

The Megayacht's Digital Achilles' Heel: Analyzing the Attack Surface and Cybersecurity as a Shipyard's Strategic Imperative

Lukas Johannes Möller
Institute for Information Systems
University of Applied Sciences Kiel
Kiel, Germany
lukas.j.moeller@student.fh-kiel.de

Abstract—The increasing digitalization of the maritime industry has transformed vessels into interconnected cyber-physical systems. Nowhere is this convergence of Information Technology (IT), Operational Technology (OT), and Internet of Things (IoT) devices more pronounced than aboard luxury megayachts. These vessels, designed for High-Net-Worth Individuals (HNWIs), integrate complex navigation, communication, and entertainment infrastructures. However, this digital sophistication introduces new cyber risks that are often not adequately addressed during construction. This paper identifies a critical gap in the industry's current approach: the insufficient integration of cybersecurity during the design and build phases at shipyards. Drawing from contemporary research and industry case studies, the paper outlines the evolving maritime threat landscape, examines the unique cyber risk profile of superyachts, and highlights how shipyards can convert cybersecurity from a reactive burden into a proactive strategic differentiator. A secure-by-design approach offers not only improved resilience but also a compelling value proposition for shipbuilders aiming to serve a security-conscious clientele.

Index Terms—Maritime Cybersecurity, Superyachts, Megayacht, Attack Surface, Secure-by-Design, IT/OT Convergence, Shipyard Risk, High-Net-Worth Individuals, Lifecycle Security, Competitive Advantage

I. INTRODUCTION

The maritime sector has entered a new digital era. Ships are no longer isolated mechanical vessels but highly networked platforms embedded with software-controlled subsystems that manage propulsion, navigation, cargo operations, and safety protocols. This shift has brought enormous efficiency and automation benefits—yet it has also introduced a vastly expanded attack surface [1], [2]. From large container ships to naval platforms, maritime cybersecurity has become a strategic concern. However, within this landscape, luxury megayachts present a particularly under-analyzed vector.

Megayachts, often owned by high-net-worth individuals (HNWIs), combine high-end leisure, global mobility, and bleeding-edge technology. These vessels are equipped with smart-home interfaces, satellite communication links, cloud-connected entertainment systems, remote monitoring sensors, and advanced navigation units—creating a complex cyber-physical ecosystem [3], [4]. This makes them attractive targets

not only for cybercriminals seeking financial gain or data but also for state-level actors or hacktivists interested in surveillance, disruption, or blackmail.

Despite these realities, cybersecurity in the superyacht domain has historically been treated as an operational afterthought. While commercial shipping is increasingly governed by regulatory standards such as the IMO's cyber risk management framework [5], superyachts—owing to their custom builds, fragmented supply chains, and discretionary privacy—are often exempt from mandatory requirements. Even when addressed, cybersecurity is typically introduced at the end of the production cycle, leaving fundamental design vulnerabilities unaddressed [6], [7].

This paper argues for a paradigm shift: cybersecurity should be embedded from the keel up. Shipyards are uniquely positioned to deliver secure-by-design vessels, addressing risk before it materializes and offering a new premium service tier. By analyzing the megayacht cyber attack surface and exposing gaps in current construction practices, this study highlights both the critical risks and the untapped market potential of cybersecurity-integrated shipbuilding.

II. THE EVOLVING MARITIME CYBER THREAT LANDSCAPE

The rapid digital transformation of the maritime domain has exposed vessels to an expanding array of cyber threats. Increasingly reliant on networked sensors, software-controlled actuators, and global connectivity, modern vessels represent attractive targets for adversaries motivated by profit, disruption, or intelligence gathering. The attack surface spans both IT systems—such as enterprise resource planning (ERP), crew Wi-Fi, and email servers—and OT systems that control propulsion, steering, power generation, and ballast water treatment [2], [8].

Several high-profile maritime incidents have demonstrated the tangible risks. The NotPetya ransomware attack crippled Maersk's global operations, resulting in estimated losses of over \$300 million [9]. More targeted attacks include the disruption of electronic navigation systems (ECDIS) via malware, spoofing of AIS and GPS data to mislead ships, and

remote access to onboard systems through vulnerable satellite terminals or weakly configured remote management tools [4], [10], [11].

The interconnected systems aboard ships include Electronic Chart Display and Information Systems (ECDIS), Automatic Identification Systems (AIS), Global Navigation Satellite Systems (GNSS), Integrated Bridge Systems (IBS), Ballast Water Management Systems (BWMS), and machinery automation networks. Many of these leverage shared infrastructure or cloud connectivity, expanding the risk of cross-domain compromise [12], [13].

Beyond technical flaws, the maritime sector also grapples with human and organizational vulnerabilities. Crew members frequently connect personal devices to onboard networks, and outdated operating systems or default credentials are not uncommon due to poor vendor lifecycle management. The lack of standardized patching procedures, fragmented supply chains, and limited cyber awareness training further exacerbate exposure [2], [14].

Regulatory efforts such as the IMO's 2021 cybersecurity mandate (MSC-FAL.1/Circ.3) have begun to address these issues by requiring cyber risk to be integrated into Safety Management Systems [5]. However, compliance varies widely, particularly in non-commercial vessel segments such as megayachts, where discretionary standards and bespoke configurations create enforcement challenges.

The maritime threat landscape is therefore not static but dynamic, with adversaries leveraging both technical exploits and social engineering. The convergence of IT/OT systems and the emergence of AI-assisted attack tools further complicate defensive efforts. Without a security-first design mindset during vessel construction, critical weaknesses may be built into ships from the outset—particularly in segments like superyachts, where operational and regulatory oversight is comparatively low [1], [3].

III. SUPERYACHTS: HIGH VALUE, HIGH COMPLEXITY, HIGH RISK

Luxury megayachts represent a unique category within the maritime domain—combining the complexity of a modern smart ship with the discretion and personalization expected by ultra-high-net-worth individuals (UHNWIs). These vessels often exceed 80 meters in length and are equipped with state-of-the-art systems for navigation, entertainment, comfort, and security. Unlike commercial ships, they integrate a high density of consumer-grade IoT devices alongside critical operational systems, significantly enlarging their digital attack surface [3], [15].

The typical superyacht incorporates the following interconnected technologies:

- **Navigation and Bridge Systems:** Including ECDIS, AIS, GNSS, radar, autopilot, and integrated bridge systems (IBS), often sourced from different vendors and loosely integrated via IP-based protocols [16].

- **Machinery Control and Automation:** PLC-based systems for engines, generators, fuel, and HVAC, frequently accessible via internal ship networks [1].
- **Communications:** VSAT, LTE fallback, satellite telephony, and onboard Wi-Fi often bridged with guest and crew devices, creating crossover risks [4].
- **Entertainment and IoT Systems:** Audio-visual systems, smart lighting, climate control, guest Wi-Fi, wearable integration, and digital concierge services—commonly relying on consumer-grade firmware with limited update lifecycles [2], [3].
- **Remote Access and Monitoring:** Remote vendor access for diagnostics or updates, cloud connectivity for telemetry or voyage data, and web interfaces for system control introduce entry points for unauthorized access [10], [17].

The attack scenarios are varied and potentially devastating: navigation spoofing that misleads crew, malware propagation via guest devices, interception of sensitive emails or phone calls, and ransomware infections that disable propulsion or hotel systems. In one documented case, an infected ECDIS delayed a vessel due to system instability [11]. In another, insecure SATCOM terminals enabled unauthenticated shell access [4].

Privacy breaches also constitute a significant risk. Megayachts often store data such as personal communications, travel itineraries, video surveillance footage, and details of on-board financial transactions. The reputational and legal implications of data leaks or targeted surveillance of UHNWIs are substantial. Attackers may exfiltrate sensitive data for extortion, competitive intelligence, or public exposure.

The human factor compounds these challenges. Guests and crew may unknowingly introduce malware via USB devices, connect insecure phones or laptops to the onboard network, or fall victim to phishing attempts while browsing at sea. Furthermore, system misconfigurations by undertrained personnel may leave critical components exposed to the internet [2], [14].

Despite these high stakes, many cybersecurity services marketed to superyacht operators—such as vulnerability scanning, training, and 24/7 monitoring—are only engaged after delivery. This reactive model often requires retrofitting security into complex systems, increasing both cost and complexity. Without security embedded during the construction phase, key architectural vulnerabilities may remain undetected and unmitigated [6], [7].

IV. FOUNDATIONS OF SECURE SHIPBUILDING

To effectively embed cybersecurity into megayacht construction, shipyards must draw from established theoretical frameworks and clearly defined security principles. However, many shipyards lack internalized models for systematically addressing cyber risk across design, integration, and delivery. This section introduces foundational concepts that can support structured decision-making and practical risk reduction.

A. Secure-by-Design in Naval Architecture

Secure-by-design refers to the proactive integration of cybersecurity mechanisms into a vessel's architecture, starting at the design stage rather than post-delivery retrofitting. In the maritime context, this involves designing segmented networks, enforcing least-privilege access control, eliminating default credentials, and ensuring encrypted communications across IT and OT systems. Secure-by-design reframes cybersecurity not as an operational bolt-on, but as a core dimension of technical quality and trust [19].

B. Threat Modeling with STRIDE

Threat modeling enables designers to identify and anticipate security weaknesses early in the lifecycle. The STRIDE framework categorizes threats into six classes: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. Applied to superyachts, this model can be used to evaluate, for example, satellite uplinks (information disclosure), weak authentication on bridge consoles (elevation of privilege), or unsegmented VLANs (spoofing/tampering risk). Mapping threats to specific components supports targeted hardening before deployment [19].

C. Risk Prioritization using DREAD

Once threats are modeled, the DREAD method can be used to prioritize mitigation. It evaluates each threat based on: Damage potential, Reproducibility, Exploitability, Affected users, and Discoverability. For example, a vulnerability in the remote monitoring interface may rank higher than a media server misconfiguration, due to greater exposure and impact. Such structured scoring helps align security investment with actual risk, particularly when budgets or deadlines are tight.

D. Lifecycle Security and the MaCRA Model

Cyber risk does not end at delivery. Lifecycle security emphasizes the need to manage threats across commissioning, routine operation, maintenance, refit, and decommissioning. The Maritime Cyber Risk Assessment (MaCRA) framework [13] supports this view by integrating risk scoring with asset criticality, connectivity profiles, and behavior-based threat surfaces. MaCRA is particularly useful for capturing long-term risks such as vendor firmware stagnation, poorly controlled guest networks, or outdated SATCOM modules.

E. Strategic Implications

Embedding these frameworks enables shipyards to move from ad hoc defense to systemic risk engineering. It supports both secure construction and client assurance—laying the groundwork for services such as security certification, digital twin testing, or automated threat simulation. Shipyards that internalize threat modeling and lifecycle thinking will be better equipped to deliver resilient vessels by design—not by retrofit.

V. SHIPYARDS AND THE CONSTRUCTION-PHASE CYBERSECURITY GAP

Shipyards are at the heart of vessel lifecycle development. They orchestrate the integration of hundreds of subsystems from diverse suppliers and are responsible for ensuring functional performance, safety, and regulatory compliance. Yet, despite the technical sophistication of the modern shipbuilding process, cybersecurity is frequently treated as an auxiliary concern—addressed only during late-stage system commissioning or post-delivery operational procedures [1], [6], [7].

This reactive approach introduces several systemic vulnerabilities:

- **Multivendor Complexity:** Megayachts incorporate systems from dozens of third-party vendors—radar, propulsion, AV, satellite, lighting—each with differing firmware maturity, patch cycles, and cybersecurity practices. Without centralized security governance during integration, misconfigurations and latent vulnerabilities proliferate [8].
- **Legacy Engineering Mindset:** Shipbuilding has traditionally prioritized mechanical robustness and physical safety over digital resilience. Cybersecurity is often perceived as the responsibility of the owner, captain, or post-delivery service provider, rather than the builder [3].
- **Time-to-Market and Cost Pressures:** In the luxury segment, the commercial drive to deliver on time and under budget often sidelines security testing, documentation, and design hardening—especially when the ship is not subject to mandatory compliance frameworks [6].
- **Lack of Secure-by-Design Standards:** While initiatives such as the IMO cybersecurity resolution and class society guidelines (e.g., ClassNK's Cyber Security Management System) offer high-level advice, there is no universally enforced standard for implementing cybersecurity during the build phase—particularly for privately commissioned vessels [5], [7].

The consequences of this construction-phase gap are twofold. First, insecure systems are delivered by default. Networks may lack segmentation, vendor credentials may remain unchanged, remote access services may be enabled without proper logging, and systems may ship with outdated software versions—introducing attack vectors that persist long after delivery. Second, remediation post-handover is more expensive and operationally disruptive. Addressing vulnerabilities after acceptance requires costly onboard visits, system replacements, or coordination with hard-to-reach vendors.

Even where cyber testing is offered, it is often performed by third-party consultants or insurers after the fact, rather than being built into the quality assurance pipeline. Penetration testing, risk assessments, or red teaming exercises conducted post-launch may uncover flaws that could have been trivially addressed during integration had cyber risk been considered upfront [10].

This structural oversight is especially paradoxical given the profile of the clientele. UHNWIs are increasingly aware of cy-

ber risks, particularly in the wake of high-profile surveillance, extortion, and data breach scandals. Yet the very vessels meant to serve as mobile sanctuaries for privacy and luxury are often constructed with limited cyber resilience by default.

However, this gap also presents a strategic opportunity: shipyards could pivot from passive risk producers to active providers of cyber-resilient vessels—embedding security throughout design, integration, validation, and documentation. In doing so, they would address both client needs and a critical vulnerability in current industry practice.

VI. IMPLICATIONS AND THE MISSED OPPORTUNITY

The absence of proactive cybersecurity during the construction phase of superyachts carries both technical and strategic consequences. First and foremost, it leads to the delivery of vessels with latent vulnerabilities—digital weak points embedded in their core architectures. Second, and equally important, it reflects a missed commercial opportunity for shipyards to transform cybersecurity from a reactive liability into a high-value service differentiator [3], [6].

A. Technical Consequences

The downstream impact of construction-phase security gaps is profound. Superyachts may leave the yard with:

- **Unsegmented Networks:** Flat network topologies connecting IT, OT, and guest systems allow attackers who breach one component to move laterally.
- **Outdated Firmware and Software:** Systems may run vulnerable versions of operating systems or embedded firmware, particularly if vendors were selected for feature delivery, not cybersecurity posture [1].
- **Weak or Default Credentials:** Vendor-supplied usernames and passwords are often not changed during deployment, creating trivial entry points.
- **Insecure Remote Access Mechanisms:** Enabled by default for support contracts, these may lack multi-factor authentication or adequate logging.

These vulnerabilities can be extremely costly to remediate post-delivery, particularly if remediation requires dry-docking, disrupting owner use, or invalidating warranty conditions. More dangerously, they may remain unaddressed until an incident occurs, with consequences ranging from ransomware lockdown to data exfiltration or hijacking of control systems [9], [17].

B. Commercial Opportunity for Shipyards

Paradoxically, the current state of underpreparedness opens the door to significant value creation. Shipyards that adopt a security-first mindset can position themselves not just as builders, but as providers of resilient, secure platforms. This shift would offer:

- **Premium Service Tiers:** Tiered offerings for cybersecurity during design, integration, and post-delivery support—bundled as value-added packages.

- **Client Assurance:** For UHNWIs concerned with privacy and digital exposure, cyber-resilience becomes a key aspect of trust in the shipyard's brand.
- **Lifecycle Partnerships:** Shipyards can evolve into long-term security partners—offering monitoring, threat intelligence, and patching as managed services.
- **Reputational Differentiation:** In a competitive market, security certifications or demonstrable secure-by-design principles could enhance brand positioning.

This strategy aligns with broader industry movements. Some classification societies are already exploring "cyber class notations," and insurers have begun factoring cybersecurity into premium models for high-value vessels [7]. However, few shipyards have integrated these aspects into their core value proposition.

Security is no longer a back-office IT concern—it is a trust enabler and brand asset. Those shipyards that recognize this paradigm early will not only deliver safer vessels but also gain a substantial edge in a market increasingly shaped by digital risk perception.

VII. RECOMMENDATIONS AND POTENTIAL SOLUTIONS

To close the construction-phase cybersecurity gap and turn digital resilience into a strategic asset, shipyards must transition from reactive compliance to proactive design. The following recommendations outline a practical, layered approach grounded in current best practices, tailored to the context of superyacht construction.

A. Integrate Cyber Risk Management Early

Cybersecurity considerations must be embedded into the earliest stages of vessel planning, including specification writing, vendor selection, and network architecture design. Threat modeling techniques such as STRIDE, attack trees, or the MaCRA framework can help identify critical vulnerabilities across the yacht's digital infrastructure before procurement decisions are finalized [13], [18].

B. Adopt Secure-by-Design Engineering

Rather than bolting security onto completed systems, shipyards should adopt secure-by-design principles across the vessel's IT and OT landscapes. This includes enforcing strong authentication protocols, role-based access control, segmented networks, and encrypted communications as defaults—not options. System interfaces should be hardened against unauthorized access, and insecure default configurations removed during installation [3], [7].

C. Strengthen Supply Chain Assurance

Each vendor product integrated into a superyacht represents a potential attack vector. Shipyards must conduct due diligence on all third-party hardware and software—requiring suppliers to provide vulnerability disclosures, update schedules, and documentation for secure integration. Where feasible, shipyards should standardize approved components and establish clear expectations regarding security posture [8].

D. Build in Monitoring and Incident Response

Security monitoring should not be left for the owner to implement post-delivery. Shipyards can integrate intrusion detection systems, logging infrastructure, and anomaly detection into the vessel at build time. Critical systems should support remote diagnostics and secure firmware updates, enabling shipyards or managed service providers to offer proactive threat response over the vessel's lifecycle [1].

E. Provide Cybersecurity Documentation and Training

A secure ship requires secure operators. Shipyards should provide clear documentation on system architectures, account hierarchies, update mechanisms, and best practices. Initial crew training—delivered either in person or via digital modules—should include phishing awareness, credential hygiene, USB risks, and correct use of remote access services [2], [14].

F. Offer Post-Delivery Security Services

Rather than ending client relationships at handover, shipyards can extend their service model to include:

- Regular vulnerability scanning and patch audits
- Remote monitoring and intrusion detection
- Incident response advisory and forensic readiness
- Crew re-training and tabletop exercises

This not only enhances vessel security but generates recurring revenue and customer loyalty.

G. Champion Industry Standards and Certification

Shipyards should contribute to the development of superyacht-specific cybersecurity standards—either through classification societies, owner consortia, or sector alliances. Early adopters could promote third-party certification schemes or develop proprietary labels (e.g., “Cyber-Resilient Yacht”) that build trust among security-conscious clients [3], [7].

Ultimately, cybersecurity must become a core competency in shipbuilding—treated with the same rigor as safety, engineering quality, or regulatory compliance. Shipyards that embrace this role will not only reduce risk exposure but establish a new frontier of excellence in luxury maritime construction.

VIII. LIMITATIONS AND FUTURE WORK

This paper proposes a shipyard-centric model for integrating cybersecurity into megayacht construction. However, several limitations must be acknowledged, both methodological and contextual.

A. Heterogeneity of Vessel Classes

The analysis centers on large (> 80 m) superyachts with complex digital systems. Smaller yachts or expedition vessels may have vastly different architectures, network topologies, and owner requirements. Future work should segment vessel typologies to assess how risk modeling and secure-by-design measures scale down (or up).

B. Exclusion of Military or Dual-Use Vessels

Military, government, or hybrid vessels fall outside this paper's scope. These platforms are often subject to different procurement regimes (e.g., MIL-STD), classified threat models, and stricter security requirements. While conceptual overlaps exist, the risk posture, documentation standards, and oversight mechanisms differ significantly from civilian megayachts.

C. Assumed Client Buy-In and Yard Capabilities

The recommendations assume that shipyards are willing and able to implement secure-by-design processes, and that clients value cybersecurity as part of the build. These assumptions require empirical validation. Market studies could assess demand elasticity for cybersecurity packages, while qualitative interviews could surface barriers such as legacy workflows, skill shortages, or perceived ROI gaps.

D. Lack of Field Validation

The analysis is based on technical literature, expert commentary, and prior case studies. It does not include first-hand red teaming of in-construction vessels or embedded fieldwork within shipyards. Future research could include penetration testing of build-phase configurations, or direct observation of system integration practices, to measure real-world alignment with proposed frameworks.

IX. CONCLUSION

The escalating complexity of maritime technology has redefined the risk landscape for luxury megayachts. These vessels, built to serve the world's most privacy-conscious clientele, are increasingly exposed to sophisticated cyber threats. The convergence of IT, OT, and IoT—combined with high network connectivity, vendor diversity, and crew-device integration—creates a vast and often misunderstood attack surface.

This paper has examined the cybersecurity challenges inherent to modern megayachts, focusing specifically on the role of shipyards during the construction phase. Evidence suggests that many current practices emphasize compliance and operational retrofitting, rather than proactive cyber resilience. This leaves critical vulnerabilities unaddressed and imposes remediation burdens on owners and operators.

Yet, embedded within this gap is an opportunity. Shipyards that transition toward secure-by-design practices—integrating threat modeling, system hardening, vendor assurance, and post-delivery services—stand to differentiate themselves in a competitive, high-margin market. For clients increasingly attuned to digital privacy and operational reliability, demonstrable cybersecurity maturity is not just a technical requirement, but a mark of craftsmanship and trust.

Cybersecurity must no longer be seen as a bolt-on feature. It is an essential layer of modern naval architecture, deserving of the same design-level attention as propulsion, stability, and aesthetics. By embracing this paradigm, shipyards can not only deliver safer vessels but also elevate their strategic position in the future of high-value maritime innovation.

REFERENCES

- [1] K. Kanwal, W. Shi, C. Kontovas, Z. Yang, and C.,H. Chang, "Maritime cybersecurity: are onboard systems ready?" *Maritime Policy & Management*, vol. 51, no. 3, pp. 484–502, 2024. DOI: <https://doi.org/10.1080/03088839.2022.2124464>.
- [2] F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, and M. Michaloliakos, "Cybersecurity Challenges in the Maritime Sector," *Network*, vol. 2, pp. 124–142, 2022. DOI: <https://doi.org/10.3390/network2010009>.
- [3] Dryad Global, "Cyber Security at Sea: Protecting Superyachts with Cyber Voyager," White Paper, 2025. [Online]. Available: <https://channel16.dryadglobal.com/cyber-security-at-sea-protecting-superyachts-with-cyber-voyager>
- [4] R. Santamarta, "SATCOM Terminals: Hacking by Air, Sea, and Land," IOActive Research, 2014. [Online]. Available: https://ioactive.com/wp-content/uploads/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf
- [5] IMO, "MSC-FAL.1/Circ.3 – Guidelines on Maritime Cyber Risk Management," International Maritime Organization, 2021. [Online]. Available: [https://www.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20\(Secretariat\).pdf](https://www.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf)
- [6] Belfry Software, "Essential Guide to Shipyard Security: What to Know in 2025," White Paper, 2025. [Online]. Available: <https://www.belfrysoftware.com/blog/shipyard-security>
- [7] ClassNK, "Cyber Security Management System for Ships," ClassNK Guidelines, 2019. [Online]. Available: https://www.classnk.com/hp/pdf/activities/cybersecurity/gl_CSMS_201904e.pdf
- [8] V. Bolbot, G. Theotokatos, E. Boulougouris, and D. Vassalos, "A novel cyber-risk assessment method for ship systems," *Safety Science*, vol. 131, p. 104908, 2020. DOI: <https://doi.org/10.1016/j.ssci.2020.104908>.
- [9] N. Newman, "Cyber pirates terrorising the high seas," *Engineering and Technology*, 2019. [Online]. Available: <https://eandt.theiet.org/content/articles/2019/04/cyber-pirates-terrorising-the-high-seas/>
- [10] B. Svilicic, J. Kamahara, J. Celic, and J. Bolmsten, "Assessing ship cyber risks: a framework and case study of ECDIS security," *WMU Journal of Maritime Affairs*, vol. 18, pp. 509–520, 2019. DOI: <https://doi.org/10.1007/s13437-019-00183-x>.
- [11] M.,S. Lund, O.,S. Hareide, and Ø. Jøsok, "An attack on an integrated navigation system," *Necesse*, vol. 3, pp. 149–163, 2018. DOI: <https://doi.org/10.21339/2464-353X.3.2.149>.
- [12] D. Lee *et al.*, "Situation awareness for autonomous ships: cybersecurity and navigation fusion," *Sensors*, vol. 22, no. 5, p. 1860, 2022. DOI: <https://doi.org/10.3390/s22051860>.
- [13] K. Tam and K. Jones, "MaCRA: A model-based framework for maritime cyber-risk assessment," *WMU Journal of Maritime Affairs*, vol. 18, no. 1, pp. 129–163, 2019. DOI: <https://doi.org/10.1007/s13437-019-00162-2>.
- [14] M.,W. Boyce *et al.*, "Human Performance in Cybersecurity: A Research Agenda," *HFES Annual Meeting Proceedings*, vol. 55, no. 1, pp. 1115–1119, 2011. DOI: <https://doi.org/10.1177/1071181311551233>.
- [15] SuperYacht Times, "Superyacht Cybersecurity: Protecting Against Cyber Threats at Sea," SYT Tech Talk, 2025. [Online]. Available: <https://superyachttechnologyshow.com/superyacht-cybersecurity-threats/>
- [16] B. Svilicic, D. Brčić, S. Žuškin, and D. Kalebić, "Raising awareness on cybersecurity of ECDIS," *Journal of Marine Navigation and Safety (TransNav)*, vol. 13, pp. 231–236, 2019. DOI: <https://doi.org/10.12716/1001.13.01.24>.
- [17] R. Santamarta, "Hacking into a Voyage Data Recorder (VDR)," IOActive Research, 2015. [Online]. Available: <https://ioactive.com/maritime-security-hacking-into-a-voyage-data-recorder-vdr/>
- [18] W. Shang, T. Gong, C. Chen, J. Hou, and P. Zeng, "Information security risk assessment method for ship control system based on fuzzy sets and attack trees," *Security and Communication Networks*, 2019. DOI: <https://doi.org/10.1155/2019/3574675>.
- [19] A. Shostack, *Threat Modeling: Designing for Security*. Wiley, 2014. [Online]. Available: <https://www.wiley.com/en-us/Threat%20Modeling%3A%20Designing%20for%20Security-p-9781118809990>