access to reliable satellite derived position safely navigate. Most of word's fleet use GPS as Positioning, Navigation and Timing system (PNT). Despite of well-known virtues, GPS has two significant vulnerabilities: low level of received signal and unprotected transmission protocol for civilian users. Very weak PGS signal makes it prone to interferences with system proper functioning. Problems with GPS may lead to improper work shipboard systems and Aids to Navigation (AtoN). Loss of GPS signal or its distortion affects such systems on board as:

- GPS and DGPS positioning
- ECDIS
- Radar/ARPA
- AIS
- Digital gyrocompass
- Track control
- Digital Selective Call (DSC)
- LRIT
- SSAS and SSRT
- Dynamic Positioning (DP)

Problems with GPS signal have also an impact on AtoN :

- AtoN positioning monitoring
- DGPS corrections
- AtoN correct deployment

– AIS
– Lights synchronization

AtoN is vital for safe navigation in confined waters when navigator needs to verify GPS position with navigational aids to confirm correctness ship's position. Weakness of GPS signal makes this system easy target for several methods of malicious attacks. Simplest way to attack GPS is jamming of signal. It is sufficient to broadcast strong signal on GPS frequency to overpower weak signal and receiver loses lock on signal from satellite. Equipment for jamming, so called jammer, is widely used for personal and military security. In some countries it can be bought legally. Figure 5 shows result of test jamming exercise where small power transmitter could interfere with GPS signal at distance 30 km [3].

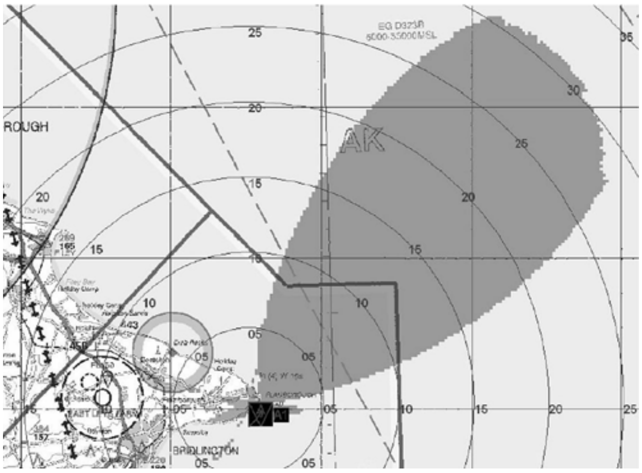


Figure 5. Experiment with 1.58 W jammer at 25 m height. Distances in km [3].

Intentional jamming can be carried out non-state actors, individuals, or small groups with portable jammers or state-sponsored i.e., North Korea [v]. In some situations, GPS signal can be jammed unintentionally by aircrafts altimeters, TV harmonics, certain radars, satellite communication equipment and malfunctioning electronic devices [8]. Providing receivers with smart array antennae with nulling properties makes equipment more resilient to jamming by surface-based transmitters. It also possible to counter jamming by powerful terrestrial PNT systems like Loran-e.

Another way of attacking is spoofing by broadcasting false GPS signals. Attack begins with transmission of signals with slightly higher power and synchronised with GPS signal. When receivers lock onto bogus signal it gradually phases out genuine GPS signal and gives false position [3]. Simple spoofing equipment can generate only static position, but more complex systems are capable of dynamic one. This kind of attack is more difficult to detect unless navigator can obtain position by independent way and analyses reason of positions discrepancy. Most prominent spoofing attack happened between 22 and 24 of June 2017 at Black Sea. 20 vessels reported their positions on land in Gelendzhik Airport [25]. Nulling array GPS antennae and powerful land based PNT system may protect user to certain degree by suppressing unwanted signal and using alternative navigation system. More radical solution foresees implementation of Navigation Message Authentication (NMA) in GPS signal. This method will require replacement of existing GPS receivers with new generation of equipment [8]. This solution may not work for meaconing attack against GPS. It is a type of spoofing when GPS signals are re-transmitted after some time. Intentional delay in satellite signal leads to position error. Re-transmission does not require mimicking of genuine GPSD signal including NMA and signal encryption does not work. Mitigation methods like nulling antennae and land based PNT may alleviate consequence of such attack.

4.2 *ECDIS*

Paper charts on large ocean-going vessels have given way to ECDIS which became nexus of electronic navigation. Such system makes marine navigation safer and more efficient but is very vulnerable to cyber-attacks like any personal computer. ECDIS works on commercially available computer operating systems prone to attacks even when regularly updated and protected by anti-malware software. Security consultants Pen Test Partners during cyber-security inspections found most of ECDIS using old outdated operating systems with one of them even working on Windows NT [33]. Operating system can be attacked through network used for updating electronic charts or USB memory sticks used for the same purpose. Results of such attack a same as on personal computer i.e., operating system crash, data encryption and deletion, planting malicious scripts, spreading malware through connected network. As a result, ECDIS becomes unusable and other equipment gets infected. For such scenario vessel must be provided with another ECDIS as a backup or set of paper charts for intended voyage. Different form of attack is jamming of spoofing GPS providing position for ECDIS. Jamming is easily detectable when system loses position input and goes into dead reckoning. Spoofing of GPS is much worse scenario. ECDIS plots on electronic chart false position from GPS receiver which is more difficult for operator to spot and react. In both situation navigator may continue navigation on ECDIS with help of radar overlay and terrestrial bearing. Unmanned vessels are in much worse situation as they rely solely on GNSS. International Organization of Lighthouse Authorities (IALA) proposed land based resilient PNT system named Enhanced Radar Positioning System (ERPS). It consists of modified racons (eRacons) and modified radars (eRadars) and is independent of GPS. eRacons provide their absolute positions in encoded response signals. eRadars use these positions for calculation own vessel's position [26]. Proposed system may provide backup navigation for unmanned vessels in confined waters but is not yet operational. ECDIS specific cyber-attack was reported by employees of security firm Naval Dome. During penetration test they acquired access to ship's navigation, radar, engines, pumps, and machinery by sending email to the captain. [12]. Position of vessel was shifted on ECDIS screen and remaining parameters were modified in way that they looked normally for officer on bridge.

4.3 *AIS*

International Convention for Safety of Life at Sea (SOLAS) introduced requirement for vessels to be fitted with AIS transponders [6]. AIS onboard device provides shore stations, nearby vessels and aircrafts with vessel and safety related information, receives such information from other transponders, tracks and monitors movement of vessels and displays transmitted AtoN information. System uses for communication two narrow radio frequency (RF) channels within marine VHF band. Received onboard information is processed by software (SW) and displayed in graphic and text form on ECDIS, radar and ARPA for navigation, collision avoidance and rescue purposes. On shore AIS information is used for vessel traffic monitoring and management by Vessel Traffic Management System (VTMS) and online AIS providers. In present state AIS has numerous vulnerabilities which should be addressed before introduction of autonomous vessels. Table 3 summarizes identified threats to AIS.

Table 3. AIS identified threats. Modified from [30].

Category	Threat	SW	RF
Spoofing	Ships	Yes	Yes
	AtoN	Yes	Yes
	SAR	Yes	Yes
	Collision		Yes
	AIS SART		Yes
	Weather Forecast		Yes
Hijacking	Hijacking	Yes	Yes
Availability	Communication slot starvation		Yes
Disruption	Frequency hoping		Yes
	Timing attack		Yes

Lack of encryption in AIS transmission allows hackers to interfere with all its functions including programming fake movement of non-existent vessel with simple equipment. [16].

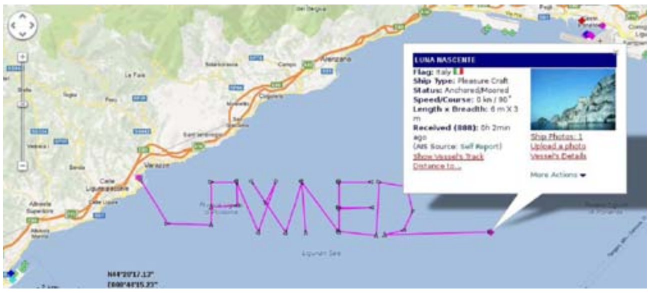


Figure 5. Trajectory of non-existent vessel showing ‘pwned’ [16].

Word ‘pwned’ used in AIS penetration test stands for ‘You have been hacked.’ AIS today is essential for INS providing information related to collision avoidance and situational awareness. Improper operation or false information can be disastrous for present and future shipping.

Integration of navigational equipment significantly changed design of marine radars. Analogue signal from transceiver is converted into digital form for processing by purpose made software. Capability of modern digital radars are far greater of their analogue predecessors, but digital processing makes them vulnerable to attack. During penetration test conducted by Naval Dom engineering team hacked into marine radar and was able to manipulate equipment’s software to delete targets from the screen [12]. Figure 6 shows attacked radar with most of the echoes deleted from the screen. Remaining targets were left to convince operator in correct operation of the radar. During the night or poor visibility such situation may become extremely dangerous. Vessel was left without most important collision prevention aid.

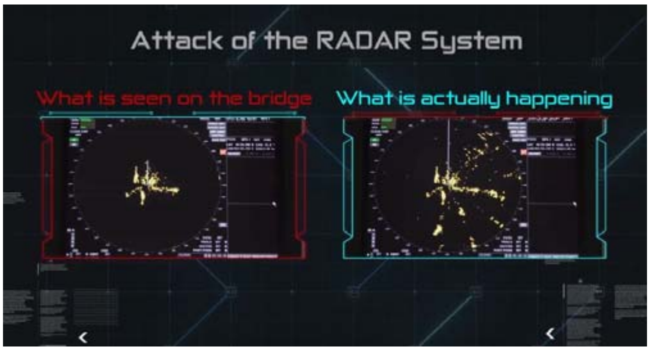

Attack of the RADAR System
What is seen on the bridge
What is actually happening

Figure 6. Attacked digital radar with most of targets deleted [12].

5 COMMUNICATION

Satellite communication is a dominant type of maritime mobile communication both for emergency and business use. Vessels operating under GMDSS rules in area A3 are fitted with Inmarsat communication equipment [6] using geostationary satellites. Primary purpose of it is communication in emergency, which is charge free. Inmarsat provides also payable business communication. Communication based on geostationary satellites has limited range in polar waters due to low elevation of satellites above horizon. Many shipping companies additionally are using satellite communication providers with their medium and low orbits satellite networks allowing for voice data transfer all around the world. Depending on service provider differ types of equipment and communication platform are used. In 2015 researcher reported that with inexpensive equipment was able to gain access to information in Globalstar uplink and could inject his own data. Lack of data encryption in modem transmitter chip was the vulnerability exploited in this experiment. [22]. Besides of hardware weak or missing protection against malicious attack software used as communication platforms is vulnerable and can be used as gateway to ship’s networks. In 2016 cybersecurity firm IOActive found two serious vulnerabilities in communication platform AmosConnect 8.0 provided by Stratos company, subsidiary of Inmarsat, for integration of large group of messaging tools for narrow band satellite communication [23]. Inmarsat first responded with reverting to older version of AmosConnect and finally withdrew software from use. and launched Fleet Secure Unified Threat Management (UTM) in 2022 [28]. Compromised communication can deny vessel’s staff access to information needed for efficient and save voyage but also can leave crew without ability to control own ship when navigation, steering and propulsion systems are penetrated by attackers. To alleviate problems with communication on short distances, when is the most needed, IALA proposed introduction of VHF Data Exchange System (VDES) [5]. Using radio frequency channels within maritime VHF band vessel is linked with terrestrial or satellite communication network providing alternative to maritime satellite communication. System is not intended to work on high seas but within range of VHF transmission it can be invaluable providing resilient means of communication.

6 CONCLUSIONS

Number cyber-attacks against shipping industry is rising rapidly within last few years threatening both shipping lines and individual vessels. Attacks directed against biggest shipping companies succeeded and incurred large financial loses. It happened despite professionally managed IT networks in large companies. Attacks aimed against ships targeted both IT and OT technologies. Compromised communication may seriously hamper ship's operations and provides gateway to OT equipment. Ongoing convergence vessel's IT and OT technologies makes maritime transport more vulnerable. Some research penetration test exposed susceptibility of technologies currently in use to simple methods of attack. Numerous vulnerabilities were found in both in software managing ship's systems and in unprotected hardware. Technologies used today onboard are not sufficiently resilient against cyber-attacks. It may lead to delay of introduction of autonomous vessels until revealed vulnerabilities are properly addressed.

REFERENCES:

[1] AGCS. Safety and Shipping Review 2022.p.9. Munich 2022

[2] Balduzzi M., Pasta A., Wilhoit K., A Security Evaluation of AIS Automated Identification System, https://www.madlab.it/papers/ais_acsac14.pdf

[3]] Direnzo III J., Drumhiller N. K., Roberts F. S., Issues in Maritime Cyber Security, p.20,23. Westphalia Press, Washington D.C. 2017

[4] Finnish National Emergency Supply Organization, The Maritime Transport Pool, Maritime Cybersecurity-Best Practices for Vessels, p.5, Helsinki 2021

[5] IALA Guideline G1117 VHF Data Exchange System (VDES) Overview Edition 3.0, electronic edition, Saint Germain en Laye, 2022.

[6] IMO, International Convention of Safety of Life at Sea (1974), Electronic Edition 2020, London

[7] IMO, Resolution MSC.252(83) Adoption of the Revised Performance Standards for Integrated Navigation Systems (INS), London, 2007

[8] INTERTANKO, Jamming and spoofing of Global Navigational Satellite System (GPS), p.5,14, London 2019

[9] Lind M., Michaelides M., Ward R., Watson R. T., Maritime Informatics, p.43, Springer, Cham 2021

[10 National Institute of Standards and Technology, US Department of Commerce, Guide to Industrial Control Systems (ICS) Security, p. 2-16,2-17, Gaithersburg, 2015

[11] Pawelski J., (2022) Barriers impending introduction of autonomous vessels. Scientific Journals of the Maritime University of Szczecin, Zeszyty Naukowe Akademii Morskiej w Szczecinie 72 (144), p.39, Szczecin 2022

[12] https://blog.geogarage.com/2017/12/nightmare-scenario-ship-critical.html,accessed 10.02.2023

[13] https://rntfnd.org/2017/11/25/hackers-took-full-control-of-container-ships-navigation-systems-for-10-hours-ihs-fairplay/,accessed 02.02.2023

[14] https://vesselautomation.com/maritime-cyber-attacks/,accessed 10.02.2023

[15] https://www.bimco.org/contracts-and-clauses/bimco-clauses/current/cyber-security-clause-2019,accessed 20.01.2023

[16] https://www.blackhat.com/docs/asia-14/materials/Balduzzi/Asia-14-Balduzzi-AIS-Exposed-Understanding-Vulnerabilities-And-Attacks.pdf,accessed 21.01.2023

[17] https://www.csoonline.com/article/3218104/stuxnet-explained-the-first-known-cyberweapon.html,accessed 02.02.2023

[18] https://www.cybersecurity-review.com/news-july-2020/maritime-cyber-attacks-increase-by-900-in-three-years/,accessed 04.02.2023

[19] https://www.darkreading.com/attacks-breaches/plcs-possessed-researchers-create-undetectable-rootkit,accessed 17.02.2023

[20] https://www.darkreading.com/threat-intelligence/stealthy-new-plc-hack-jumps-the-air-gap,accessed 11.02.2023

[21] https://www.darkreading.com/vulnerabilities-threats/hijacking-a-plc-using-its-own-network-features,accessed 09.02.2023

[22] https://www.defenseone.com/technology/2015/08/hacker-cracks-satellite-communications-network/118915/,accessed 17.02.2023

[23] https://gcaptain.com/inmarsat-shipboard-communication-platform-found-vulnerable-to-hacking/,accessed 08.02.2023

[24] https://gcaptain.com/international-maritime-organization-hit-by-cyber-attack/,accessed 17.02.2023

[25] https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/,accessed 12.02.2023

[26] https://www.iala-aism.org/e-bulletin/enhanced-radar-positioning-system/,accessed 15.02.2023

[27] https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/,accessed 15.02.2023

[28] https://www.inmarsat.com/en/news/latest-news/maritime/2022/fleet-secure-cybercrime-unified-threat-management.html,accessed 14.02.2023

[29] https://www.iua.co.uk/IUA_Member/Clauses/eLibrary/Clauses_Search.aspx?CAT=PAC,accessed 08.02.2023

[30] https://www.madlab.it/papers/ais_acsac14.pdf,accessed 10.02.2023

[31] https://www.missionsecure.com/resources/comprehensive-guide-to-maritime-security-ebook, accessed 15.022023

[32] https://www.otorio.com/blog/maritime-port-cyber-security-the-achilles-heel-of-the-global-economy/,accessed 17.02.2023

[33] https://www.pentestpartners.com/security-blog/hacking-tracking-stealing-and-sinking-ships/,accessed 14.02.2023

[34] https://www.techopedia.com/iiot-vs-iot-the-bigger-risks-of-the-industrial-internet-of-things/2/34394#:~:text=The%20defining%20difference%20between%20Internet%20of%20Things%20%28IoT%29,as%20manufacturing%2C%20supply%20chain%20monitoring%20and%20management%20systems., accessed 07.02.2023