sciendo

Land Forces Academy Review
Vol. XXX, No. 3(119), 2025

EXPLORING RISK MANAGEMENT OF MARITIME LOGISTICS INFORMATION TECHNOLOGY PROJECTS AND ASSOCIATED CYBERSECURITY CONSTRUCTS

Jessica PARKER
Marymount University, Arlington, VA, USA
ORCID: https://orcid.org/0009-0008-9574-327
j0p80903@marymount.edu

Darrell Norman BURRELL
Marymount University, Arlington, VA, USA
ORCID: https://orcid.org/0000-0002-4675-9544
dburrell@marymount.edu

Calvin NOBLES
University of Maryland Global Campus, Adelphi, MD, USA
ORCID: https://orcid.org/0000-0003-4002-1108
calvin.nobles@umgc.edu

Matthew SHEFFIELD
Marymount University, Arlington, VA, USA
mss85819@marymount.edu

ABSTRACT

The Department of Defense (DoD) confronts formidable challenges in modernizing maritime logistics and supply chain IT systems essential for military readiness and national security. Transformation efforts must navigate complex interagency coordination, cybersecurity risks, and operational demands across multi-domain environments. This qualitative study, drawing insights from seasoned former logistics officers, examines best practices for mitigating risks inherent in such initiatives. Key strategies include integrating robust risk management frameworks, enhancing cybersecurity, ensuring interoperability, and employing advanced analytics to inform decision-making. The research underscores the value of continuous stakeholder engagement, regulatory compliance, scenario planning, and the adoption of emerging technologies such as artificial intelligence to improve resilience and efficiency. By addressing the prevalent failure rates of digital transformation projects, these recommendations offer a pragmatic roadmap for building agile, modern logistics systems. The findings hold critical implications for the DoD's capacity to respond rapidly to crises, safeguard national security interests, and support humanitarian operations.

KEYWORDS: Maritime Logistics IT, Digital Transformation, Risk Management, Supply Chain Modernization, Logistics Management Technology

JEL Codes: C61, D81, L91, M15, O33

DOI: 10.2478/raft-2025-0042
© 2025 Jessica Parker et al. This work is licensed under the Creative Commons Attribution-Non Commercial-No Derivatives 3.0 License.

1. Introduction

The U.S. Department of Defense (DoD) aims to provide military forces capable of deterring conflict and safeguarding national security (U.S. Department of Defense, 2022; Deputy Assistant Secretary of Defense for Logistics, 2024). To achieve this, the DoD needs to manage and optimize its data and technology as critical strategic resources, supporting a robust, coordinated military organization that, in partnership with allied nations, maintains American influence while supporting collective security and global prosperity (Metz, 2024). The scope of the Maritime Logistics Information Technology (Log IT) portfolio spans cybersecurity, audit requirements, regulatory compliance, inventory visibility, and modernization (Lopez, 2024). Log IT is part of an overall defense strategy to optimize systems and enhance capabilities and decision-making with actionable data (Metz, 2024). In defense organizations, transformational technology projects come with challenges that must be addressed to manage risk effectively, protect valuable logistics data, and ensure quality, interoperability, and integration with evolving technologies like Artificial Intelligence (Deputy Assistant Secretary of Defense, 2024).

For national security-focused maritime organizations, like the DoD, digital transformation and modernization have become integral to achieving their mission (Deputy Assistant Secretary of Defense, 2024). However, digital transformation projects are complex and impact the organization beyond technological changes (Kraus et al., 2021; Detrow & Roughead, 2024). Research consistently highlights the high failure rates of digital transformation projects, indicating that 70% fail to meet their intended goals (Bloch et al., 2012) and, despite more than a decade of progress, a 2023 KPMG study reported a 51% failure rate in the U.S. (KPMG, 2023). These failures reduce profitability, impede performance, and prevent organizations from enhancing capabilities (KPMG, 2023). When modernizing systems responsible for the defense of a nation, particular care is needed to avoid adverse outcomes that put lives at risk. Applying well-researched practices in problem-solving and risk management can assist organizations in overcoming the hurdles and complexities of digital transformation for networked systems like Log IT.

In the complex landscape of modern warfare, where traditional operations and sophisticated cyber and data-driven strategies intersect (Detrow & Roughead, 2024), maritime Log IT serves as both a weapon and a vulnerability (Deputy Assistant Secretary of Defense for Logistics, 2024). Enhancing maritime Log IT systems will strengthen the DoD's capacity to prevail in conflicts, particularly in an era of competition between major powers where warfare has become increasingly dependent on technology (Detrow & Roughead, 2024). By optimizing logistics data management and analysis, the U.S. supply chain is strengthened, and military leaders can exploit untapped strategic, operational, and tactical opportunities, ensuring that the U.S. military remains superior in conventional and unconventional warfare (Deputy Assistant Secretary of Defense for Logistics, 2024).

2. Problem Statement

The DoD faces the challenge of transforming maritime technology systems to enhance military readiness and ensure national security. Actionable and effective risk management techniques are critical in an environment with cybersecurity responsibilities distributed across multiple agencies (Metz, 2024). Moreover, an organization must coordinate activities across multiple military agencies and

external allied forces (Deputy Assistant Secretary of Defense for Logistics, 2024). As the Log IT portfolio is vital for national security, it must also be resilient enough as it relates to risk management planning frameworks to function when communications are impeded and when the military is engaged in warfare (Deputy Assistant Secretary of Defense for Logistics, 2024). The successful transformation of the Log IT network of systems is a key strategic objective of the DoD, enabling improved logistics command and control (Deputy Assistant Secretary of Defense for Logistics, 2024).

2.1. Purpose of the Inquiry

Applied research in the domain of maritime logistics and supply chain IT systems serves a crucial purpose: to bridge the persistent gap between theoretical knowledge and the operational realities confronting defense organizations. This inquiry is motivated not by abstract curiosity alone, but by the urgent need to identify practical solutions that can directly enhance military readiness and national security. As digital transformation initiatives continue to suffer high failure rates, the purpose of this research is to illuminate viable pathways for overcoming systemic risks, such as cybersecurity vulnerabilities, data interoperability challenges, and logistical inefficiencies. By engaging practitioners who possess firsthand operational expertise, the study aims to extract insights that are immediately relevant and implementable, thus ensuring that research outcomes extend beyond academic discourse to deliver tangible value within high-stakes environments.

Equally important, this inquiry is purpose-driven in seeking to produce knowledge that can inform strategic decisions and operational policies. The focus on best practices and risk mitigation frameworks reflects the essential role of applied research in shaping interventions that are evidence-based, context-sensitive, and capable of mitigating the consequences of technological failures. For the DoD, where logistical breakdowns can compromise mission success and national security, research that delivers actionable strategies is not merely beneficial, it is indispensable. Thus, the purpose of this inquiry is firmly rooted in translating knowledge into practice, empowering decision-makers to implement reforms that strengthen resilience, operational agility, and technological integration across maritime logistics systems.

2.2. Significance and Novelty of the Inquiry

The significance of this inquiry lies in its direct engagement with the operational imperatives of national defense logistics, a domain where technological efficacy and strategic readiness are inextricably linked. Applied research such as this addresses a critical gap by not merely diagnosing the high failure rates of digital transformation projects but offering context-specific, actionable remedies. Unlike purely theoretical studies, the present inquiry delivers practical frameworks and recommendations that defense organizations can adopt to enhance their logistics systems' security, efficiency, and interoperability. In doing so, it contributes to safeguarding national interests and mitigating the risk of systemic disruptions that could compromise both military operations and humanitarian response capabilities.

Moreover, the novelty of this research is embedded in its methodological approach and its substantive focus on multi-domain interoperability and cybersecurity within maritime logistics – a nexus of concerns that has been insufficiently explored in prior literature. By incorporating iterative focus group methodologies and leveraging insights from experienced logistics officers,

the study transcends surface-level analysis to capture the tacit, operational knowledge essential for effective transformation. This approach yields a nuanced understanding of how technological and organizational variables intersect in complex defense environments. The research's emphasis on practical solutions, validated through expert consensus and triangulation with existing literature, underscores its originality and ensures that its contributions are both innovative and immediately applicable to the pressing challenges facing national security infrastructures.

2.3. Nature of the Inquiry

This inquiry is inherently applied, problem-focused, and solution-oriented, distinguishing itself from purely theoretical research by prioritizing practical outcomes that can inform policy and operational practice. Its nature is characterized by a deliberate engagement with real-world complexities, specifically, the transformation of maritime logistics IT systems in environments marked by geopolitical tensions, cybersecurity threats, and operational uncertainty. Rather than seeking to develop abstract models detached from context, the research interrogates the lived experiences and expert insights of practitioners tasked with navigating these challenges. By doing so, it aims to generate knowledge that is not only academically rigorous but operationally relevant, ensuring that its findings can be integrated into ongoing efforts to modernize and secure critical defense infrastructures.

Furthermore, the inquiry's applied nature is reinforced by its methodological design, which emphasizes participatory, iterative engagement through focus groups and structured brainstorming techniques. This participatory approach fosters the co-creation of knowledge between researchers and practitioners, enhancing both the credibility and applicability of the findings. It reflects the principle that solutions to complex organizational challenges cannot emerge solely from theoretical postulation but must be rooted in the practical wisdom and adaptive strategies developed by those working directly within the field. Thus, the nature of this inquiry is deeply aligned with the ethos of applied research: to transform scholarly insight into actionable guidance that solves pressing real-world problems and strengthens institutional resilience.

3. Background

The DoD's ability to manage maritime Log IT systems directly impacts national security. As warfare increasingly incorporates cyber and data-driven strategies, the quality and accuracy of logistics data become both a powerful asset and an area of risk. Ensuring that IT projects within the DoD are successful by using research-proven techniques for problem-solving and risk management helps maintain the operational readiness of military forces, ensuring that they can deter conflict and respond swiftly to threats.

Digital logistics systems are equally important in disaster and humanitarian relief efforts, where rapid deployment and resource management are critical (Niyazi & Behnamian, 2023). Technology that supports logistics can precisely coordinate supplies, personnel, and relief efforts, even when communication infrastructure is damaged (Niyazi & Behnamian, 2023). When logistics systems are optimized through successful digital transformation, they can enhance the ability of military and humanitarian organizations to respond swiftly to crises, minimizing human suffering and accelerating recovery. Failure in these projects can mean delayed responses, resource misallocation, and further human hardship. Logistical command and control systems like Log IT must function seamlessly across land, sea, air, space, and cyber domains (Deputy Assistant Secretary of Defense for Logistics, 2024). Successful supply chain

and logistics management in times of war requires resilient systems that provide accurate and timely data (Agrawal et al., 2023). Applying systematic approaches to digital transformation helps military organizations avoid project failures and benefit from operational, tactical, and strategic opportunities for improved outcomes.

4. PDCA Cycle (Plan-Do-Check-Act)

The PDCA or Deming Cycle is a problem-solving framework incorporating continuous improvement for improved quality (American Society for Quality, 2024; International Organization for Standardization, 2015; Parker, 2023). This approach is particularly beneficial to digital transformation projects, where ongoing, iterative evaluation identifies issues that emerge during implementation and ensures adjustments are made to adapt (Parker, 2023). The four stages of PDCA, Plan, Do, Check, and Act, enable government logistics and supply chain IT organizations to adopt a structured approach for implementation project management, ensuring that every step of the transformation process is validated and adjusted when needed (Parker, 2023).

- **Plan**: Determine what needs to be changed and build a plan (Parker, 2023). This may happen in stages for a digital transformation project, where project teams assess the initiative's scope, define objectives, break down the work into manageable pieces, and identify potential risks. For each manageable piece of work, develop a detailed plan.
- **Do**: Implement a change that can be validated (Parker, 2023).
- **Check** and validate the implemented change to ensure the results match the plan's expected results (Parker, 2023).
- **Act**: Based on the evaluation, incorporate lessons learned. When the Check step demonstrates that the change did not work, repeat the process, beginning with a new plan (Parker, 2023).

Corrective actions using PDCA will be made incrementally throughout the project lifecycle rather than all at once at the end of the implementation (Parker, 2023).

5. Shell's Scenario Planning Model

Shell's Scenario Planning Model was created in the 1970s to address unpredictable changes in the oil industry (Norouzi et al., 2020). Moreover, it enabled Shell Oil Company to effectively adapt to changes in the energy market in later decades (Norouzi et al., 2020; Vecchiato, 2019). However, this model has applicability beyond the oil industry and has evolved into a strategic tool for developing stories of the possible future based on analysis of potential driving forces and uncertainties (Amer et al., 2013; Rodney, 2022). The model helps organizations consider possible future outcomes beyond what financial models may predict (Amer et al., 2013; Rodney, 2022). These scenarios can be effectively integrated into the overall project by developing alternative plans to enact should the imagined scenario become a reality (Amer et al., 2013; Rodney, 2022).

5.1. Key Principles

- **Make It Plausible, Not Probable**

This helps create a story where assumptions can be analyzed along with an understanding of what dynamics make it a viable future (Louen et al., 2023).

- **Strike a Balance Between Relevant and Challenging**

While considering unexpected events, describe the potential disruption regarding impacts relevant to leadership (Louen et al., 2023).

- **Tell Stories That Are Memorable Yet Disposable**

The stories created through this process must be sufficiently memorable to

enable effective discussion about the issues identified while not becoming so familiar that they are no longer evolving (Louen et al., 2023).

➢ **Add Numbers to Narrative**

Quantifying the impacts of scenarios guides response planning and can uncover hidden assumptions (Louen et al., 2023).

➢ **Scenarios Open Doors**

By incorporating external stakeholder perspectives in the scenarios, plausible futures can encourage conversation and information exchanges that enhance planning for all participants while building stronger relationships (Louen et al., 2023).

➢ **Manage Disagreement as an Asset**

Scenarios support a focus on strategy and priorities by exploring what might happen to impact them, encouraging discussion and inquiry to reach a shared understanding (Louen et al., 2023).

➢ **Fit into a Broader Strategic Management System**

By exploring what might be possible beyond the current competitive environment and market/industry trends, organizations can examine tradeoffs between what is working well now and what might enable success in plausible futures (Louen et al., 2023).

Utilizing Shell's Scenario Planning Model can help the DoD envision multiple plausible futures and develop strategies to respond to and address potential adversarial actions should one of the possibilities become a reality.

6. Monte Carlo Risk Analysis

Monte Carlo Risk Analysis is an analytical process that uses simulations and probabilities to provide a range for how much a project will cost or the expected completion date, along with the likelihood of values within the range (Wilkinson & Kupers R. 2013; Mulcahy, 2003; Qazi et al., 2023). These simulations can also identify how likely a task will be on the project's critical path (Wilkinson & Kupers, 2013; Mulcahy, 2003; Qazi et al., 2023), which can be used to inform additional risk management planning activities. An additional application of Monte Carlo Risk Analysis is to use simulations to evaluate supply chain resilience given different scenarios by associating risks with performance measures (Wilkinson & Kupers, 2013; Mulcahy, 2003; Qazi et al., 2023; Züst et al., 2021).

6.1. The Process

➢ **Optimistic, Most Likely, and Pessimistic Outcomes**

Assign values to each activity for the best-case (optimistic), most likely, and worst-case (pessimistic) scenario outcomes (Wilkinson & Kupers, 2013; Mulcahy, 2003; Qazi et al., 2023). An alternative approach provides a set of values that can be used to calculate certainty that ranges from almost certain at 0.99 to almost uncertain at 0.01 (Wilkinson & Kupers, 2013; Mulcahy, 2003; Qazi et al., 2023).

➢ **Run the Simulations**

Typically, a software tool conducts a random sampling using one of the assigned scenario outcomes for each task, iterating through the project multiple times (500 or more) to generate a distribution of project outcomes with probabilities (Wilkinson & Kupers, 2013; Mulcahy, 2003; Qazi et al., 2023). This could be done manually but would be time-consuming.

➢ **Review the Probability Distribution**

By reviewing the forecasts based on the simulations, the probabilities of various outcomes can be assessed to determine which warrants additional risk mitigation planning (Wilkinson & Kupers, 2013; Mulcahy, 2003; Qazi et al., 2023).

Monte Carlo Risk Analysis facilitates informed decision-making by modeling probabilities connected to scenarios and outcomes (Wilkinson & Kupers, 2013; Mulcahy, 2003; Qazi et al., 2023). This

analysis enables the DoD to manage risk and further evaluate outcomes from plausible scenarios identified using the Shell Scenario Planning Model.

Given the high failure rates of digital transformation projects and the strategic importance of supply chain management, organizations like the DoD can increase the likelihood of success by integrating these tools into project management processes: the PDCA cycle, Shell's Scenario Planning Model, and Monte Carlo Risk Analysis. These well-researched and time-tested tools support continuous process improvement and effective risk management to help complex projects like the digital transformation of Log IT succeed.

7. Research Design

This study employed a qualitative focus group design to examine best practices in maritime IT logistics and supply chain project risk management within a DoD context. Focus groups were selected as the primary methodology because they enable dynamic, interactive exploration of participant experiences, particularly in high-stakes, technically complex environments like military logistics. The method's suitability is further justified by its capacity to generate collective insight through peer dialogue, surfacing tacit knowledge among subject matter experts. Applying this design to naval logistics officers, the study captured multifaceted perspectives grounded in both operational decision-making and systems-level transformation. The focus group structure thus enhanced the depth and relevance of the data, mirroring stakeholder engagement strategies used by Fortune 500 firms to support innovation and mitigate organizational risk. This approach aligns with the study's objective of deriving real-world, scalable strategies from practitioner expertise.

7.1. Participant Selection

Participants were recruited using snowball sampling initiated through LinkedIn networks, allowing the study to identify individuals with specialized expertise in maritime logistics and IT systems integration. This approach facilitated access to an elite professional population that might otherwise be difficult to reach. Creswell (2013) contends that qualitative research can achieve sufficient depth with approximately 10 participants when studying a relatively homogeneous expert group, a standard this study met by engaging eleven former logistics officers. Inclusion criteria required at least three years of management experience in maritime logistics IT, decision-making authority, and availability for a 90-minute virtual session.

7.2. Data Analysis and Interpretation

Clarification of participant responses was ensured through rigorous analytic procedures. The eleven participants' contributions were not merely interpreted through researcher inference but were systematically coded and thematically analyzed. An embedded iterative process, comprising four phases, facilitated member validation and minimized interpretive bias. In Phase One, participants shared unfiltered experiences concerning challenges, successes, and lessons learned in managing maritime IT logistics risk. In Phase Two, the research team organized these data into preliminary thematic categories, which were then returned to participants in breakout groups for further elaboration and clarification. Phase Three employed the Nominal Group Technique, enabling participants to anonymously rank best practices based on feasibility and strategic impact. In Phase Four, final themes and recommendations were validated through member checking and triangulated with existing literature. This rigorous approach ensured that findings reflected participant

consensus rather than researcher assumptions, thereby enhancing the study's credibility and transferability.

7.3. Aims

This study aimed to identify the best practices for managing maritime IT logistics and supply chain project risk management. The findings are expected to contribute to developing actionable strategies for improving risk management frameworks, enhancing operational efficiency, and ensuring system resilience in national security-focused maritime organizations.

7.4. Brainstorming Exercise and Data Collection Procedures

The brainstorming exercise in this study was designed to systematically elicit, refine, and prioritize expert insights regarding best practices for managing maritime IT logistics and supply chain project risk in a DoD context. The process involved four iterative phases to ensure comprehensive data capture and convergence toward actionable recommendations, enhancing both transparency and replicability.

➢ **Phase 1: Initial Brainstorming and Data Collection**

Participants engaged in a virtual 90-minute focus group session, facilitated via a secure video conferencing platform to ensure confidentiality and accessibility. Data collection was guided by a semi-structured interview protocol consisting of open-ended questions designed to promote broad and deep discussion. The facilitator posed the following core questions to stimulate initial brainstorming:

●**Challenges**

What are the primary obstacles currently faced in managing maritime IT logistics and supply chain risks?

How do these challenges manifest operationally?

●**Strategies**

What practices or strategies have you successfully implemented or observed to mitigate these challenges?

●**Lessons Learned**

Can you share specific lessons learned from past project successes or failures in maritime IT logistics?

What would you do differently in future projects?

●**Future Recommendations**

What recommendations would you make for improving IT project risk management in the context of national security and operational resilience?

Participants were encouraged to contribute freely, build on one another's insights, and introduce new topics not explicitly covered in the protocol. A scribe documented responses in real time to ensure a complete and accurate record of the discussion, fostering transparency in the data collection process.

➢ **Phase 2: Thematic Grouping and Iterative Exploration**

Following Phase 1, the research team conducted an initial thematic analysis of the brainstorming data. Emergent themes included:

- Cybersecurity and system integrity
- Inventory visibility and data optimization
- System interoperability across operational domains
- Integration of emerging technologies such as artificial intelligence (AI)

In Phase 2, these preliminary themes were presented back to participants for validation and deeper exploration. Participants were divided into smaller breakout groups and provided with targeted questions to refine each theme:

1. What are the most critical sub-challenges within your assigned theme?
2. What specific best practices address these challenges effectively?

3. Are there interdependencies or conflicts between your theme and others that should be considered?

Groups then reconvened in plenary to share their elaborations, fostering cross-group dialogue and collaborative refinement of the thematic structure.

➢ **Phase 3: Prioritization and Consensus Building**

In Phase 3, the Nominal Group Technique (NGT) was employed to prioritize proposed best practices systematically. Participants anonymously ranked their top three recommendations for each theme based on criteria including feasibility, strategic impact, and alignment with DoD objectives. The facilitator aggregated the rankings and presented the results, prompting further discussion to reconcile any discrepancies and ensure collective consensus. This structured prioritization enhanced transparency and minimized potential dominance by more vocal individuals.

➢ **Phase 4: Final Recommendations and Validation**

In the final phase, the research team synthesized the prioritized insights into a consolidated list of recommendations. This draft was distributed to all participants for member checking, accompanied by targeted follow-up questions:

- Do these recommendations accurately reflect your perspectives?
- Are there any gaps, ambiguities, or misrepresentations in the synthesized findings?
- Are there recommendations you would modify, remove, or add?

Participant feedback was integrated into the final report, ensuring the recommendations were both accurate and contextually relevant. Triangulation was performed by cross-referencing the final recommendations with existing literature, DoD reports, and organizational best practices, further bolstering the validity of the outcomes.

7.5. Data Saturation and Sample Size Justification

Participants were recruited via snowball sampling initiated through professional networks on LinkedIn. This approach facilitated access to an expert population with specialized knowledge of maritime logistics and IT systems. Creswell (2013) posits that qualitative studies focusing on relatively homogeneous expert groups can achieve analytical depth with approximately 10 participants. Consistent with this guidance, the study engaged eleven former logistics officers who met rigorous inclusion criteria, including a minimum of three years of maritime logistics IT management experience and decision-making authority. Data saturation, which is the point at which no new themes or insights emerge, was systematically monitored throughout the focus group.

7.6. Analytic Rigor and Trustworthiness

Several measures were implemented to uphold analytic rigor and ensure the trustworthiness of the findings:

1. Triangulation: Emergent themes were cross-validated against relevant academic literature and DoD reports to contextualize findings within broader industry standards.
2. Member Checking: Participants reviewed the synthesized findings to verify accuracy and interpretative fidelity.
3. Inter-Coder Reliability: Two independent analysts coded the data. Discrepancies were resolved through consensus discussions, enhancing consistency and reducing interpretive bias.

These methodological safeguards collectively strengthened the credibility, dependability, and confirmability of the study's findings.

7.7. Ethical Considerations and Study Limitations

Ethical protocols were rigorously followed, including informed consent, confidentiality assurances, and secure data storage. Given the sensitive nature of military operations, these measures were essential to promoting candid dialogue and safeguarding participant privacy.

Despite generating robust insights, certain limitations persist. The reliance on a single focus group constrains the generalizability of findings and limits representation from other military branches or allied partners. While thematic saturation was achieved, future research should consider additional focus groups or comparative studies across different service branches to capture a broader spectrum of perspectives. Acknowledging these limitations situates the findings appropriately within the study's defined scope and provides a foundation for future inquiry and methodological replication.

8. Results and Focus Group Final Recommendations

This approach generated rich qualitative data and fostered participant ownership of the results, enhancing the credibility and applicability of the findings. The refined recommendations are expected to contribute significantly to developing resilient risk management frameworks within national security-focused maritime organizations. The developed recommendations are as follows:

1. Organizations must prioritize integrating robust risk management frameworks tailored to the unique complexities of maritime logistics and supply chain IT projects to enhance resilience against potential disruptions.
2. Cybersecurity measures should be a primary focus, ensuring that data integrity and system reliability are maintained in environments susceptible to cyber threats and operational vulnerabilities.
3. Agencies should implement strategies to achieve regulatory compliance and meet audit requirements while simultaneously modernizing systems to align with evolving technological standards.
4. Enhanced inventory visibility and data optimization are essential to improving decision-making capabilities, enabling more effective resource allocation and operational efficiency.
5. To ensure seamless operations, particularly in high-stakes military environments, interoperability and integration of systems across multiple domains, including land, sea, air, space, and cyber, should be emphasized.
6. The application of actionable data analytics should be expanded to uncover untapped strategic, operational, and tactical opportunities, ensuring leadership can make informed decisions.
7. Digital transformation initiatives should be grounded in well-researched problem-solving methodologies that address technological and organizational complexities to mitigate the high failure rates historically associated with such projects.
8. Continuous training and engagement of project stakeholders should be encouraged to align goals and expectations while fostering collaboration across diverse military branches and allied forces.
9. Project planning must account for scenarios involving communication interruptions and operational challenges during warfare, ensuring systems remain functional and reliable under duress.
10. Regular audits and reviews of IT systems should be conducted to monitor progress, assess risk levels, and implement corrective actions promptly to maintain alignment with strategic objectives.
11. Leveraging optimized logistics systems that enable rapid deployment, precise coordination, and effective resource management even in compromised

communication environments should enhance disaster and humanitarian relief capabilities.

12. Advances in artificial intelligence and machine learning should be explored to improve system capabilities, predictive analytics, and operational efficiency in maritime IT logistics.

13. A culture of continuous improvement should be fostered, where lessons learned from previous projects are documented and applied to future initiatives to build institutional knowledge and reduce risk exposure.

14. Strategic partnerships and collaborations with allied nations and private sector technology providers should be developed to share best practices, resources, and innovations in IT logistics management.

9. Conclusion

This study underscores the urgent need for transformative managerial change in the U.S. Department of Defense's maritime logistics and supply chain IT systems, positioning such reform as the cornerstone of modern military readiness. Like overhauling the navigation system of a fleet before setting sail into stormy waters, integrating advanced risk management frameworks, cybersecurity protocols, and interoperability mechanisms across land, sea, air, space, and cyber domains is not optional but essential. Through the voices of former logistics officers, strategic captains who have weathered complex logistical storms, the research reveals the tangled web of coordination challenges and digital vulnerabilities that impede progress. These firsthand insights serve as compass points, guiding attention toward essential best practices, such as embedding regulatory compliance like rivets in a steel hull, improving inventory visibility as one would illuminate a darkened engine room, and integrating scenario planning as a captain would consult tide charts before a high-stakes voyage.

The findings extend beyond academic discourse, offering a lifeline to defense leaders navigating the turbulent waters of digital transformation in high-consequence environments. With over half of such efforts historically running aground, the study presents a beacon of structured, evidence-informed strategies for successful modernization. By treating artificial intelligence not as a mere tool but as an intelligent co-navigator, and by emphasizing the necessity of managerial stakeholder engagement as the rudder that maintains course alignment, the study charts a pragmatic and future-oriented path forward. Institutionalizing proactive risk mitigation becomes akin to reinforcing a vessel's bulkheads before entering combat zones, an act of foresight that may determine mission success or failure. Ultimately, this research delivers a vital managerial and organizational blueprint for constructing resilient, responsive, and technologically agile logistics systems that not only secure national interests but also uphold global stability in an era increasingly defined by cyber-kinetic convergence.

REFERENCES

Agrawal, S., Agrawal, R., Kumar, A., Luthra, S., & Garza-Reyes, J.A. (2023). Can industry 5.0 technologies overcome supply chain disruptions? – A perspective study on pandemics, war, and climate change issues. *Operations Management Research. 17(2),* 453-68. Available at: https://doi.org/10.1007/s12063-023-00410-y.

Amer, M., Daim, T.U., & Jetter, A. (2013). A review of scenario planning. *Futures, 46*, 23-40. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0016328712001978.

American Society for Quality. (2024). *PDCA cycle – What is the plan-do-check-act cycle?* Available at: https://asq.org/quality-resources/pdca-cycle.

Bloch, M., Blumberg, S., & Laartz, J. (2012). *Delivering large-scale IT projects on time, on budget, and value*. Available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/delivering-large-scale-it-projects-on-time-on-budget-and-on-value.

Creswell, J.W. (2013). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches* (3rd ed.). SAGE Publications.

Deputy Assistant Secretary of Defense for Logistics (2024). *Logistics information technology strategy: 2024-2029*. Department of Defense. Available at: https://www.acq.osd.mil/log/LOG_SD/.policy_vault.html/2024_OSD_Logistics_IT_Strategy_020224.pdf.

Detrow, S., & Roughead, G. (2024). The need for AI in the U.S. military. *National Public Radio*. Available at: https://www.npr.org/programs/all-things-considered/2024/09/21/all-things-considered-for-september-21-2024?showDate=2024-09-21.

Hassenstein, M.J., & Vanella, P. (2022). Data Quality – Concepts and Problems. *Encyclopedia,* 2(1), 498-510. Available at: https://doi.org/10.3390/encyclopedia2010032.

International Organization for Standardization. (2015). *INTERNATIONAL STANDARD ISO 9001: Quality management systems – Requirements (ISO 9001)*.

KPMG. (2023). *U.S. technology survey: Key findings*. Available at: https://kpmg.com/kpmg-us/content/dam/kpmg/corporate-communications/pdf/2023/2023-technology-survey-key-findings-final.pdf.

Kraus, S., Jones, P., Kailer, N., Weinmann, A., Chaparro-Banegas, N., & Roig-Tierno, N. (2021). Digital transformation: An overview of the current state of the art of research. *Sage Open, 11(3)*, 21582440211047576.

Lopez, S. (2024). *Logistics information technology strategy*. DLMS Summit; 2024. Available at: https://www.dla.mil/Portals/104/Documents/DLMS/Summit/Day1/03.%20ODASD%20Log%20IT%20Strategy%20(Lopez).pdf.

Louen, C., Höing, N., Böhnen, C., & Kuhnimhof, T. (2023). *Scenario planning as an approach to structure the development of transport planning alternatives*. Case Studies on Transport Policy. 14:101089.

Mahboub, H., & Sadok, H. (2023). Contribution to a better digital transformation implementation: An integrative approach. In *Machine Learning and Artificial Intelligence.* 120-5. IOS Press. Available at: https://doi.org/10.3233/faia230773.

Metz, D. (2024). *OSD IT digital modernization roadmap: FY2026 -2030 [Internet]*. Office of the Secretary of Defense Chief Information Officer. Available at: https://dam.defense.gov/Portals/47/Documents/IMT/OSD%20IT%20Digital%20Modernization%20Roadmap%20FY2026-FY2030.pdf.

Mulcahy, R. (2003). *Risk management: Tricks of the trade for project managers*. Minnetonka, MN: RMC Publications, Inc.

Niyazi, M., & Behnamian, J. (2023). Application of emerging digital technologies in disaster relief operations: a systematic review. *Archives of Computational Methods in Engineering, 30(3)*, 1579-99. Available at: https://doi.org/10.1007/s11831-022-09835-3.

Norouzi, N., Fani, M., & Ziarani, Z.K. (2020). The fall of oil age: A scenario planning approach over the last peak oil of human history by 2040. *Journal of Petroleum Science and Engineering.* 188:106827.

Parker, J. (2023). Cybersecurity breach case study. In *Applied Research Approaches to Technology, Healthcare, and Business,* 89-102. IGI Global.

Qazi, A., Simsekler, M.C., & Formaneck, S. (2023). Supply chain risk network value at risk assessment using Bayesian belief networks and Monte Carlo simulation. *Annals of Operations Research, 322(1)*, 241-72.

Rodney Turner, J. (2022). Using principal – steward contracting and scenario planning to manage megaprojects. *Project Management Journal, 53(1)*, 8-16. Available at: https://doi.org/10.1177/87569728211061836.

U.S. Department of Defense. (2022). *About U.S. Department of Defense*. Available at: https://www.defense.gov/About/.

Van Veldhoven, Z., & Vanthienen, J. (2023). Best practices for digital transformation based on a systematic literature review. *Digital Transformation and Society, 2(2),* 104-28. Available at: https://doi.org/10.1108/DTS-11-2022-0057.

Vecchiato, R. (2019). Scenario planning, cognition, and strategic investment decisions in a turbulent environment. *Long Range Planning, 52(5),* 101865.

Wilkinson, A., & Kupers, R. (2013). Living in the Futures. *Harvard Business Review.* Available at: https://hbr.org/2013/05/living-in-the-futures.

Züst, S., Huonder, M., West, S., & Stoll, O. (2021). Life-cycle oriented risk assessment using a Monte Carlo simulation. *Applied Sciences, 12(1)*, 8.