

Revista Sextante

ISSN : 2665-3923

Vol: 31 No: 01 (2024)

Cybersecurity Challenges in Modern Naval Defense Systems: Threat Assessment and Mitigation Strategies

Lars E. Hendriksen

Department of Cyber Defence and Maritime Security, Oresund Institute for Naval Technology, Copenhagen, Denmark

Article History

Received dec, 09th , 2024

Accepted dec, 10th , 2024

Published dec, 11th, 2024



© 2024 The Authors. This article is an Open Access article distributed under the terms and conditions of the Creative Commons Attribution(CC-BY)license
<https://creativecommons.org/licenses/by/4.0>

Abstract

Modern warships, submarines, naval aircraft, and their supporting shore facilities depend on interconnected digital systems for navigation, communications, propulsion control, sensing, logistics, and command. This dependence delivers major operational benefits but also exposes naval forces to cyber threats from states, criminal groups, and insiders. This article examines cybersecurity challenges in modern naval defence systems and evaluates approaches to threat assessment and mitigation. It describes the digital architecture of contemporary naval platforms, characterises the main threat actors and attack surfaces, reviews assessment methodologies, analyses vulnerabilities in navigation, communications, and control systems, and considers supply chain and shore infrastructure risks. It then discusses mitigation strategies built on defence in depth, segmentation, zero trust principles, monitoring, resilience, and training. The analysis indicates that no single control can secure naval systems, that long equipment lifecycles and complex supply chains create persistent exposure, and that human and organisational factors are as significant as technical safeguards. The article concludes with policy and operational recommendations that emphasise resilience, the ability to operate in degraded conditions, and continuous learning. The discussion stays at the level of strategy and defensive practice.

Keywords: naval cybersecurity, threat assessment, maritime cyber risk, defence in depth, operational resilience

INTRODUCTION

Naval vessels have evolved from mechanical machines into floating networks. A modern surface combatant integrates radar, sonar, electronic warfare, weapon control, navigation, propulsion management, damage control, and communications through shipboard networks that connect hundreds or thousands of devices. Submarines and naval aircraft follow a similar trajectory, while ports, shipyards, and command centres add further layers of digital infrastructure. Each connection offers operational advantages, yet each also presents an opportunity for adversaries to observe, disrupt, or manipulate. Cyber operations have become a standard instrument of statecraft and conflict. Singer

and Friedman describe how cyberspace has created new forms of espionage, sabotage, and coercion that blur the boundary between peace and war (Singer and Friedman, 2014). Rid argued that cyber operations tend to work through subversion, espionage, and sabotage rather than through direct violence, which means that their strategic effect often lies in eroding trust and degrading capability below the threshold of open conflict (Rid, 2012). For navies, which depend on trusted data and reliable control, such effects can be serious. The maritime environment adds distinctive challenges. Ships operate far from home with limited bandwidth, often rely on satellite links, and remain at sea for long periods during which software cannot easily be patched. Equipment is built to last for decades, so systems designed before modern threats were understood continue to serve alongside newer technology. Many operational technologies, such as engine controls and navigation sensors, were not designed with security in mind. This article addresses how naval organisations can understand and reduce these risks. It proceeds through nine thematic sections covering cyber dependence, threat actors, attack surfaces, assessment methodologies, vulnerabilities in critical systems, supply chain and shore risks, mitigation strategies, human and organisational factors, and policy directions. A summary and a list of references follow.

Cyber Dependence of Modern Naval Systems:

The degree of digital integration in modern naval forces is difficult to overstate. Navigation relies on satellite positioning, electronic charts, and inertial systems. Communications use radio, satellite, and data links to share information among ships, aircraft, and headquarters. Sensors feed combat management systems that fuse data and support decisions. Machinery control systems regulate power generation, propulsion, and auxiliary equipment, often with remote monitoring and diagnostics. This integration increases capability. Shared situational awareness allows dispersed units to operate as a coordinated force. Automation reduces crew workload and enables smaller complements. Condition monitoring improves maintenance and availability. Digital logistics streamlines the supply of parts and fuel. These benefits are central to contemporary naval concepts, which assume that information advantage translates into operational advantage. The same integration creates systemic dependence. If navigation data are corrupted, if communications are denied, or if control systems are manipulated, effects can cascade across functions. A degraded network may hinder weapons employment, reduce awareness, and impair the ability to manoeuvre safely. The more a force relies on connectivity, the greater the incentive for adversaries to attack it. Understanding dependence is the starting point for risk management. Navies need to know which functions are most critical, which systems support them, and what alternatives exist if those systems fail. Mapping these dependencies reveals single points of failure and guides decisions on redundancy, segregation, and fallback procedures.

Threat Actors and Motivations:

The threat environment includes several categories of actor. State sponsored groups pursue intelligence collection, positioning of access for use in a crisis, and disruption of military capability. They typically possess substantial resources, patience, and the ability to develop tailored techniques. Their targets include naval design data, operational plans, communications, and the networks of shipbuilders and suppliers. Criminal groups are motivated mainly by financial gain. Ransomware attacks on shipping companies, ports, and defence contractors have shown that criminals can disrupt operations and steal sensitive data. Even when a naval force is not the intended target, its suppliers and partners may be, which creates indirect exposure. Hacktivists seek publicity or political influence and may use relatively simple methods to deface websites or disrupt services. Insiders form another category. Employees, contractors, and service members with legitimate access may cause harm deliberately or through negligence. Because they already operate inside trusted boundaries, insiders can be harder to detect than external attackers, and their actions may bypass perimeter defences. Hutchins, Cloppert, and Amin proposed the intrusion kill chain as a way of understanding how adversaries proceed through stages from reconnaissance to achieving their objectives, and they argued that defenders can gain advantage by detecting and disrupting activity at any stage (Hutchins et al., 2011). This intelligence driven view encourages navies to study adversary behaviour rather than react to individual incidents. It also underscores that threats are persistent and adaptive.

Attack Surfaces Across Naval Platforms and Infrastructure:

The attack surface of a naval force extends well beyond the visible network on a ship. It includes shipboard information technology, such as administrative systems and email, and operational technology, such as engine controllers, navigation equipment, and sensors. It also includes interfaces to shore, such as satellite links, maintenance connections, removable media, and software update channels, as well as the networks of ports, shipyards, depots, and command centres. Operational technology deserves particular attention. Svilicic and colleagues conducted an experimental assessment of a ship's cyber risk and demonstrated that onboard systems can contain vulnerabilities arising from default configurations, weak authentication, and insufficient segregation between networks (Svilicic et al., 2019). Such findings are consistent with the broader observation that equipment designed for reliability in isolated environments is now connected to wider networks without commensurate security. Navigation and timing are especially sensitive. Bhatti and Humphreys showed that false satellite signals could mislead a receiver and gradually influence a vessel's

course without raising obvious alarms, illustrating how reliance on a single external signal can be exploited (Bhatti and Humphreys, 2017). The lesson for naval planners is to cross check navigation sources and to monitor for anomalies rather than to trust any one input. Other surfaces include wireless connections, portable devices brought aboard, third party maintenance laptops, and cloud services used for data analysis. Each additional pathway should be justified, controlled, and monitored. The figure below presents an illustrative comparison of the relative exposure of several categories of naval attack surface, as discussed in the literature, expressed on a standardised index from zero to one hundred. The values are stylised to show relative magnitude and should not be read as measured data.

Threat Assessment Methodologies:

Threat assessment seeks to identify what could go wrong, who might cause it, how likely it is, and what the consequences would be. Tam and Jones developed a model based framework for maritime cyber risk assessment that links assets, vulnerabilities, threats, and consequences in a structured way and supports the comparison of risks across ship systems (Tam and Jones, 2019). Such frameworks allow navies to prioritise limited resources toward the most significant exposures. General frameworks provide a foundation. The National Institute of Standards and Technology framework for improving critical infrastructure cybersecurity organises activities into functions of identifying, protecting, detecting, responding, and recovering, offering a common vocabulary for organisations of different kinds (National Institute of Standards and Technology, 2018). Maritime guidance has adapted similar principles, and the International Maritime Organization requires that cyber risk be addressed within safety management systems, which signals that cyber risk is now regarded as part of operational safety (International Maritime Organization, 2017). Methods used in assessment include asset inventories, dependency mapping, vulnerability scanning of systems that can be safely tested, penetration testing in controlled environments, red team exercises that emulate adversary behaviour, and scenario analysis that explores the consequences of loss or manipulation of key functions. Intelligence on adversary techniques informs the choice of scenarios and the assessment of likelihood. Several cautions apply. Testing operational technology on live platforms can itself create safety risks, so laboratories and test beds are preferable. Likelihood is hard to estimate for deliberate adversaries, whose behaviour adapts to defences. Assessments become outdated quickly and must be refreshed as systems, configurations, and threats change. Finally, results should be communicated in terms of operational consequences, such as loss of navigation accuracy or delayed weapons response, so that commanders can understand and act on them.

Navigation, Communications, and Combat System Vulnerabilities:

Certain systems are so critical to naval operations that their protection receives special emphasis. Navigation and timing systems support safe passage, formation keeping, and the synchronisation of other equipment. Interference, deception, or loss of satellite signals can degrade accuracy and disrupt dependent systems, which is why naval forces combine satellite navigation with inertial and other independent sources and train crews to navigate without electronic aids (Bhatti and Humphreys, 2017). Communications are another critical dependency. Naval forces rely on links that range from line of sight radio to satellite connections, and these links are subject to jamming, interception, and compromise of keys and configuration. Because ships often have limited bandwidth, security measures must be efficient, and operational procedures must allow continued command in degraded conditions, using reduced emissions, alternative paths, and pre planned instructions based on commander's intent. Combat management and weapon control systems integrate sensor data and support decisions on engagement. Their consequences make them high value targets, although they are often better protected and more isolated than administrative networks. The principal risks concern corruption of data that feed these systems, compromise of software during maintenance or updates, and unauthorised access through interfaces that connect them to other networks. Maintaining strict segregation, controlling data flows through carefully designed gateways, and verifying the integrity of software are central safeguards. Machinery and platform control systems, which govern power and propulsion, present a safety dimension. Manipulation of these systems could affect the ability of a vessel to manoeuvre or remain afloat. Svilicic and colleagues noted that operational technology on ships often lacks basic security features and may have been commissioned with default credentials and open interfaces (Svilicic et al., 2019). Hardening these systems, while preserving their safety functions and reliability, is a demanding engineering task that requires cooperation between cyber specialists and marine engineers.

Supply Chain and Shore Infrastructure Risks:

Naval systems are built from components and software supplied by many organisations across several countries. This supply chain is a major source of risk. Compromised hardware, malicious or vulnerable software libraries, tampered updates, and weak security at suppliers can all introduce weaknesses before a system reaches the fleet. Because adversaries can target a smaller, less protected supplier to reach a more heavily defended customer, security in the supply chain is only as strong as its weakest link. Shipyards, maintenance depots, and contractors pose particular exposure. They handle sensitive design data and often connect directly to vessels during repair and upgrade. Maintenance laptops, diagnostic tools, and removable media may carry malware between networks if not carefully controlled. The long lifecycle of naval equipment means that systems must be supported and updated for decades,

during which suppliers may change, merge, or cease operations. Shore infrastructure forms another dependency. Ports, fuel depots, power supplies, satellite ground stations, and data centres underpin deployed operations. Libicki observed that cyber operations may be used to disrupt the supporting infrastructure of a military force, and that the difficulty of attribution and the uncertainty of effects complicate deterrence and response (Libicki, 2009). A disruption of logistics or communications ashore can hamper operations at sea without any direct attack on a warship. Mitigation requires supply chain risk management that includes supplier vetting, contractual security requirements, software bills of materials, integrity verification of updates, and monitoring of third party access. Governments can also pursue diversification of suppliers, trusted manufacturing, and joint standards with allies. These measures take time and cost money but reduce systemic vulnerability.

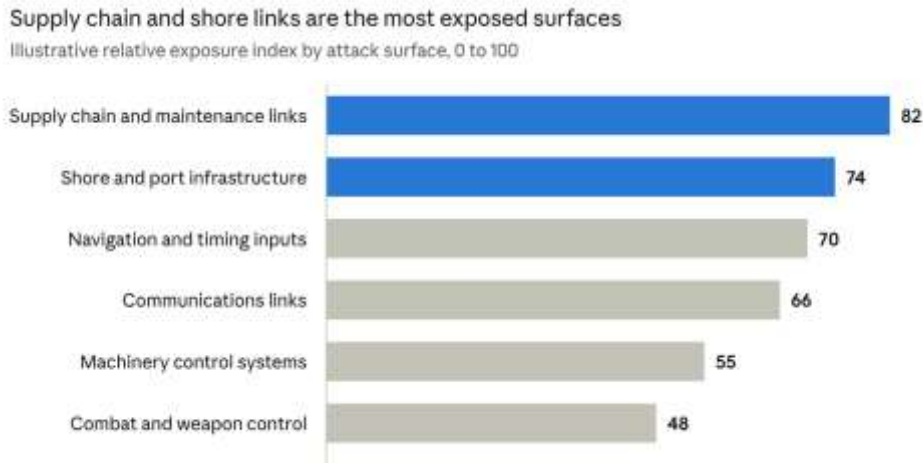
Mitigation Strategies and Defence in Depth:

No single control can secure a complex naval system, so effective strategies rely on layers. Defence in depth combines measures at several levels so that the failure of one does not lead to compromise. The first layer is architectural. Networks should be segmented so that a breach in one area cannot easily spread to others, and critical operational technology should be separated from administrative and internet connected systems, with tightly controlled gateways between them. The second layer is access control and identity. Zero trust principles, which assume that no user, device, or network location is inherently trusted and that every access request must be verified, are increasingly applied to defence networks (Rose et al., 2020). Strong authentication, least privilege, and continuous verification reduce the damage that stolen credentials or malicious insiders can cause. In the shipboard environment, these principles must be adapted to constraints such as intermittent connectivity and the need for rapid access in emergencies. The third layer is detection and response. Monitoring of network traffic, system behaviour, and configuration changes can reveal intrusions early, and the intrusion kill chain model suggests that disrupting an adversary at any stage can prevent success (Hutchins et al., 2011). Ships need onboard capability for detection and initial response, supported by shore based security operations centres that can analyse data, share threat intelligence, and coordinate reaction across the fleet. The fourth layer is resilience. Systems should be designed to degrade gracefully, with manual fallback options and the ability to recover quickly from compromise. Regular backups, tested recovery procedures, and the maintenance of analogue or alternative means of navigation, communication, and control all contribute. Security also needs to be built into acquisition, so that new systems are designed with secure architectures, patching mechanisms, and testing before delivery, rather than having protection added later.

Human Factors, Training, and Organisational Resilience:

Many cyber incidents begin with human error or manipulation. Phishing messages, careless handling of removable media, weak passwords, and failure to follow procedures are common causes. Reason's analysis of human error distinguished between active failures by individuals and latent conditions in organisations that make failure more likely, and he argued that managing the latter is vital to safety (Reason, 1990). The same logic applies to cyber security, where design choices, workload, and culture shape the likelihood of mistakes. Training is therefore essential. Naval personnel at all levels need to understand the basic threats, recognise suspicious behaviour, and know how to report incidents without fear of blame. Specialist cyber and engineering staff need advanced skills and opportunities to practise in realistic environments. Exercises that combine cyber events with operational scenarios help commanders understand the consequences and rehearse decisions under pressure. Boyes and Isbell, in a code of practice for cyber security on ships, stress that security must be part of overall ship management, with defined responsibilities, procedures, and awareness among crew, rather than a purely technical matter handled by specialists (Boyes and Isbell, 2017). Their approach reflects the principle that people, processes, and technology must be addressed together. Organisational resilience also depends on leadership and culture. Leaders should make cyber risk visible, resource it adequately, and treat incident reporting as a source of learning. Retention of skilled personnel is a continuing challenge, since cyber expertise is in high demand in the commercial sector. Career paths, incentives, and partnerships with industry and academia can help navies attract and keep the talent they need. Effective cyber defence requires clear governance. Responsibilities should be defined for system owners, operators, security authorities, and commanders, and standards should be applied consistently across platforms and bases. The requirement to integrate cyber risk into safety management reflects a growing recognition that cyber resilience is part of operational readiness (International Maritime Organization, 2017). Regular audits, independent testing, and reporting to senior leadership help maintain accountability. International cooperation is important. Navies operate together, share data, and depend on common infrastructure, so weaknesses in one partner can affect others. Sharing threat intelligence, aligning standards, and conducting combined cyber exercises can improve collective resilience. Cooperation with commercial shipping and port operators is also valuable, since civil and military maritime systems are closely intertwined. Several future developments will shape the challenge. Greater autonomy, artificial intelligence, and the growth of connected sensors will expand the attack surface and introduce new vulnerabilities, such as manipulation of the data on which machine learning systems depend. Quantum computing may eventually threaten current cryptographic methods, which makes

planning for cryptographic agility prudent. At the same time, defensive technologies, including automated detection and response, may improve the ability to protect complex systems. Research priorities include methods for safely testing operational technology, metrics for the effectiveness of cyber defences, and approaches to maintaining operations under sustained degradation. Singer and Friedman's observation that cyberspace changes the nature of conflict without removing its human and political foundations suggests that technical solutions must be accompanied by strategy, doctrine, and judgement (Singer and Friedman, 2014).



Summary:

This article has examined cybersecurity challenges in modern naval defence systems and the strategies available to address them. Naval forces depend on interconnected systems for navigation, communications, sensing, weapon control, and platform management, which creates both capability and vulnerability. Threats come from state actors, criminals, hacktivists, and insiders, and the attack surface extends across ships, supply chains, and shore infrastructure. Structured assessment methods help prioritise risks, while mitigation relies on layered defences, segmentation, zero trust principles, monitoring, and resilience, supported by training and sound governance. Because adversaries adapt and equipment lasts for decades, cyber security must be treated as a continuing process embedded in design, acquisition, operations, and culture. Navies that map their dependencies, prepare to operate in degraded conditions, and cooperate with allies and industry will be better placed to preserve their operational effectiveness in a contested digital environment.

References:

- Bhatti, J., and Humphreys, T. E. (2017). Hostile control of ships via false GPS signals: Demonstration and detection. *NAVIGATION*, 64(1), 51–66.
- Boyes, H., and Isbell, R. (2017). *Code of Practice: Cyber Security for Ships*. London: Institution of Engineering and Technology.
- Hutchins, E. M., Cloppert, M. J., and Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare and Security Research*, 1(1), 80–106.
- International Maritime Organization. (2017). *Maritime Cyber Risk Management in Safety Management Systems (Resolution MSC.428(98))*. London: IMO.
- Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation.
- National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. Gaithersburg: NIST.
- Reason, J. (1990). *Human Error*. Cambridge: Cambridge University Press.
- Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*, 35(1), 5–32.
- Rose, S., Borchert, O., Mitchell, S., and Connelly, S. (2020). *Zero Trust Architecture (NIST Special Publication 800-207)*. Gaithersburg: National Institute of Standards and Technology.

- Singer, P. W., and Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press.
- Svilicic, B., Kamahara, J., Rooks, M., and Yano, Y. (2019). Maritime cyber risk management: An experimental ship assessment. *Journal of Navigation*, 72(5), 1108–1120.
- Tam, K., and Jones, K. (2019). MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, 18(1), 129–163.