Network Attacks Against Marine Radar Systems: A Taxonomy, Simulation Environment, and Dataset

Konrad Wolsing*†, Antoine Saillard*†, Jan Bauer*, Eric Wagner*†, Christian van Sloun†,
Ina Berenice Fink†, Mari Schmidt*, Klaus Wehrle†*, and Martin Henze‡*
*Cyber Analysis & Defense, Fraunhofer FKIE, Germany · {firstname.lastname}@fkie.fraunhofer.de
†Communication and Distributed Systems, RWTH Aachen University, Germany · {lastname}@comsys.rwth-aachen.de
‡Security and Privacy in Industrial Cooperation, RWTH Aachen University, Germany · henze@cs.rwth-aachen.de

***Abstract*—Shipboard marine radar systems are essential for safe navigation, helping seafarers perceive their surroundings as they provide bearing and range estimations, object detection, and tracking. Since onboard systems have become increasingly digitized, interconnecting distributed electronics, radars have been integrated into modern bridge systems. But digitization increases the risk of cyberattacks, especially as vessels cannot be considered air-gapped. Consequently, in-depth security is crucial. However, particularly radar systems are not sufficiently protected against harmful network-level adversaries. Therefore, we ask: Can seafarers believe their eyes? In this paper, we identify possible attacks on radar communication and discuss how these threaten safe vessel operation in an attack taxonomy. Furthermore, we develop a holistic simulation environment with radar, complementary nautical sensors, and prototypically implemented cyberattacks from our taxonomy. Finally, leveraging this environment, we create a comprehensive dataset (RadarPWN) with radar network attacks that provides a foundation for future security research to secure marine radar communication.**

***Index Terms*—Marine Radar; Maritime Cyber Security; Radar Dataset; Navico BR24; NMEA 0183; AIS**

I. Introduction

Radio detection and ranging (radar) technology enables the detection and localization of objects through the emission of electromagnetic waves and the reception of their reflection. While radar technology is critical in various applications, onboard radar systems are particularly important for the navigation of aircraft and vessels. In the maritime domain, radar increases the safety of sea traffic by showing landmasses and physical objects on dedicated displays. Additionally, known landmarks or special aids to navigation, *e.g.*, reflectors, allow radar to serve as a position fix. Especially in busy areas or low visibility conditions, radar is crucial to prevent collisions. The international SOLAS Convention [28] therefore requires radars for passenger vessels or vessels above 300 gross tonnage.

On a vessel's bridge, radar data is processed and fused with information from other nautical sensors to generate predictive motion vectors of other vessels. It is also supplemented by the automatic identification system (AIS) [4], [19], a maritime radio broadcast system to exchange identity, position, and course information of ships in geographic proximity. All these components are connected to an integrated bridge system (IBS), usually via Ethernet-based IT networks [17], [21], [25].

However, individual maritime components and the communication channels over which sensitive navigation data is transmitted are rarely secured in practice, resulting in serious risks of cyberattacks. These include attacks targeting IBSs [17] to disrupt operational processes, manipulate nautical situation pictures, or impact navigational decisions. Both can have serious consequences since accidents cause immense economic damage, as the Suez Canal incident in 2021 revealed [20], and ultimately endangers people's and the environment's safety.

While the security implications of insecure maritime systems have been well studied for typical communication protocols [7], [32], navigation systems [1], [2], [21], IBSs [3], [17], and AIS [4], [16], marine radar security has not been the focus of research so far. As many marine navigation radars rely on non-standard, often vendor-specific, and proprietary communication protocols, a comprehensive cybersecurity and threat analysis is challenging and requires the identification of inherent similarities. Still, radar communication, in particular, is vulnerable to cyberattacks, as proofs-of-concepts for the related aviation sector have demonstrated [10], [11], [35].

Despite the general knowledge that radar communication is vulnerable, the exact capabilities, especially in the maritime sector, remain unknown. The resulting lack of awareness and information restricts the development of effective mitigations. To bridge this gap, in this paper, we study the cyberthreats resulting from radar communication vulnerabilities in maritime systems. More precisely, our main contributions to improving the security of marine radar systems are as follows:

- We identify network-level attacks against marine radar and organize them in a comprehensive taxonomy to serve as a foundation for developing future countermeasures (Sec. IV).
- We implement a holistic simulation environment (Sec. V) based on the representative Navico BR24 protocol and execute attacks against radar communication deduced from the taxonomy in realistic scenarios as intelligent multi-sensor attacks with the help of our Radar Attack Tool (Sec. VI).
- Finally, we derive RadarPWN[1], an extensive dataset comprising various sophisticated attacks on marine navigation radar, which lays the foundation for future security research and the development of mitigation techniques (Sec. VII).

[1]The RadarPWN dataset, the simulation environment's source code, and the radar attack tool are made available at https://doi.org/10.5281/zenodo.6805559

 DOI: 10.1109/LCN53696.2022.9843801

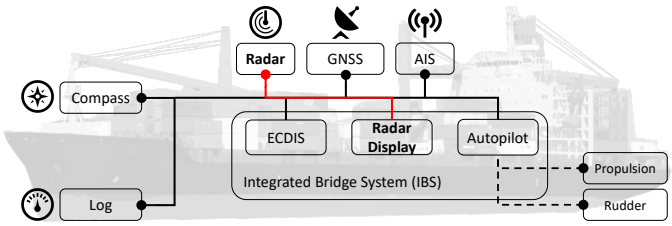


Fig. 1. Modern maritime systems comprise a multitude of navigational sensors interconnected with a shared Ethernet-based network. The use of proprietary yet insecure radar network protocols poses a potential cybersecurity risk.

II. Background on Marine Radar and Bridges

The primary duty of a vessel's crew is a safe operation, which especially comprises navigation and collision avoidance. To this end, they are assisted by various digital systems.

A. Digital Systems Onboard Vessels

Safe operation demands precise and extensive environmental observations, *i.e.*, measuring the heading with a compass or the speed with a log. Suchlike sensors are nowadays fully digitized and augmented with global navigation satellite systems (GNSSs), enabling worldwide localization (*cf.* Fig. 1). In addition, AIS transceivers periodically broadcast vessels' positions increasing situational awareness and assisting in collision avoidance, especially in traffic-dense areas.

While these systems contribute to either navigation or collision avoidance exclusively, radar is capable of addressing both: While static landmasses or buoys are visualized, automatic tracking of moving objects, enabled by an automatic radar plotting aid (ARPA), can reveal another vessel's course (*cf.* Fig. 2). Moreover, measuring the bearing and distance to charted objects also enables secondary means for localization.

All, sometimes even redundant, sensors distributed across the entire vessel get aggregated into a central IBS and visualized on nautical displays, *e.g.*, electronic chart display and information systems (ECDISs), to support the crew's decisions. Based on that data, an autopilot may control the rudder and propulsion, steering along pre-defined waypoints.

The foundation to transmit sensed data to the IBS is usually a regular Ethernet-based network, turning a modern vessel into a tightly integrated cyber-physical system [25]. A common solution for the transmission of nautical data, except for radar, is NMEA 0183. Developed initially as a human-readable, serial point-to-point protocol, this standard has been transferred to multicast UDP communication over conventional Ethernet [21], [25]. However, NMEA 0183 over Ethernet is neither encrypted nor integrity protected.

B. Overview of Radar Protocols

Similar to nautical sensors connected to the IBS, marine radar systems typically include a sensing device attached to an antenna and a display and control unit. The antenna, placed on the exterior of a vessel's hull, emits electromagnetic waves in short pulses while rotating along its vertical axis. By measuring the time and amplitude of backscattered waves (hereinafter

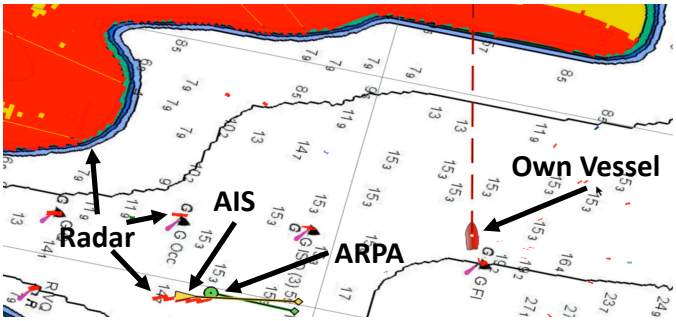


Fig. 2. Radar visualizes landmasses, buoys, and surrounding vessels (red). Moving targets can be tracked with ARPA (green circles), which are additionally complemented by AIS broadcasts (yellow triangles).

referred to as echoes), obstacles can be located relative to the antenna's position. The display and control unit is placed inside the IBS and typically connected via existing Ethernet.

Unlike other maritime data communication (*cf.* Sec. II-A), no standardized radar protocol exists. Instead, vendors use proprietary protocols to transmit radar images to the IBS and send back control sequences. To conduct a comprehensive security analysis, we first investigate the inherent (dis)similarities of eight protocol families across three vendors by analyzing their respective implementations in the open source radar_pi plugin [24] for OpenCPN [23], a widely used chart plotter.

As shown in Tab. I, all eight protocols share a similar data structure transmitting echoes' reception strengths to the display in scanlines, likely due to the common underlying measurement principle. Scanlines encode a single bearing or portion of an azimuthal degree as byte arrays where the first value corresponds to the bin closest to the radar, *i.e.*, the first echo returning to the antenna, and subsequent values are progressively farther. The radar image's resolution depends on the scanline array's length (radial) and the number of scanlines (angular) required to make up a 360 ° sweep. Due to size limitations in IP/UDP, a datagram usually encodes a fraction of the image (*e.g.*, 32 scanlines per datagram for Navico BR24).

All eight protocols have in common that they rely on unprotected UDP transmissions posing a cybersecurity threat. Furthermore, discovering radar devices within a network is often made simple through the use of statically assigned IP addresses and the broadcasting of UDP packets.

However, radar protocols still exhibit slight flavors between vendors and individual radar families. The main differences include the interpretation of a scanline's range, its conversion to azimuth angles, the image's resolution, and the datagram header formats. Moreover, adjusting parameters like the resolution during operation usually includes vendor-specific control sequences. Overall, Navico BR24 shares the most common features, as can be seen in Tab. I. Because its data and control structure are, furthermore, well documented [14], it is chosen for our further research. With its typical lack of protective network security features, it serves as a representative protocol for developing our novel marine radar attack taxonomy that takes the insufficient security of maritime systems into account.

TABLE I
THE EIGHT MARINE RADAR PROTOCOLS UNDER STUDY ALL RELY ON UNPROTECTED UDP MULTICAST CONNECTIONS. PRIMARILY THE RESOLUTION AND DATAGRAM ENCODING DIFFER SLIGHTLY.

Vendor	Protocol	UDP	Auth.	Discovery	Scanlines*	Resolution*		
						Echo	Angular	Radial
Garmin	HD	✓	✗	static IP	1	1 bit	720	252
	xHD	✓	✗	static IP	1	8 bit	1440	705
Navico	3G	✓	✗	advertised	32	8 bit	2048	1024
	4G	✓	✗	advertised	32	8 bit	2048	1024
	BR24	✓	✗	static IP	32	8 bit	2048	1024
	HALO	✓	✗	advertised	32	8 bit	2048	1024
Raymarine	E120	✓	✗	advertised	1024	8 bit	2048	1024
	Quantum	✓	✗	advertised	1	8 bit	250	250

Properties marked with * indicate maxima.

III. RELATED WORK ON RADAR CYBERSECURITY

Maritime cybersecurity has increasingly become a subject of interest to researchers. Consequently, attacks against IBSs [17] and associated components such as GNSS [5], [6], NMEA [7], [32], or AIS [4], [5], [19] are well researched. In contrast, the security-related investigation of marine radar systems constitutes a critical gap in the current research landscape, even though existing research is alarming: A vulnerability scan of the shipboard radars of two oil/chemical tankers revealed a broad range of security risks (*e.g.*, missing access control) and attack points [31]. Outside the maritime sector, Cohen *et al.* [11] provide a general threat taxonomy and a concerning attack scenario by realistically simulating the manipulation of radar data in air traffic control. Nevertheless, thorough security analyses regarding marine radar systems and specific security solutions are missing to date.

While different countermeasures to thwart maritime attacks exist, they focus on AIS [16], NMEA [7], and GNSS [6], [18] or offer general security improvements, *e.g.*, by segmenting the network topology into different zones [26]. Furthermore, although not specific to maritime settings, multiple security solutions and mitigation approaches target radar systems in general or specific application fields. For example, deep learning-based anomaly detection can detect manipulations of data streams between the radar and the control system, as demonstrated with real radar data from experimental [12] and aerial radar systems [15]. Besides detective measures, hash-based integrity checks and encryption were developed for the ASTERIX protocol used for data exchange in air traffic control and evaluated within simulated communication between aircraft and airport control [10]. Finally, algorithmic approaches, including numerical evaluation, aim toward consistent snapshots of distributed radar networks to increase resilience [22] or combat false data injection [27], [35].

These research efforts provide valuable insights and directions for improving radar-related security. However, it is unlikely that these can be readily transferred to maritime scenarios. For instance, radar data from *stationary* air traffic control does not necessarily serve for evaluating *mobile* shipboard radar solutions. Furthermore, the datasets and simulations used in existing radar-related work, often depending on hardware access [15], cannot be used to reliably develop and evaluate new maritime-specific security solutions. Thus, related work does not sufficiently provide the means to analyze, develop, and evaluate security solutions for marine radar systems.

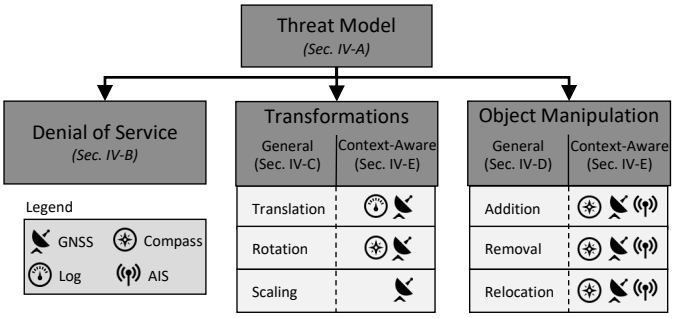


Fig. 3. Network-based attacks on marine radar systems can be classified into *Denial of Service*, *Transformation*, and *Object Manipulation*. By incorporating external situational knowledge (indicated by respective icons), these basic types can be enhanced to stealthier *context-aware* attacks.

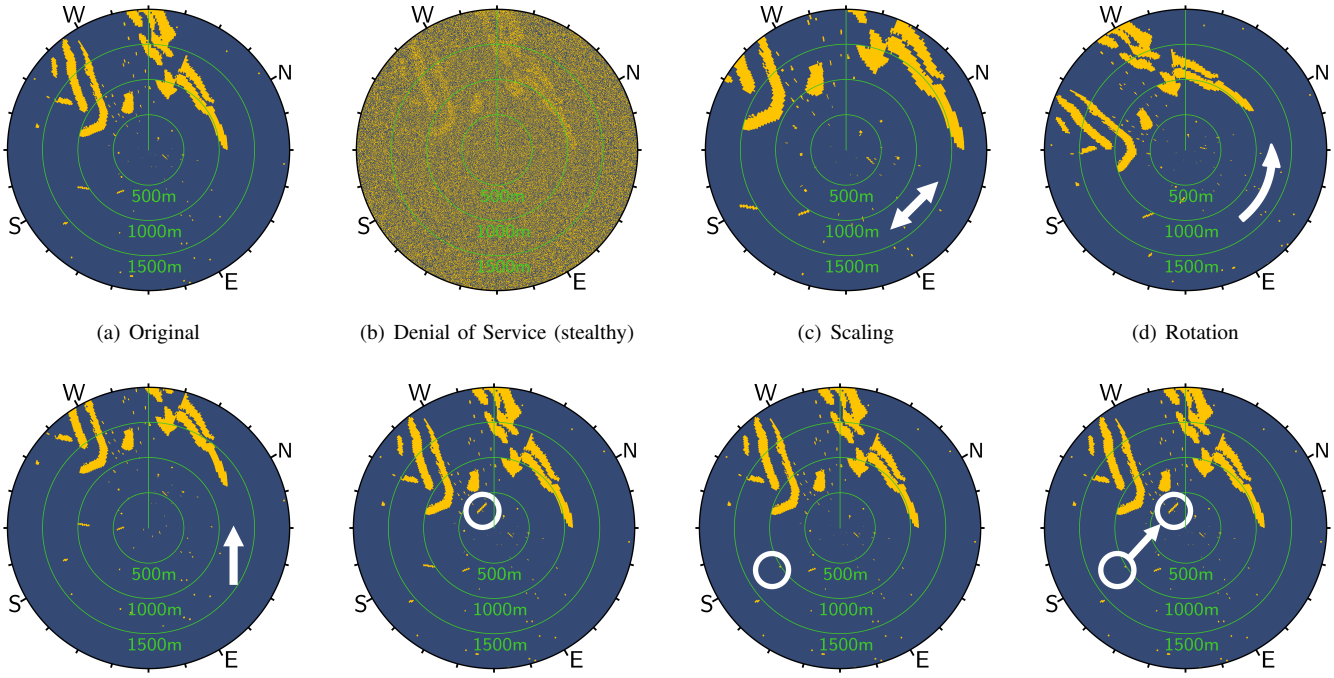
IV. TAXONOMY OF NETWORK-BASED RADAR ATTACKS

To address the gap in research on *network* cybersecurity of marine radar, we develop an attack taxonomy and discuss the consequences individual types of attacks can have on nautical decisions. As depicted in Fig. 3, our taxonomy covers different types of manipulations of the visualized radar data. Starting from a threat model (Sec. IV-A), we explore vectors for Denial of Service (DoS) attacks (Sec. IV-B) before moving on to attacks involving basic image transformations (Sec. IV-C) or targeted object manipulations (Sec. IV-D) and closing with progressively stealthier context-aware attacks (Sec. IV-E).

A. Threat Model

We consider an attacker who intends to manipulate the navigation radar image shown in the IBS by manipulating the transmission of radar network packets. Tampering with the displayed contents may affect nautical decisions and result in the inability to navigate securely or, in the worst case, endanger the vessel or its surroundings. While maritime networks are supposedly *water*-gapped, *i.e.*, physically isolated, they still expose significant attack surfaces. Typical attack vectors, *e.g.*, ranging from satellite communication to human factors, can lead to compromised devices and malware implants [5], [9], [17], [33]. Even a direct compromise of the radar unit is possible, *e.g.*, by exploiting software and operating systems [31].

In this paper, we specifically focus on an attacker who has already gained control over an arbitrary network device with the ability to read and alter radar communication due to the lack of integrity protection (*cf.* Sec. II-B). These typical Machine-in-the-Middle (MitM) attack capabilities can then be enhanced by overhearing other nautical information, such as the vessel's current position, to further improve the manipulated image's realism and conduct situative and stealthy attacks. This is simplified by the fact that standard nautical protocols, such as NMEA 0183 over Ethernet, also lack confidentiality (*cf.* Sec. II-A). It should be noted, however, that even an attacker on-the-side that cannot directly manipulate



(a) Original (b) Denial of Service (stealthy) (c) Scaling (d) Rotation

(e) Translation (f) Object Addition (g) Object Removal (h) Object Relocation

Fig. 4. Our taxonomy defines seven classes of attacks against marine radar. Manipulating the radar image can lead to severe consequences if misinterpreted by the crew. While DoS attacks (Fig. 4(b)) disable the radar or obscure smaller objects through artificial noise, transformation attacks (Fig. 4(c)–(e)) affect derived nautical data, *e.g.*, distances to landmasses. In contrast, manipulating, *e.g.*, surrounding ships' radar reflections (Fig. 4(f)-(h)) endangers vessels' safety.

the radar communication can still cause significant damage by injecting malicious radar data superimposing the original data. Nevertheless, this paper focuses on MitM attacks because the resulting consequences are potentially more deceptive and difficult to address in future security mechanisms.

B. Denial of Service Attacks

First, we consider DoS attacks, where the attacker impedes the regular use of the radar, which can take different forms. The simplest but most detectable form is blocking all communication between the radar and display unit (*cf.* Fig. 1). However, due to the lack of integrity protection, DoS attacks can also be carried out by altering the displayed content. In this case, arbitrary modifications are possible that reduce the usefulness of the radar image, such as freezing or progressively blurring it. In both cases, an observer on the bridge might remain unaware of the attack and could attribute the distortions to a hardware failure or environmental conditions. Fig. 4(b) illustrates the result of a blurring DoS attack compared to the original radar image depicted in Fig. 4(a). Thus, a paralyzed radar system has detrimental consequences as it reduces vessels' ability to localize and navigate.

C. Transformation Attacks

Since attackers can manipulate the radar image arbitrarily (*cf.* Sec. IV-B), they can apply general image transformations. Therefore, we consider the three fundamental transformations (scaling, rotation, and translation) that can be used to manipulate seafarers' perception of their current environment and discuss their value for an attacker. To stretch on the consequences of such manipulations, one must consider that radar is a navigational instrument used to determine ranges and bearings, especially under poor visibility conditions. Thus, wrong navigational decisions can ultimately lead to accidents.

1) Scaling: Scaling the radar image produces a mismatch between the dialed and displayed range. Increasing the zoom level, *i.e.*, displaying a smaller portion of the radar image and thus increasing perceived distances (*cf.* Fig. 4(c)), is trivial once protocol datagrams can be manipulated. As all information of the smaller portion is contained within the original larger image, it can be cropped and re-scaled. If the zoom level is instead decreased, additional information is required to fill in the blank spaces at the edge of the screen. However, these could be (artificially) generated, *e.g.*, from cartographic information, according to the vessel's current position.

2) Rotation: Similarly, rotating the radar image disturbs the perceived bearing of landmarks or other vessels (*cf.* Fig. 4(d)). The consequences of such an attack can be detrimental, as a false bearing to a vessel on a collision course can reduce valuable time to initiate evasion maneuvers or a rotation can induce a course correction resulting in a displacement.

3) Translation: Third, translating the radar image sideways or along the direction of travel can create the impression of drift or velocity changes. For instance, as shown in Fig. 4(e), translation in the direction of the vessel's heading gives the impression of a slowdown and increases the perceived

remaining distance to hazards, thus increasing the risk of head-on collisions. Technically, besides redrawing the transmitted echoes, this effect can equivalently be achieved by progressively increasing the delay between network packets. However, a translation induces a parallax effect, *i.e.*, objects become visible or disappear from the radar display due to the changed perspective, which the attacker cannot easily compensate for.

Overall, image transformations are effective means of performing targeted attacks on nautical decisions with hazardous consequences, as the position of a vessel could be misjudged, and obstacles may not be adequately avoided.

D. Object Manipulation Attacks

While image transformations are well suited to manipulate static surroundings (*e.g.*, landmasses), an attacker could also selectively manipulate stationary/mobile objects, *e.g.*, aids to navigation or other vessels traveling the seas. By selectively manipulating portions of a radar image, adding, removing, and/or repositioning individual radar echoes is feasible.

1) Addition: Adding new objects (moving or stationary) can be performed by manipulating the datagram and scanline contents for the specific location to resemble the desired radar echo, as shown in Fig. 4(f). A new echo may cause the navigator to adjust the vessel's course and force it to enter dangerous waters in an attempt to avoid the supposed collision.

2) Removal: In contrast, an attacker could also manipulate the network traffic to hide the presence of certain radar echoes (*cf.* Fig. 4(g)), *e.g.*, to provoke a collision. While visual surveillance could identify the existence of the removed object, poor visibility can shorten the reaction time for adequate evasion maneuvers, thus making a collision inevitable.

3) Relocation: Lastly, an attack can relocate objects (*cf.* Fig. 4(h)), which can be seen as a combination of the two previous attacks. Here, the difference in the position between original and relocated objects just becomes progressively erroneous, whereas the (non-)existence of added or removed objects can be verified visually. Hence, such a manipulation is harder to detect, even in good visibility conditions.

While object manipulation requires a detailed analysis of the image's content to identify individual echoes, redrawing the data at network-level remains fairly simple as it is analog to, *e.g.*, adding random noise (*cf.* Sec. IV-B). At the same time, they show that even a minimal change in the information displayed by the radar can lead to far-reaching consequences.

E. Sophisticated Context-Aware Radar Manipulations

All considered attacks enable an attacker to change the displayed radar image arbitrarily. So far, they are conducted regardless of the current navigational situation, and the outcome, *e.g.*, a rotation attack placed during a critical course correction, could be much more severe. In addition, since radar is not the only shipboard system used for navigational purposes (*cf.* Sec. II-A), targets removed from the radar display may still be visible via other means such as AIS.

Conversely, sophisticated, context-aware, and situative radar attacks can realize stealthy and hardly detectable attacks. Due to the nature of modern vessels' network traffic, which primarily consists of broadcasted and unencrypted UDP messages (*cf.* Sec. II-A), there are unique opportunities in which specific attacks benefit from additional external information. In Fig. 3, we depict relevant relations between attack types and common external information and highlight two examples of how to utilize them in the following.

First, *passively* overhearing navigational status updates, such as the GNSS position, speed, or heading, allows attacks to be triggered remotely upon arrival in a given region or translating the radar image in the vessel's direction during acceleration for further disguise. Also, potential targets for the removal attacks can be inferred from AIS or ARPA. Second, *actively* manipulating the network's traffic, as proven successful [17], can enhance radar manipulations, *e.g.*, by dropping AIS-related messages during an object removal. In that case, the MitM attacker needs to be capable of dropping the related information. Unless seafarers can visually confirm the incorrectness of the data provided by the IBS, it is unlikely that such sophisticated attacks will be detected.

Overall, the taxonomy highlights that attacks against marine radar systems' network communication can potentially be performed easily and have far-reaching consequences, which might not be directly detectable by the vessel's crew.

V. Marine Radar Simulation Environment

Radar attacks pose a severe threat to the safe operation of vessels. Being theoretically feasible (Sec. IV), it remains unknown whether these can be conducted *practically* against maritime systems. Because attacking real vessels introduces a serious operational risk, we use simulation for our evaluation to safely conduct radar attacks. However, there exists no holistic maritime simulation framework to adequately perform advanced network-based radar attacks (*cf.* Sec. III). Therefore, we set out to design our own. Using a simulation approach provides further benefits, including reproducibility and adaptability in the case of upcoming attacks or architectures. Moreover, it can serve as an evaluation platform for radar security solutions by the research community. To this end, we initially define requirements to be fulfilled (Sec. V-A), describe our final design (Sec. V-B), and assess our environment (Sec. V-C).

A. Requirements for a Radar Simulation Environment

To develop a simulation environment that also serves as a scientific tool, we refer to common practices and guidelines [34]. First, details about the simulation must be made *transparent* to avoid false conclusions from conducted experiments. Next, *adaptability* facilitates the future addition of components, *e.g.*, implementing more sophisticated radar attacks or protocols. Ensuring *realism*, *i.e.*, that deduced results are transferable to the real world, is of utmost importance since only then do approaches also tackle the pressing challenges in real systems. Finally, *availability* and *replicability* are important properties, allowing others to reproduce experiments. During the following design of the radar simulation environment, we take special care to fulfill these properties.

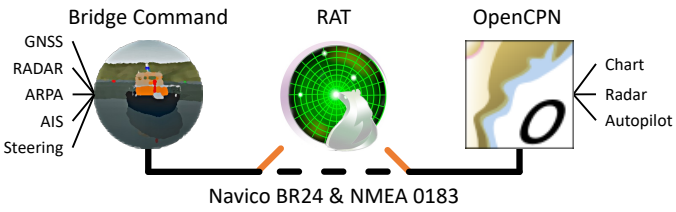


Fig. 5. The radar simulation environment consists of two components. Bridge Command (BC) simulates a virtual ship and surrounding vessels, while OpenCPN serves as a chart plotter, including a radar display and an autopilot. Finally, RAT (Sec. VI) injects radar cyberattacks into the network traffic.

B. Design of a Radar Simulation Environment

To design a radar simulation environment with a high degree of *realism*, we model all relevant parts of modern vessels according to the model established in Fig. 1 (*cf.* Sec. II-A). This involves sensors measuring the vessel's simulated surroundings, especially radar, including an ARPA, GNSS, and AIS, as well as actuators controlling the vessel in speed and direction. These components should be connected over regular Ethernet and communicate with an IBS via common maritime standards and radar protocols (*cf.* Sec. II-B), against which cyberattacks will be conducted subsequently. Our simulation environment is designed along this generic model (*cf.* Fig. 5).

1) Radar and Environmental Simulation: As a basis for the marine radar and environmental simulation, we choose Bridge Command (BC) [8], an open source software for training navigational and radar skills, which has also found use in research [1], [30]. It features realistic virtual maps, including terrain, other surrounding vessels, and buoys, which can all affect the radar image, as well as an integrated ARPA. BC allows users to pilot a vessel while corresponding nautical data is relayed over the network via NMEA 0183.

Since BC does not natively support the transmission of radar images to radar displays over the network, we add this functionality by implementing a radar protocol. We choose the representative Navico BR24 radar protocol family (*cf.* Sec. II-B) and further enhance the resolution of BC's radar simulation to increase the radar's *realism*. Finally, we add support for broadcasting AIS Class A reports, signaling the position, heading, and speed of surrounding vessels, as context-aware attacks require this information (*cf.* Sec. IV-E).

2) Designing Realistic Scenarios: Besides modeling digital systems, designing realistic scenarios is of equal importance. First, the terrain significantly influences the final radar image, and second, potential radar security solutions have to cope with varying environmental conditions in practice, *i.e.*, operate in unknown environments. To this end, we design three scenarios with diverging properties, as shown in Tab. II.

BC already comes with several maps, all of which include terrain, buoys, and vessels, from which we select *Simple Estuary*, a fictional map, and *Santa Catalina*, modeled like the real island off the coast of California. As both scenarios mainly consist of steep shorelines and mountains, we add the mostly flat *Rostock* scenario, a German port on the Baltic Sea. We generated the map from actual height cartography material and added buoys according to nautical charts. Furthermore, surrounding vessels in the scenarios Santa Catalina and Rostock were modeled using historical AIS data of both regions.

TABLE II
THE SIMULATION ENVIRONMENT FEATURES THREE SCENARIOS WITH DIVERGING MAPS, VESSELS, AND ROUTES FOR THE AUTOPILOT.

Scenario name	Map	Vessels	Route
Simple Estuary	hilly estuary (fictional)	13 (fictional)*	5.9 nm*
Santa Catalina	hilly island (real)	90 (historical AIS)*	5.5 nm*
Rostock	flat harbor (real)*	76 (historical AIS)*	3.9 nm*

Items marked with * were contributed by us.

3) IBS and Autopilot: To model the IBS, we choose OpenCPN [23], an open source chart plotter and navigation aid. OpenCPN receives the maritime network protocol data and simultaneously serves as the radar display and control unit via its radar_pi plugin [24] (*cf.* Fig. 5). Finally, to tackle the *replicability* of individual experiments and to ensure that the simulated vessel navigates along the same waypoints within the environment, we leverage OpenCPN's autopilot functionality coupled with our autopilot implementation in BC using the exchange of standard NMEA 0183 autopilot sentences via the network. For each scenario, we mark out a predefined route (*cf.* Tab. II) with a duration of roughly 18 minutes as input for the autopilot.

Overall, the radar simulation environment allows piloting vessels in realistic scenarios along repetitive paths and observing the generated network traffic transmitted towards an IBS.

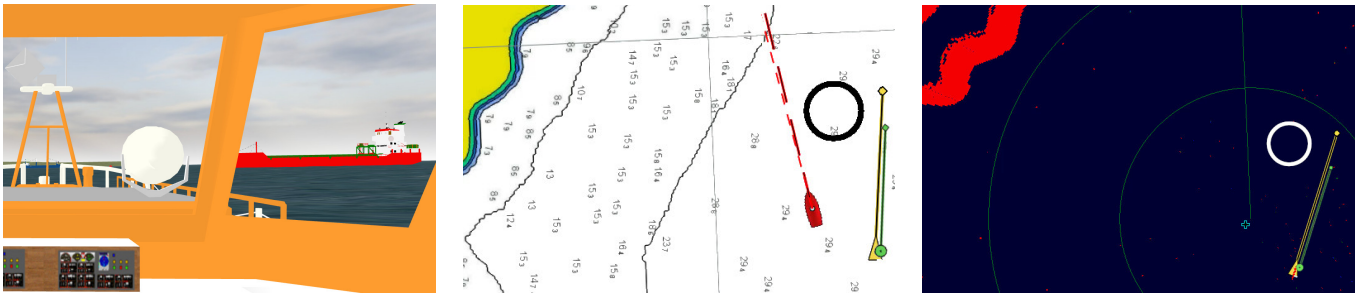
C. Requirement Assessment

After presenting the technical design and providing an overview of our implementation, we assess the developed environment w.r.t. the requirements from Sec. V-A.

Beginning with *realism*, we compared the simulation's network traffic to recordings of an actual vessel (Deneb[2]) and found that only a few proprietary NMEA sentences specific to that vessel and ones irrelevant for radar, such as GNSS satellite reception strength, were missing. Additionally, we carefully examined the radar image quality. Landmasses and buoys are located correctly, and other vessels' radar echoes are consistent with AIS and ARPA tracking, as initially shown in the previous Fig. 2, taken from the simulation of the Simple Estuary map. The terrain even masks objects behind line of sight. Compared to real systems, minor constraints are the low resolution of landscapes and BC's simplified radar reflectivity model.

Adaptability is provided by the extensibility of the environment's components. Further radar protocols can be effortlessly integrated, scenarios interchanged in BC, and arbitrary attacks added to RAT (*cf.* Sec. VI). Finally, by sharing the testbed with the research community together with its documentation, we tackle *availability*, *transparency*, and *replicability*, making it an ideal platform to conduct scientific radar security research.

[2]Deneb: https://www.bsh.de/EN/The_BSH/Our_ships/Our_ships_node.html



(a) Simulated view from the bridge in BC (b) RAT removes AIS and ARPA target in OpenCPN (c) RAT overwrites the vessel's radar echoes

Fig. 6. RAT effectively overwrites objects' radar echoes shown on the radar display (Fig. 6(c)) and simultaneously blocks AIS and ARPA related tracking information displayed on the chart display (Fig. 6(b)). Navigators relying solely on insecure digital systems could overlook the hazard depicted in Fig. 6(a).

VI. Radar Attack Tool (RAT)

With the realistic radar simulation environment at hand, we can finally examine radar-specific network attacks practically. This is accomplished by our Radar Attack Tool (RAT), which serves as a proof-of-concept for all network-based attacks laid out in Sec. IV. Therefore, it interfaces with the communication between the sensor network and the IBS as MitM, *i.e.*, a malicious device with complete control over traversing traffic.

Technically, RAT bases on Scapy, a Python interface for packet manipulation. While RAT is designed with a multitude of radar protocols in mind, based on the observations in Sec. II-B, for this proof-of-concept, we focus on the Navico BR24, already supported by the simulation environment. Sec. VI-A discusses the challenges and unique opportunities of implementing the different attack types along BR24.

A. Attack Implementation

As established in Fig. 3, there are four attack classes: DoS, transformation, object manipulation, and context-aware attacks. In the following, we showcase their application to a real radar protocol (Navico BR24 *cf.* Sec. II-B) and explicitly highlight the latter class of context-aware attacks that utilizes external knowledge from nautical NMEA 0183 data.

1) Denial of Service: DoS attacks can be executed easily against many protocols. It suffices to overwrite the scanline's pixels with arbitrary data, *i.e.*, noise or blank, as no integrity protection is in place. Given a single scanline, the number of scanlines per radar sweep, and a pixel position, RAT can convert the location of that pixel from polar to Cartesian coordinates and vice versa [14]. Thus, the entire radar image can be redrawn arbitrarily or frozen to the last image, constituting a sophisticated variant. Alternatively, a DoS can also be achieved in BR24 by altering specific control communication registers to instruct the radar unit to turn off continuously.

2) Transformation: The transformation attacks are divided into three subcategories according to our taxonomy and can be implemented quite efficiently for BR24. Regarding the *scaling* attack, the pixels associated within each scanline need to be modified by either zooming in or out. Note that extending the range requires generating artificial pixels not scanned by the radar (*cf.* Sec. IV-C). To this end, RAT can configure the radar to scan a larger area and only forward a rescaled sub-image. In BR24, this is largely simplified by the fact that this can be achieved by manipulating the scale field in the datagram header instead of individual pixels. The same holds for the *rotation* attack, respectively attacking the header's angle field. To rotate an image pixel-wise, the data associated with a specific scanline need to be shifted to another scanline or even across multiple UDP packets. Lastly, *translation* attacks require more effort and are solely based on pixel manipulation accomplished analog to redrawing entire images (*cf.* DoS). Again this may affect pixels across different UDP packets.

Still, a sudden transformation can introduce a noticeable discontinuity in the radar image. To make transformation attacks more subtle, RAT leverages external sensor data from the network, like the rate of turn announced via NMEA 0183, for further disguise (*cf.* Sec. IV-E), *e.g.*, incrementally rotating or translating the radar image during a vessel's course correction further than intended. This approach is similar to redirected walking, known from virtual reality and used to bend virtual worlds without users noticing to trick them into exploring larger virtual worlds than real space allows for [29].

3) Object Manipulation: Attacks adding, removing, or relocating radar echoes are enabled by the additional contextual information sensors provide and require selectively redrawing parts of the image by adding or blanking echoes. However, the seamless integration into an IBS with its complementary tracking capabilities, *i.e.*, AIS or ARPA, is more challenging.

Considering *additions* first, these can be performed in two steps. First, a new radar echo needs to be introduced, after which appropriate ARPA and AIS messages need to be generated for that echo. The latter can simply be injected into existing UDP broadcast traffic. Since AIS refers to absolute GNSS positions instead of ARPA's relative radar vector bearings and distances, the position of the newly added echo needs to be calculated, *e.g.*, derived from overhearing the vessel's actual position in the network. The *removal* of objects is analog to additions yet requires an attacker who can not only intercept the radar image but also suppress the corresponding AIS and ARPA messages towards the IBS. *Relocation* of objects can be assembled by combining both methods.

TABLE III
THE RADARPWN DATASET CONTAINS SAMPLES FROM ALL THREE ATTACK TYPES INCLUDING DIFFERENT VARIATIONS.

Attack Type	Example	Variations	Σ
DoS	Fig. 4(b)	blank, random, freeze, turn off	4
Scaling	Fig. 4(c)	pixel-wise, protocol header	2
Rotation	Fig. 4(d)	pixel-wise, protocol header, context-aware	3
Translation	Fig. 4(e)	pixel-wise, context-aware	2
Addition	Fig. 4(f)	context-aware (including AIS & ARPA)	1
Removal	Fig. 4(g)	context-aware (including AIS & ARPA)	1
Relocation	Fig. 4(h)	context-aware (including AIS & ARPA)	1

Concluding, RAT is the first tool to launch a wide range of network-based cyberattacks against marine radar and IBSs that holistically integrates complementary nautical data. Combined with the simulation environment (*cf.* Sec. V), these tools provides the means to execute harmful network-based radar attacks in a safe environment as exemplarily depicted in Fig. 6 and establish a valuable basis for future security research.

VII. RADARPWN DATASET

Marine radar communication is inherently insecure w.r.t. the protocol's designs (Sec. II-B) and consequentially susceptible to a variety of network-based cyberattacks (Sec. IV), which demand further preventive or detective countermeasures beyond existing related work. However, a thorough scientific evaluation is needed to assess the effectiveness of new approaches. While research in other domains, such as industrial control systems, has access to a wide range of established datasets and testbeds [13], to the best of our knowledge, there is no such dedicated dataset for marine radar.

To close this gap, we record RadarPWN, a comprehensive, easy-to-use, and documented dataset, including cyberattacks against radar communication in modern IBSs. As is common in other security domains, a collection of network captures (as pcap files) along with descriptive labels on when and which attacks were conducted builds the core of our dataset. To that end, we connect BC, RAT, and OpenCPN via virtual networks (*cf.* Fig. 5) and record the link between RAT and OpenCPN such that all malicious activities of RAT toward the radar display are captured. The recordings contain NMEA 0183 packets, including the important GNSS, AIS, and ARPA messages alongside the BR24 radar and control stream.

Regarding cyberattacks, the dataset covers all seven basic attack types from the taxonomy in a variety of configurations, as summarized in Tab. III. For DoS, we overwrite the radar data in three variations and also turn it off via BR24 control commands. Transformation attacks are either static (based on pixel-wise or protocol header modifications) or context-aware amplifying the vessel's motion (*cf.* Sec. VI-A). Regarding object manipulations, we record context-aware variants also affecting radar, AIS, and ARPA at the same time. To allow research focusing on specific attack types, a single network trace in the dataset records all variations of one type, randomized in order, timing, and parameterization. Finally, to introduce statistical variance, we record the attacks within all three worlds (*cf.* Tab. II) and repeat each experiment three times. Between repeated runs, we slightly alter the routes' waypoints to introduce realistic variance. This may be required for developing countermeasures such as machine-learning evaluating on similar train and test samples.

In summary, the resulting dataset consists of 72 traffic captures (the 8 attack types, including benign as shown in Fig. 4, executed and repeated 3 times in each of the 3 worlds) worth about 22 hours of vessel and radar network data. Besides benchmarking the performance of new security approaches on the RadarPWN dataset, the entire simulation environment with RAT can be used to conduct in-depth experiments beyond the scope of the dataset.

VIII. CONCLUSION

Shipboard marine radars' reliable and trustworthy operation is fundamental for safe navigation and, thus, critical for the global shipping industry. However, existing radar systems and the communication protocols they employ display serious and threatening vulnerabilities, as our paper shows. As part of our initial threat analysis, we identified potential network-based cyberattacks against marine radar, ranging from simple but disruptive approaches to sophisticated and deceptive attacks that leverage situational knowledge to impact crew's decisions. We then structured the identified attacks into a novel attack taxonomy, establishing four major attack categories.

To investigate their practical feasibility, we developed a maritime simulation environment that, for the first time, enables the holistic simulation of radar communication in a modern shipboard network. With our Radar Attack Tool (RAT), we thereupon implemented proof-of-concept attacks for all categories from the taxonomy. The combination of RAT and our simulation environment enables the development, testing, and practical demonstration of attacks exploiting radar communication protocol's vulnerabilities and provides an environment to design and evaluate countermeasures. Finally, to address the lack of scientific datasets in the domain, we leveraged these capabilities to record RadarPWN, a comprehensive marine dataset with cyberattacks against the Navico BR24 radar protocol. This dataset has the potential to foster future security research necessary for marine radar security and to secure shipboard networks.

For future work, we believe that our work will pave the way to develop and explore effective countermeasures. Using our simulation environment, we plan to investigate preventive measures that can be seamlessly integrated into existing maritime systems to better protect radar communication against the identified attacks. At the same time, we focus our considerations on detective methods. In particular, we see the great potential of our RadarPWN dataset, which allows us to apply approaches from the domain of anomaly detection to radar images. Both directions promise to enhance the cybersecurity of marine radar systems and thus increase vessels' safety on the seas.

ACKNOWLEDGMENTS

This work is part of the project MUM2 (https://www.mum-project.com). It was partially funded by the German Federal Ministry of Economic Affairs and Climate Action (BMWK) within the "Maritime Research Programme" with contract number 03SX543B managed by the Project Management Jülich (PTJ). The authors are responsible for the contents of this publication.

REFERENCES

[1] A. Amro, A. Oruc, V. Gkioulos, and S. Katsikas, "Navigation Data Anomaly Analysis and Detection," *Information*, vol. 13, no. 3, 2022.

[2] A. Androjna and M. Perkovic, "Impact of Spoofing of Navigation Systems on Maritime Situational Awareness," *Transactions on Maritime Science (ToMS)*, vol. 10, no. 2, Oct 2021.

[3] M. S. K. Awan and M. A. Al Ghamdi, "Understanding the Vulnerabilities in Digital Components of An Integrated Bridge System (IBS)," *Journal of Marine Science and Engineering*, vol. 7, no. 10, Oct 2019.

[4] M. Balduzzi, A. Pasta, and K. Wilhoit, "A Security Evaluation of AIS Automated Identification System," in *Proc. of ACSAC*, 2014.

[5] M. A. Ben Farah, E. Ukwandu, H. Hindy, D. Brosset, M. Bures, I. Andonovic, and X. Bellekens, "Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends," *Information*, vol. 13, no. 1, 2022.

[6] J. Bhatti and T. E. Humphreys, "Hostile Control of Ships Via False GPS Signals: Demonstration and Detection," *Journal of the Institute of Navigation*, vol. 64, no. 1, 2017.

[7] C. Boudehenn, O. Jacq, M. Lannuzel, J.-C. Cexus, and A. Boudraa, "Navigation anomaly detection: An added value for Maritime Cyber Situational Awareness," in *Proc. of CyberSA*, 2021.

[8] bridgecommand, "bc," https://github.com/bridgecommand/bc, 2022.

[9] M. Caprolu, R. D. Pietro, S. Raponi, S. Sciancalepore, and P. Tedeschi, "Vessels Cybersecurity: Issues, Challenges, and the Road Ahead," *IEEE Communications Magazine*, vol. 58, no. 6, 2020.

[10] E. E. Casanovas, T. E. Buchaillot, and F. Baigorria, "Vulnerability of Radar Protocol and Proposed Mitigation," *Journal of ICT Standardization*, vol. 4, no. 1, 2016.

[11] S. Cohen, T. Gluck, Y. Elovici, and A. Shabtai, "Security Analysis of Radar Systems," in *Proc. of CPS-SPC*, 2019.

[12] S. Cohen, E. Levy, A. Shaked, T. Cohen, Y. Elovici, and A. Shabtai, "RadArnomaly: Protecting Radar Systems from Data Manipulation Attacks," 2021, arXiv, cs.CR, 2106.07074.

[13] M. Conti, D. Donadel, and F. Turrin, "A survey on industrial control system testbeds and datasets for security research," *IEEE Communications Surveys Tutorials*, vol. 23, no. 4, 2021.

[14] A. Dabrowski, S. Busch, and R. Stelzer, "A Digital Interface for Imagery and Control of a Navico/Lowrance Broadband Radar," in *Proc. of Robotic Sailing*, 2011.

[15] T. de Riberolles, Y. Zou, G. Silvestre, E. Lochin, and J. Song, "Anomaly Detection for ICS Based on Deep Learning: A Use Case for Aeronautical Radar Data," *Annals of Telecommunications*, Jan. 2022.

[16] A. Goudosis and S. Katsikas, "Secure AIS with Identity-Based Authentication and Encryption," *TransNav*, vol. 14, no. 2, 2020.

[17] C. Hemminghaus, J. Bauer, and E. Padilla, "BRAT: A BRidge Attack Tool for Cyber Security Assessments of Maritime Systems," *TransNav*, vol. 15, no. 1, 2021.

[18] K. Jansen, N. O. Tippenhauer, and C. Pöpper, "Multi-Receiver GPS Spoofing Detection: Error Models and Realization," in *Proc. of ACSAC*, 2016.

[19] G. C. Kessler, P. Craiger, and J. C. Haass, "A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System," *TransNav*, vol. 12, no. 3, 2018.

[20] J. M.-y. Lee and E. Y.-c. Wong, "Suez canal blockage: an analysis of legal impact, risks and liabilities to the global supply chain," in *MATEC Web of Conferences*, vol. 339. EDP Sciences, 2021.

[21] M. S. Lund, J. E. Gulland, O. S. Hareide, Ø. Jøsok, and K. O. C. Weum, "Integrity of integrated navigation systems," in *Proc. of CNS*, 2018.

[22] H. Mansouri, A.-S. K. Pathan, and M. Aliouat, "A snapshot security protocol for radar network protection," in *Proc. of DAT*, 2017.

[23] OpenCPN, "OpenCPN," https://github.com/OpenCPN/OpenCPN, 2022.

[24] opencpn-radar pi, "radar_pi," https://github.com/opencpn-radar-pi/radar_pi, 2022.

[25] Ø. J. Rødseth, M. J. Christensen, and K. Lee, "Design challenges and decisions for a new ship data network," in *Proc. of ISIS*, Hamburg, Germany, 2011.

[26] Ø. J. Rødseth and Å. Tjora, "A system architecture for an unmanned ship," in *Proc. of COMPIT*, 2014.

[27] Y. Shui, Y. Wang, Y. Li, Y. Shan, N. Cui, and B. Pang, "Consensus-Based Distributed Target Tracking with False Data Injection Attacks over Radar Network," *Applied Sciences*, vol. 11, no. 10, 2021.

[28] SOLAS Chapter V – 1/7/02, "Safety of Navigation," 2002, IMO.

[29] F. Steinicke, G. Bruder, J. Jerald, H. Frenz, and M. Lappe, "Analyses of human sensitivity to redirected walking," in *Proc. of VRST*, 2008.

[30] T. C. Stratmann, D. Brauer, and S. Boll, "Supporting the Perception of Spatially Distributed Information on Ship Bridges," in *Proc.of MuC*, 2019.

[31] B. Sviličić, I. Rudan, V. Frančić, and D. Mohović, "Towards a Cyber Secure Shipboard Radar," *Journal of Navigation*, vol. 73, no. 3, 2020.

[32] K. Tam, R. Hopcraft, K. Moara-Nkwe, J. Misas, W. Andrews, A. Harish, P. Giménez, T. Crichton, and K. Jones, "Case Study of a Cyber-Physical Attack Affecting Port and Ship Operational Safety," *Journal of Transportation Technologies*, vol. 12, no. 1, 2022.

[33] K. Tam and K. Jones, "Factors affecting cyber risk in maritime," in *Proc. of Cyber SA*, 2019.

[34] R. Uetz, C. Hemminghaus, L. Hackländer, P. Schlipper, and M. Henze, "Reproducible and Adaptable Log Data Generation for Sound Cybersecurity Experiments," in *Proc. of ACSAC*, 2021.

[35] C. Yang, L. Feng, H. Zhang, S. He, and Z. Shi, "A Novel Data Fusion Algorithm to Combat False Data Injection Attacks in Networked Radar Systems," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, 2018.