

Optimizing Naval Logistics and Supply Chain Resilience Through Digital Technologies

Fatima Z. Benali

Department of Defence Logistics and Supply Chain Management, Atlas Institute for Maritime Logistics Research, Casablanca, Morocco

Article History

Received June, 09th, 2024

Accepted June, 10th, 2024

Published June, 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

Naval operations depend on the continuous flow of fuel, munitions, spare parts, food, medical supplies, and personnel across oceans, often far from home bases and under threat. Disruption of these flows can reduce readiness faster than any shortage of ships or weapons. This article examines how digital technologies can optimise naval logistics and strengthen supply chain resilience. It reviews the characteristics of naval logistics, the concepts of resilience and vulnerability, and the contributions of real time visibility, predictive analytics, additive manufacturing, autonomous systems, and digital platforms. It also analyses the risks introduced by digital dependence, including cybersecurity and data integrity concerns, and considers allied interoperability and industrial base issues. Drawing on research in supply chain management, military logistics, and digital transformation, the analysis finds that digital tools can improve visibility, shorten response times, reduce inventory burdens, and enable adaptation to disruption, but that their benefits depend on data quality, secure architectures, skilled people, and organisational change. The article concludes that resilience is best achieved by combining digital capability with redundancy, flexibility, and collaboration, and it offers recommendations for naval organisations seeking to modernise sustainment.

Keywords: naval logistics, supply chain resilience, digital technologies, predictive analytics, additive manufacturing

INTRODUCTION

An old maxim holds that amateurs talk about tactics, while professionals talk about logistics. Naval forces illustrate the point. A modern warship consumes fuel at a prodigious rate, requires thousands of spare parts, carries limited stores of munitions and food, and depends on timely replenishment to remain at sea. Fleets operating in distant waters rely on a

chain of ports, depots, tankers, supply ships, aircraft, and commercial carriers that stretches across continents. Kress describes military logistics as the art and science of sustaining operations, emphasising that the design and management of supply networks are decisive for the ability of forces to act (Kress, 2016). Supply chains face an increasingly turbulent environment. Natural hazards, pandemics, cyber attacks, geopolitical shocks, and adversary action can interrupt flows at many points. Christopher and Peck argued that modern supply chains have become more vulnerable because of globalisation, lean practices, and reliance on single sources, and that resilience, meaning the ability to return to the original or a better state after disruption, must be built into design (Christopher and Peck, 2004). For navies, the stakes are higher still, since disruption may occur in wartime and since the consequences include mission failure. Digital technologies promise to transform logistics. Sensors and tracking provide visibility of assets, analytics forecast demand and failures, additive manufacturing can produce parts near the point of need, autonomous vehicles can move supplies, and digital platforms integrate planning and execution across organisations. Tjahjono and colleagues examined what Industry 4.0 means for supply chains and concluded that digital technologies affect procurement, production, distribution, and customer interaction, with potential gains in efficiency, flexibility, and responsiveness (Tjahjono et al., 2017). This article asks how digital technologies can optimise naval logistics and strengthen resilience, and what risks and conditions apply. It proceeds through nine thematic sections addressing the naval logistics environment, resilience concepts, visibility, predictive analytics, additive manufacturing, autonomous systems and platforms, cybersecurity, allied interoperability, and implementation pathways. A summary and a list of references follow.

Naval Logistics in the Maritime Operating Environment:

Naval logistics shares features with commercial logistics but is shaped by distinctive conditions. First, ships operate at great distances from support, and the oceans offer no roads or fixed supply points. Replenishment at sea allows tankers and supply ships to transfer fuel, stores, and munitions to warships underway, but it requires specialised vessels, favourable weather, and exposure of both ships during the transfer. Second, naval consumption is intense and uneven. Fuel demand depends on speed and operating tempo, and spare parts demand depends on machinery condition and usage. Munitions demand in combat can be sudden and large. Forecasting these needs is difficult, and the penalty for shortages is operational failure. Third, naval platforms are complex and varied, with long service lives. Parts may be obsolete, suppliers may have exited the market, and configuration differences between ships complicate stockholding. Fourth, the threat environment is contested. Adversaries may target logistic ships, ports, and communications, and cyber attacks may disrupt information systems. Fifth, naval logistics depends on both military and commercial assets, including chartered shipping, commercial ports, and civilian contractors. This dependence on civil providers creates efficiencies but also exposure to market conditions and civil sector disruptions. Eccles, in his classic study of logistics in national defence, argued that logistics must be integrated with strategy and operations from the outset, since logistic feasibility defines the range of possible plans (Eccles, 1959). That insight remains valid. The aim of optimisation is not merely cost reduction but the maximisation of operational capability, measured by readiness, endurance, and the ability to sustain the fleet under stress.

Concepts of Supply Chain Resilience and Vulnerability:

Resilience has been defined in several ways. Sheffi and Rice described the resilient enterprise as one that can reduce the probability of disruptions, reduce the time and impact of disruptions when they occur, and recover quickly, and they stressed the roles of flexibility and organisational culture alongside redundancy (Sheffi and Rice, 2005). Pettit, Croxton, and Fiksel reviewed the evolution of resilience in supply chain management and emphasised that resilience involves both the capabilities to anticipate and respond and the vulnerabilities that expose a system to harm (Pettit et al., 2019). mVulnerability in naval supply chains takes several forms. Single points of failure arise when one supplier, port, or transport link provides a critical item. Long lead times and low inventories leave little buffer. Concentration of production in a few locations or countries creates geopolitical exposure. Fragile information systems can disrupt coordination, and dependence on commercial infrastructure may leave gaps in crises. Resilience can be built through several strategies. Redundancy, such as holding strategic stocks or qualifying multiple suppliers, provides buffers. Flexibility, such as the ability to switch routes, sources, or production methods, allows adaptation. Visibility and collaboration, such as shared information with suppliers and partners, improve early warning and coordinated response. Wieland and Wallenburg found that relational competencies, including communication, integration, and collaboration with partners, enhance resilience, which implies that trust and relationships are as important as technology (Wieland and Wallenburg, 2013). A tension exists between efficiency and resilience. Lean systems minimise inventory and cost but are brittle, while redundant systems cost more in peacetime. Military organisations must decide how much insurance to buy against disruption. Digital technologies can reduce this tension by providing information and flexibility that substitute for some physical redundancy, though they cannot remove the need for buffers entirely.

Digital Visibility and Real-Time Tracking:

Visibility, meaning knowledge of where assets are and what condition they are in, is the foundation of effective logistics. Traditionally, naval organisations relied on periodic reports and manual records, which meant that inventories and positions were out of date as soon as they were recorded. Digital technologies provide continuous, accurate, and shared visibility. Radio frequency identification tags, barcodes, and global positioning devices track containers, pallets, and individual items through depots, ports, and vessels. Sensors report the condition of sensitive cargo, such as temperature of medical supplies or shock to delicate equipment. Telemetry from ships reports fuel levels, consumption, and equipment status, allowing logisticians to anticipate needs. Integrated information systems consolidate these data into a common operating picture of the sustainment network. Ivanov, Dolgui, and Sokolov examined the impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics and argued that digital tools enhance visibility, speed up detection of disruption, and support simulation of its propagation, enabling faster and better informed responses (Ivanov et al., 2019). In naval logistics, a disruption at a port or supplier can be traced through the network to identify which ships and operations are affected, and alternative sources and routes can be evaluated. Visibility has limits. Data may be incomplete or inconsistent, particularly across organisations and legacy systems. Tracking at sea depends on communications that may be constrained or denied. Excessive transparency may also reveal sensitive information about operations and capabilities, so access controls and security are essential. Nevertheless, improved visibility generally reduces uncertainty, shortens response times, and enables better allocation of scarce resources.

Predictive Analytics and Demand Forecasting:

With data come opportunities for prediction. Wang and colleagues surveyed the use of big data analytics in logistics and supply chain management and described applications including demand forecasting, inventory optimisation, transport planning, and risk assessment, while noting challenges of data quality, integration, and talent (Wang et al., 2016). In naval logistics, analytics can forecast spare parts demand from equipment condition and usage, predict fuel consumption from operating plans, and estimate the arrival of supplies under uncertain conditions. Predictive maintenance links directly to logistics. When sensors and models forecast component failures, the supply system can position the necessary parts in advance, schedule repairs during planned periods, and avoid emergency shipments. This approach reduces both stockouts and excess inventory. At fleet level, analysis of failure patterns can identify items with chronic reliability problems and guide design changes or procurement decisions. Optimisation models support planning. They can determine the best location of depots and stocks, the optimal routing and scheduling of supply ships, and the allocation of limited capacity among competing demands. Simulation allows planners to test the effect of disruption and to compare mitigation options, such as pre positioning stocks or diversifying sources, before committing resources. Decisions made with analytics still require judgement. Models rely on historical data that may not reflect wartime conditions, and they can fail when circumstances change. Planners need to understand model assumptions, test sensitivity, and maintain the ability to override recommendations. The figure below presents an illustrative comparison of the relative contribution of several digital measures to supply chain resilience, 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

Additive Manufacturing and Distributed Production:

Additive manufacturing, commonly known as three dimensional printing, builds objects layer by layer from digital designs. Attaran reviewed the rise of three dimensional printing and described advantages over traditional manufacturing, including the ability to produce complex geometries, to make small quantities economically, to reduce lead times, and to shift production closer to the point of use, while noting limits on materials, speed, and certification (Attaran, 2017). These characteristics suit naval logistics, where demand for many parts is low and unpredictable and where supply lines are long. Production of spare parts on demand reduces the need to hold large inventories of rarely used items. Digital part libraries, stored securely, replace physical stocks for certain categories of components. Parts that are obsolete or out of production can be reproduced from scans or designs. Tools, fixtures, brackets, covers, and non critical components are the first candidates, and as certification and materials improve, more demanding parts may follow. Placement of printers can vary. Depots and shipyards can serve as production hubs for fleets, while tenders, repair ships, and some larger combatants may carry printers for use at sea. Forward production reduces the time spent waiting for parts and may allow ships to remain on station. Distributed production also enhances resilience, since the loss of a single factory or transport link no longer halts supply of the printed items. Challenges remain. Quality assurance and certification of printed parts for safety critical applications require rigorous testing. Material properties may differ from those of conventionally made parts. Intellectual property and data rights must be negotiated with original manufacturers, and the digital files themselves become targets for theft or manipulation. Training of personnel and maintenance of equipment under shipboard conditions add further requirements. A staged approach that begins with low risk parts and builds experience is therefore sensible.

Autonomous Systems and Digital Platforms in Replenishment:

Autonomous and uncrewed systems are beginning to alter how supplies move. Unmanned aerial vehicles can deliver small, urgent items between ships and shore or between ships, reducing reliance on crewed helicopters for light loads. Uncrewed surface and underwater vehicles may transport cargo or support port operations in the future. Automated guided vehicles and robotic handling in depots and ports improve throughput and reduce manual labour, and automated storage systems increase accuracy and speed. In ports and logistics hubs, automation of cranes, vehicles, and warehouses is already established in commercial settings, and naval organisations can learn from this experience. Autonomous trucks and convoys may reduce the exposure of personnel in hazardous environments. Smart containers with sensors and secure locks add protection and tracking, while robotics supports tasks such as loading, inspection, and maintenance in difficult conditions. Digital platforms tie these elements together. Integrated planning platforms link demand forecasts, inventory data, transport capacity, and maintenance schedules, enabling coordinated decisions across the supply chain. Cloud based systems provide shared access to data for authorised partners, and application interfaces allow different systems to exchange information. Tjahjono and colleagues noted that the integration of systems across the supply chain is central to realising the benefits of digital transformation, since isolated tools yield limited value (Tjahjono et al., 2017). Distributed ledger technologies have been proposed for tracking provenance and ensuring the integrity of records, which may help counter counterfeit parts and support audit trails. Their practical value depends on integration with existing systems and on the cost and complexity of implementation. As with other digital tools, the choice should be driven by operational needs rather than by novelty. Digital platforms should also be designed to degrade gracefully, so that logisticians can continue to operate with reduced connectivity or manual methods.

Cybersecurity and Data Integrity in Digital Supply Chains:

Digitalisation expands the attack surface of logistic systems. Adversaries may seek to disrupt supply by attacking transport management systems, port operations, or supplier networks, to steal sensitive data on stocks, schedules, and capabilities, or to corrupt data so that planners make poor decisions. Because supply chains involve many organisations, a weakness at a small supplier or service provider can provide a path into larger systems. Svilicic and colleagues demonstrated in an experimental ship assessment that maritime systems can have vulnerabilities such as weak authentication and insufficient network segregation, which illustrates the kinds of weaknesses that may exist in connected logistic equipment and shipboard support systems (Svilicic et al., 2019). Manipulated inventory records or falsified condition data could cause stockouts or misdirected shipments, and disruption of communications could prevent coordination. Data integrity is as important as confidentiality. Logistic decisions depend on accurate information, and tampering that is subtle may be more damaging than obvious outages. Controls include strong authentication, encryption, network segmentation, continuous monitoring, and integrity checks on critical data and software. Secure design of platforms and rigorous vetting of suppliers reduce exposure. Recovery plans, regular backups, and the ability to revert to manual procedures ensure continuity when systems are compromised. Resilience therefore calls for a combined approach. Ivanov and colleagues emphasised that digital technologies can enhance supply chain risk analytics but that they also introduce new dependencies, which implies that organisations must treat cyber risk as a component of supply chain risk (Ivanov et al., 2019). Exercises that simulate cyber disruption of logistics, and that test fallback arrangements, should be part of routine preparation.

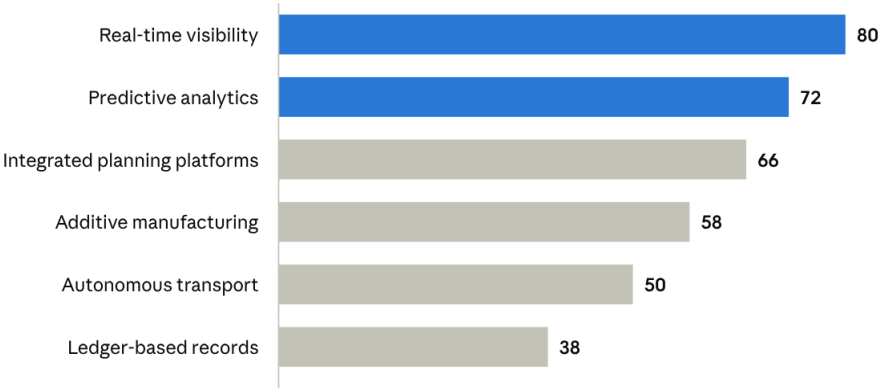
Allied Interoperability and Industrial Base Considerations:

Naval operations are often multinational, and logistics is an area in which allies can both support and constrain each other. Shared ports, common fuel standards, cross servicing agreements, and the ability to exchange stores and parts increase flexibility. Interoperability of information systems and data standards enables allies to see each other's needs and capacities, coordinate transport, and pool resources. Digital technologies can facilitate this cooperation, but they also require agreement on standards, security, and data sharing rules. Differences in national systems, classification regimes, and technical approaches can hinder integration. Joint exercises, common data models, and shared platforms help to build trust and capability. Ivanov and Dolgui argued that supply networks should be considered as intertwined systems whose survivability depends on the interaction of many actors, which supports a collaborative view of resilience among allied partners (Ivanov and Dolgui, 2020). The industrial base is a further consideration. Navies depend on shipyards, component manufacturers, and technology firms whose capacity, geographic concentration, and financial health affect sustainment. Digital tools can improve visibility of supplier networks, identify dependencies on critical materials and single sources, and monitor risk indicators. Governments can use this insight to diversify suppliers, maintain strategic reserves, and support domestic or allied production capabilities for essential items. Procurement practices influence resilience. Contracts that secure data rights, allow for design flexibility, and require cybersecurity and open interfaces enable more adaptive logistics. Performance based arrangements can align incentives for availability but must preserve the ability to switch suppliers and to support operations in contested conditions. Cooperation with commercial shipping and logistics firms also requires clear arrangements for crisis use and protection.

Implementation Pathways and Future Directions:

Implementing digital logistics is a long and complex undertaking. Several principles can guide the effort. First, organisations should begin with operational problems, such as stockouts of critical parts or delays in replenishment, rather than with technology. Second, they should invest in data foundations, including common standards, clean master data, and reliable collection, because analytics are only as good as the data they use. Third, they should pursue incremental delivery with pilot projects, learning from experience before scaling. Fourth, they should integrate technology with people and processes. Logisticians need training to use analytics and digital tools, and organisational procedures should be adapted so that insights lead to action. Culture matters, since a willingness to share data and to trust partners is essential. Wieland and Wallenburg's finding that relational competencies enhance resilience supports attention to collaboration alongside technology (Wieland and Wallenburg, 2013). Fifth, they should embed security and resilience from the start, including fallback procedures and redundancy for critical functions. Sixth, they should measure results using meaningful indicators, such as availability, delivery time, inventory levels, and recovery time after disruption, and use them to refine approaches. Seventh, they should work with industry and allies to align standards, share lessons, and build interoperable capabilities. Future developments will include more advanced artificial intelligence for planning and anomaly detection, greater use of autonomous transport, improved additive manufacturing materials and certification, and richer digital twins of logistics networks that simulate disruption and recovery. At the same time, adversaries will target digital systems and supply lines. Research should evaluate the measurable returns of digital logistics, examine the trade-offs between efficiency and resilience, and develop methods for sustaining operations in degraded digital environments. The enduring lesson, consistent with Kress's account of military logistics, is that sustainment must be designed as an integral part of operations rather than as an afterthought (Kress, 2016).

Visibility and analytics contribute most to supply chain resilience
Illustrative contribution index by digital measure, 0 to 100



Summary:

This article has examined how digital technologies can optimise naval logistics and strengthen supply chain resilience. Naval sustainment is shaped by distance, intense and uncertain consumption, complex platforms, contested conditions, and reliance on both military and civil assets. Resilience requires the ability to anticipate, absorb, and recover from disruption, through redundancy, flexibility, visibility, and collaboration. Digital technologies contribute by providing real time visibility, predictive analytics, additive manufacturing for distributed production, autonomous systems and integrated platforms for movement and planning. They also introduce risks, including cyber vulnerability and data integrity threats, which must be managed through secure design and fallback procedures. Allied interoperability and industrial base considerations further shape outcomes. Naval organisations that combine digital capability with strong data foundations, trained personnel, secure architectures, and collaborative relationships are best placed to sustain operations under stress.

References:

Attaran, M. (2017). The rise of 3-D printing: The advantages of additive manufacturing over traditional manufacturing. *Business Horizons*, 60(5), 677–688.

Christopher, M., and Peck, H. (2004). Building the resilient supply chain. *International Journal of Logistics Management*, 15(2), 1–14.

Eccles, H. E. (1959). *Logistics in the National Defense*. Harrisburg: Stackpole Company.

- Ivanov, D., and Dolgui, A. (2020). Viability of intertwined supply networks: Extending the supply chain resilience angles towards survivability. *International Journal of Production Research*, 58(10), 2904–2915.
- Ivanov, D., Dolgui, A., and Sokolov, B. (2019). The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. *International Journal of Production Research*, 57(3), 829–846.
- Kress, M. (2016). *Operational Logistics: The Art and Science of Sustaining Military Operations* (2nd ed.). Cham: Springer.
- Pettit, T. J., Croxton, K. L., and Fiksel, J. (2019). The evolution of resilience in supply chain management: A retrospective on ensuring supply chain resilience. *Journal of Business Logistics*, 40(1), 56–65.
- Sheffi, Y., and Rice, J. B. (2005). A supply chain view of the resilient enterprise. *MIT Sloan Management Review*, 47(1), 41–48.
- 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.
- Tjahjono, B., Esplugues, C., Ares, E., and Pelaez, G. (2017). What does Industry 4.0 mean to supply chain? *Procedia Manufacturing*, 13, 1175–1182.
- Wang, G., Gunasekaran, A., Ngai, E. W. T., and Papadopoulos, T. (2016). Big data analytics in logistics and supply chain management: Certain investigations for research and applications. *International Journal of Production Economics*, 176, 98–110.
- Wieland, A., and Wallenburg, C. M. (2013). The influence of relational competencies on supply chain resilience: A relational view. *International Journal of Physical Distribution and Logistics Management*, 43(4), 300–320.