Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p26352-cd

Dynamic Assessment of Maritime Cybersecurity Risk: A System Dynamics Approach

Shushan He

Centre for Risk Research, Department of Decision Analytics & Risk , University of Southampton Business School, University of Southampton, United Kingdom. E-mail: Sh2u21@soton.ac.uk

Mario P. Brito

Centre for Risk Research, Department of Decision Analytics & Risk , University of Southampton Business School, University of Southampton, United Kingdom. E-mail: M.P.Brito@soton.ac.uk

Nawfal Al Hashimy

School of Electronics and Computer Science, University of Southampton, United Kingdom. E-mail: Nawfal@soton.ac.uk

This study develops a socio-technical system dynamics(SD) model for dynamic cybersecurity risk assessment of autonomous vessel navigation systems under GNSS spoofing threats. Cybersecurity risk in this context is inherently socio-technical, emerging from the interaction between technical navigation vulnerabilities, human-in-the-loop operational behavior, organizational investment decisions, and recovery processes.
The proposed model represents an integrated ship-shore system and conceptualizes cybersecurity risk as an evolving system behavior shaped by feedback loops. By explicitly modeling feedback,time delays, and capacity limits, the framework moves beyond static probability-consequence approaches commonly used in maritime cybersecurity assessment.
The developed model was assessed for plausibility using standard SD validation approach. The model is then used to simulate alternative cybersecurity management strategies to examine how cyber risk evolves under contrasting policy choices. Simulation results highlight non-linear risk responses, in which successful attacks and associated losses change over time as system conditions and management action interact. By operationalizing cybersecurity risk as scenario, consequences and occurrence, the study offers a feedback-driven decision-support framework for autonomous vessel.

Keywords: Maritime Cybersecurity, System Dynamics, Socio-Technical Modeling, Risk Analysis, Cyber Risk.

1. Introduction

The maritime sector is undergoing rapid digitalization, resulting in growing reliance on software-driven navigation systems, such as the Global Navigation Satellite System (GNSS) Bolbot et al. (2022). While these technologies enhance navigational efficiency and safety, they simultaneously expand the cyber attack surface. This issue is particularly pronounced in autonomous vessels, where navigation functions are governed by complex software architectures with limited direct human oversight Wróbel et al. (2020).

Within this context, GNSS spoofing represents a critical cybersecurity threat due to its direct impact on positioning integrity. In autonomous vessel operations, compromised navigation data can propagate across integrated shipboard and shore-based systems, amplifying operational disruption when human intervention is constrained Tam and Jones (2018). Consequently, navigation-related cybersecurity risks should be understood as systemic socio-technical challenges rather than isolated technical failures.

Despite this, maritime cybersecurity assessment practices largely rely on static representations Tam and Jones (2019), limiting their ability to capture how risk levels and mitigation effectiveness evolve over time and constraining long-term decision-making Afenyo and Caesar (2023).

To address this limitation, this study develops a socio-technical System Dynamics (SD) model to analyze the dynamic evolution of cybersecurity risk in autonomous vessel navigation sys-

tems under GNSS spoofing. The model captures interactions among system vulnerability, human and technical defense capacities, investment behavior, and recovery processes. Scenario-based simulations are used to examine how alternative cybersecurity strategies influence risk trajectories over time, providing a time-dependent decision-support framework.

2. Related Works

Existing maritime cybersecurity research has predominantly focused on navigation-related threats, particularly GNSS spoofing and jamming, providing important insights into attack mechanism and system vulnerabilitiesYu et al. (2023). However, this body of work has largely remained confined to technical analyses.

2.1. *GNSS Spoofing and Maritime Cyber Risk Assessment*

A substantial body of literature examines GNSS spoofing in maritime navigation, primarily focusing on detection methods and signal-level analysis Hopcraft and Martin (2018). While these studies provide valuable technical insights, they typically treat cyber incidents as isolated events and do not capture how vulnerabilities evolve over time or interact with operational processes. In parallel, maritime cybersecurity risk assessment has been advanced through structured frameworks such as MaCRA, which support vulnerability identification and risk evaluation Tam and Jones (2019). However, these approaches are limited in representing temporal dynamics, such as delayed defense accumulation, evolving exposure, and cumulative impacts.

2.2. *System Dynamics in Cybersecurity Modeling*

Although SD has been applied in cybersecurity and critical infrastructure contexts, existing applications are largely limited to generic system settings and do not capture domain-specific risks such as GNSS spoofing in maritime navigation systems Loh et al. (2020). Furthermore, they rarely incorporate socio-technical interactions within integrated ship–shore systems.

2.3. *Research Gap and Novelty*

Based on the above discussion, three key gaps are identified. First, existing GNSS spoofing studies predominantly focus on technical vulnerabilities and detection mechanisms Svilicic et al. (2019), with limited consideration of how cyber risk emerges from socio-technical interactions in autonomous vessel operations. Second, current maritime cybersecurity risk assessment approaches are largely static, providing snapshot-based evaluations that do not capture the dynamic evolution of cyber risk over time. Third, the application of SD to maritime navigation systems remains underdeveloped, limiting the modeling of feedback-driven and time-dependent cyber risk under GNSS spoofing scenarios.

To address these gaps, this study makes three main contributions. First, it develops a socio-technical SD model that integrates navigation-system vulnerability, human and technical defense capacities, and recovery processes within a ship–shore system. Second, it formulates time-dependent cybersecurity management scenarios, including proactive versus reactive investment and vulnerability reduction strategies. Third, it enables dynamic analysis of cyber risk evolution, revealing non-linear effects that cannot be captured by conventional static approaches.

3. Methodology

This study adopts a SD methodology to develop a socio-technical model for dynamic cybersecurity risk assessment in autonomous vessel navigation systems under GNSS spoofing threats. The overall methodology workflow comprises model design, model development, verification and validation, and scenario-based numerical simulation. In this research, the development of stock-flow diagram, the implementation of verification and validation checks, and execution of simulations are all carried out using the Vensim PLE platform.

3.1. *Model Design*

The model design phase establishes the modeling objective and system boundary. The purpose of the model is to examine how navigation system cybersecurity risk evolves dynamically and how

different cybersecurity management strategies influence risk outcomes over time.

Before the model is formally presented, the following hypotheses are established on prior research on maritime cybersecurity risk and operational characteristics of autonomous vessels Tam and Jones (2019).

The system boundary is restricted to a single autonomous vessel and its associated shore control center. The model will capture the endogenous evolution of navigation system cyber vulnerability and cyber defense capacity through technical, human, and managerial mechanisms, while cyber attacks are treated as exogenous intrusion attempts whose success emerges from system interactions rather than explicit attack vectors. Human-in-the-loop cyber defense behavior, technical defense investment, and recovery actions are included insofar as they affect navigation-related operational damage.

3.2. *Case Description*

A representative autonomous surface vessel is adopted as the case study to evaluate the proposed model, as its high level of automation results in extensive reliance on cyber systems, making it particularly susceptible to cyber attacks. The analysis focuses on the navigation system, which is essential for autonomous operation and directly influences vessel safety Kavallieratos et al. (2019). GNSS spoofing is selected as the representative attack scenario because its effects on navigation performance are quantifiable and therefore well suited for model-based analysis Bolbot et al. (2022).

3.3. *Model Development*

The model is simulated 30-month horizon with a monthly time step, which is sufficient to represent delayed defense accumulation, vulnerability growth, and persistence of operational impacts, while avoiding excessive long-term uncertainty common in cybersecurity forecasting Nazareth and Choi (2015). Model outputs focus on the number of successful attacks and cumulative navigation-related operational damage, which together characterize the evolving cybersecurity risk profile.

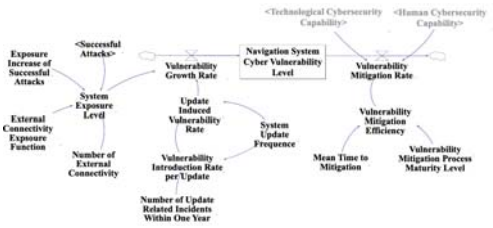

Fig. 1.Navigation system cyber vulnerability subsystem

3.3.1. *Stock and Flow Diagram*

The model is implemented as a stock–flow diagram comprising four interacting subsystems: navigation system cyber vulnerability, human cybersecurity capability, technological cybersecurity capability, and attack impact and recovery.

3.3.2. *Navigation System Cyber Vulnerability Subsystem*

This subsystem (Fig. 1) models the dynamic evolution of navigation-system cyber vulnerability level. Navigation system cyber vulnerability is represented as a stock variable capturing the accumulated level of cyber exposure, which increases through vulnerability growth and decreases through mitigation and defense capacity over time. Vulnerability growth arises from system exposure due to increasing external connectivity and ship–shore integration, as well as update-induced vulnerabilities introduced during software updates and system integration Tam and Jones (2018). Vulnerability mitigation is jointly determined by human cyber defense capacity and technical navigation-system defenses, scaled by mitigation effectiveness Vasan et al. (2025).

3.3.3. *Human Cybersecurity Capability Subsystem*

This subsystem (Fig. 2) models the dynamic evolution of human cybersecurity capability. Human cybersecurity capability is represented as an accumulated stock capturing the ability of onboard and shore-based personnel to detect and respond to navigation-related cyber anomalies. Capacity increases through cybersecurity awareness training,

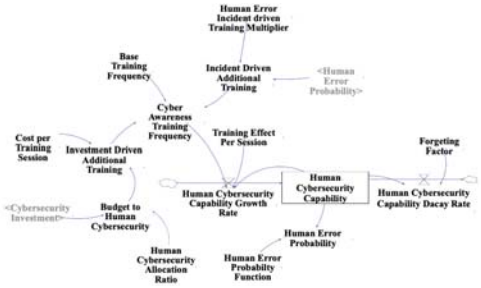

Fig. 2.Human cybersecurity capability subsystem

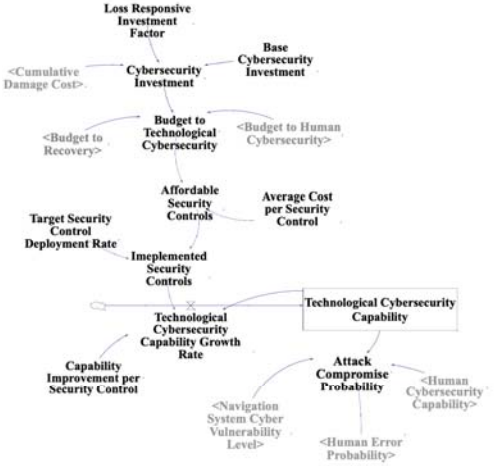

Fig. 3.Technological cybersecurity capability subsystem

whose effectiveness exhibits diminishing returns, and adapts endogenously to organizational investment decisions and perceived cyber risk Kanwal et al. (2024). In parallel, human cybersecurity capability gradually decays over time due to forgetting effects in the absence of sustained training, providing a counterbalancing dynamic to capability accumulation Haugli-Sandvik et al. (2024).

3.3.4. *Technological Cybersecurity Capability Subsystem*

This subsystem (Fig. 3) represents the dynamic accumulation of technological cybersecurity capability within the vessel's navigation system. Technological cybersecurity capability is modeled as an accumulated stock reflecting protection embedded in navigation-related hardware, software, and

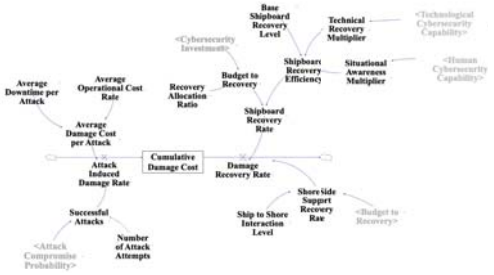

Fig. 4.Attack impact and recovery subsystem

system configurations through security hardening and upgrade activities. Capacity growth is driven by targeted defense upgrades, whose effectiveness depends on implementation quality and upgrade frequency, and is endogenously constrained by organizational cybersecurity investment and project costs, resulting in gradual rather than instantaneous defense accumulation Alcaide and Llave (2020). As technological cybersecurity capability increases, it reduces the probability of successful attacks, together with human cybersecurity capability and system cyber vulnerability.

3.3.5. *Attack Impact and Recovery Subsystem*

This subsystem (Fig. 4) captures how successful GNSS spoofing attacks translate into navigation related operational losses and how these losses are mitigated through recovery over time. Operational impact is represented as an accumulated stock of cumulative damage cost, reflecting the gradual resolution of cyber-induced disruption. Damage accumulation is driven by the frequency of successful attacks and their navigation-dependent operational consequences, such as degraded navigation performance leading to downtime and economic loss. Recovery is split into shipboard recovery and shore-side support, reflecting the operational reality of autonomous vessels. Sumon et al. (2025). Human and technological cybersecurity capability indirectly influence this subsystem by reducing attack success and enhancing recovery efficiency.

3.4. *Model Verification and Validation*

Prior to numerical simulation, the proposed model was verified and validated to assess structural

correctness and behavioral plausibility. Following established SD practice Sterman (2000), the evaluation focused on dimensional consistency, extreme condition behavior, and the reproduction of plausible dynamic patterns.

Dimensional consistency checks were applied to all equations to ensure unit compatibility among stocks, flows, and auxiliary variables. In addition, the causal structure and feedback loops were reviewed against the conceptual framework and relevant maritime cybersecurity literature to ensure theoretical coherence.

Model robustness was examined through a set of extreme condition tests across the four subsystems, adopting the methodology in Zhang et al. (2025). The tested parameters and their baseline and extreme values are summarized in Table 1. These tests apply intentionally unrealistic but structurally informative inputs to evaluate whether model behavior remains logically consistent.

The resulting system responses are illustrated in Fig. 5. Across all scenarios, the model exhibits internally consistent behavior. For example, extreme increases in external connectivity or attack frequency lead to rapid escalation of navigation-system vulnerability and cumulative damage.

Given the limited availability of longitudinal maritime cybersecurity data, validation focuses on pattern-oriented assessment rather than point-wise historical fitting Barlas (1996). A baseline scenario is defined to represent the reference evolution of cybersecurity risk under typical system conditions, including cybersecurity investment,initial defense capacities, and background attack frequency. This establishes a benchmark trajectory of attack success, damage accumulation, and defense development in the absence of targeted interventions Armenia et al. (2021).

As shown in Fig. 6, the baseline simulation exhibits an escalation–adaptation pattern: successful attacks initially increase with rising exposure and limited defenses, and subsequently decline as delayed cybersecurity capabilities take effect. This behavior is consistent with prior cybersecurity studies and empirical evidence on GNSS spoofing Androjna and Perkovič (2021).

4. Strategy Design

Building on the baseline scenario, two classes of cybersecurity management strategies are designed to examine how alternative decision logic shape risk dynamics over time.

The first strategy considers cybersecurity investment by contrasting proactive investment, characterized by higher baseline spending, with reactive investment triggered by accumulated losses, reflecting trade-offs between anticipatory and loss-driven security decisions Nazareth and Choi (2015).

The second strategy focuses on vulnerability management by reducing external system exposure and accelerating mitigation processes, representing organizational measures such as network segmentation and improved incident response that limit attack propagation and damage accumulation Bolbot et al. (2022).

By comparing the time-dependent trajectories of successful attacks and cumulative damage across scenarios, the model enables systematic evaluation of long-term cyber risk dynamics and trade-offs across alternative cybersecurity management strategies.

5. Result Analysis

As established above, the baseline simulation defines a plausible reference trajectory against which subsequent strategies are evaluated.

5.1. *Cybersecurity Investment Strategy*

Fig. 8 compares proactive and reactive cybersecurity investment strategies. Under reactive investment, delayed resource allocation allows elevated attack success rates to persist, leading to sustained accumulation of operational damage. In contrast, proactive investment accelerates defense capacity development, suppresses attack success earlier, and stabilizes cumulative damage at a lower level. The results demonstrate that investment timing is critical, early commitment reduces long-term cyber risk more effectively than loss-triggered responses.

Table 1.Input parameters for the extreme condition tests of the four subsystems

	Vulnerability Subsystem	**Human Cybersecurity Subsystem**	**Technological Cybersecurity Subsystem**	**Attack Impact Subsystem**
Extreme condition name	Extreme Connectivity	Extreme Training	Extreme Investment	Extreme Attack
Description	An extreme scenario with unusually high external system connectivity	An extreme scenario with very intensive cyber awareness training	An extreme scenario with significantly reduced cybersecurity investment	An extreme scenario with exceptionally high attack frequency
Tested variable	Number of external connectivity interfaces	Base training frequency	Base cybersecurity investment	Number of attack attempts
Base condition value	11 (Interface)	0.3 (Session/Month)	8000 (£/Month)	5 (Attack/Month)
Extreme condition value	55 (Interface)	3 (Session/Month)	800 (£/Month)	50 (Attack/Month)

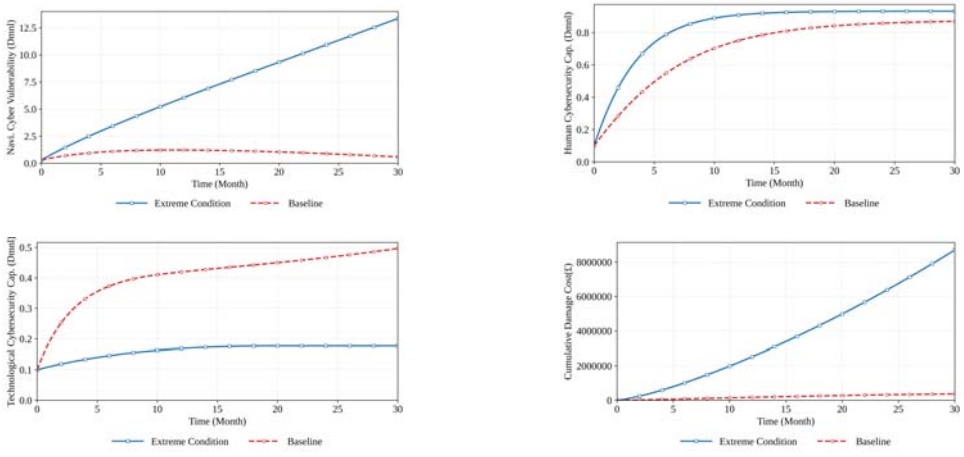

Fig. 5.Extreme condition responses

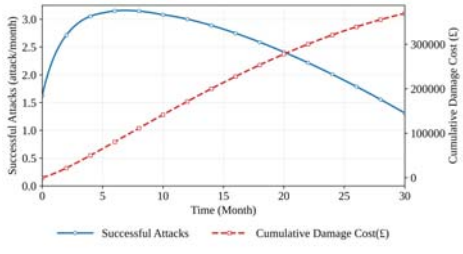

Fig. 6.Baseline simulation results of attack and cost dynamics

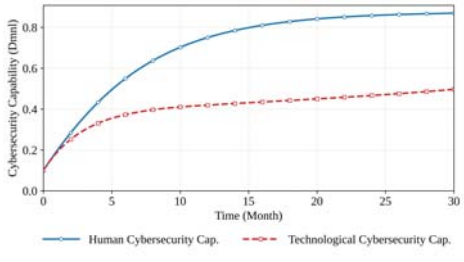

Fig. 7.Baseline simulation results of defense dynamics

5.2. *Vulnerability management strategy*

Fig. 9 shows the impact of vulnerability management through reduced external connectivity and

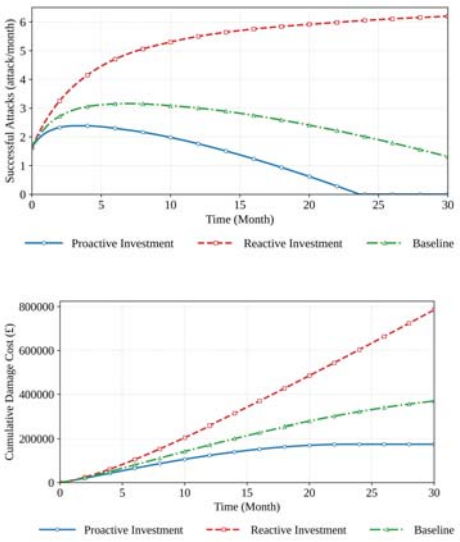

Fig. 8.Simulation result of different cybersecurity investment strategy

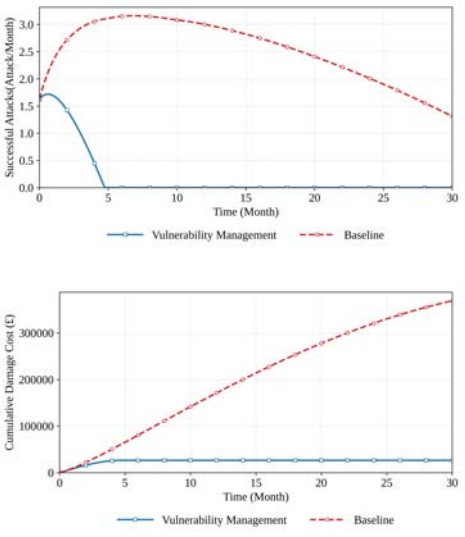

Fig. 9.Simulation result of vulnerability management strategy

faster mitigation. Successful attacks are rapidly suppressed, reaching near-zero levels within the first 6–8 months. Consequently, cumulative operational damage stabilizes early rather than increasing over time. These results indicate that structural vulnerability reduction provides a fast and decisive risk control mechanism, outperforming strategies that rely primarily on gradual defense accumulation.

6. Conclusion

This paper developed a SD-based framework to assess cybersecurity risk in autonomous vessel navigation systems under GNSS spoofing threats. By modeling navigation-system vulnerability, human and technical defense capacities, and attack impact and recovery as interacting stocks and flows, the approach captures how cyber risk evolves over time. Simulation results show that cyber risk initially escalates due to high exposure and delayed defense accumulation, before stabilizing as defensive capacities mature. Strategy analysis demonstrates that proactive investment and targeted vulnerability management significantly reduce successful attack incidents and cumulative operational damage, while reactive investment allows elevated risk to persist. The findings highlight the importance of accounting for feedback, delay, and accumulation effects in maritime cybersecurity risk management and provide a dynamic decision-support basis for evaluating cybersecurity strategies in autonomous vessel operations.

References

Afenyo, M. and L. D. Caesar (2023). Maritime cybersecurity threats: Gaps and directions for future research. *Ocean & Coastal Management 236*, 106493.

Alcaide, J. I. and R. G. Llave (2020). Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia 45*, 547–554.

Androjna, A. and M. Perkovič (2021). Impact of spoofing of navigation systems on maritime situational awareness. *Transactions on Maritime Science 10*(02), 361–373.

Armenia, S., M. Angelini, F. Nonino, G. Palombi, and M. F. Schlitzer (2021). A dynamic simulation approach to support the evaluation of

cyber risks and security investments in smes. *Decision Support Systems 147*, 113580.

Barlas, Y. (1996). Formal aspects of model validity and validation in system dynamics. *System Dynamics Review: The Journal of the System Dynamics Society 12*(3), 183–210.

Bolbot, V., K. Kulkarni, P. Brunou, O. V. Banda, and M. Musharraf (2022). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection 39*, 100571.

Haugli-Sandvik, M., M. S. Lund, and F. B. Bjørneseth (2024). Maritime decision-makers and cyber security: deck officers' perception of cyber risks towards it and ot systems. *International Journal of Information Security 23*(3), 1721–1739.

Hopcraft, R. and K. M. Martin (2018). Effective maritime cybersecurity regulation–the case for a cyber code. *Journal of the Indian Ocean Region 14*(3), 354–366.

Kanwal, K., W. Shi, C. Kontovas, Z. Yang, and C.-H. Chang (2024). Maritime cybersecurity: are onboard systems ready? *Maritime Policy & Management 51*(3), 484–502.

Kavallieratos, G., S. Katsikas, and V. Gkioulos (2019). Cyber-attacks against the autonomous ship. In *Computer Security: ESORICS 2018 International Workshops, CyberICPS 2018 and SECPRE 2018, Barcelona, Spain, September 6–7, 2018, Revised Selected Papers 2*, pp. 20–36. Springer.

Loh, T. Y., M. P. Brito, N. Bose, J. Xu, and K. Tenekedjiev (2020). Human error in autonomous underwater vehicle deployment: a system dynamics approach. *Risk Analysis 40*(6), 1258–1278.

Nazareth, D. L. and J. Choi (2015). A system dynamics model for information security management. *Information & management 52*(1), 123–134.

Sterman, J. D. (2000). *Business Dynamics: Systems Thinking and Modeling for a Complex World* (1 ed.). New York, NY: McGraw-Hill Education.

Sumon, M. M. A., H. Kim, and B. Rokseth (2025). Hazard analysis of autonomous vessel operation during the interaction and execution between remote operation centre controller and onboard controllers. *Journal of Shipping and Trade 10*(1), 25.

Svilicic, B., J. Kamahara, J. Celic, and J. Bolmsten (2019). Assessing ship cyber risks: A framework and case study of ecdis security. *WMU Journal of Maritime Affairs 18*(3), 509–520.

Tam, K. and K. Jones (2019). Macra: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs 18*, 129–163.

Tam, K. and K. D. Jones (2018). Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. *Journal of Cyber Policy 3*(2), 147–164.

Vasan, D., M. Hammoudeh, A. F. Ahmed, and H. Naeem (2025). Cyber-attacks: Securing ship navigation systems using multi-layer cross-validation defense. *Computers & Security*, 104706.

Wróbel, K., M. Gil, and J. Montewka (2020). Identifying research directions of a remotely-controlled merchant ship by revisiting her system-theoretic safety control structure. *Safety Science 129*, 104797.

Yu, H., Q. Meng, Z. Fang, and J. Liu (2023). Literature review on maritime cybersecurity: state-of-the-art. *The Journal of Navigation 76*(4-5), 453–466.

Zhang, J., X. Xin, R. Dubey, T. T. Nguyen, X. Shi, N. Li, and Z. Yang (2025). Impact of the ripple effect on the resilience of multimodal container port operations: A system dynamics simulation approach. *Risk Analysis*.