

Revista Sextante

ISSN : 2665-3923

Vol: 34 No: 01 (2026)

The Role of Emerging Technologies in Transforming Military Logistics and Support Systems

Keiko Ndlovu-Fernandez

Institute for Defense Logistics and Supply Chain Innovation Pacific Rim Institute of Technology, Singapore

Article History

Received June, 12th , 2026

Accepted June, 13th , 2026

Published June, 14th, 2026



© 2026 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

Military logistics and support systems determine how quickly forces can deploy, how long they can sustain operations, and how effectively they can recover and reconstitute. Emerging technologies, including artificial intelligence, the Internet of Things, additive manufacturing, autonomous vehicles and drones, blockchain, digital twins, and robotics, are reshaping these functions by improving visibility, forecasting, responsiveness, and resilience. This article presents an integrative conceptual review of how these technologies are transforming military logistics and support. It examines conceptual foundations, forecasting, asset visibility, distributed manufacturing, autonomous sustainment, data integrity, contested logistics, workforce and doctrine, and interoperability and policy. A conceptual graph compares the expected logistics impact of each technology with the maturity of its military adoption, indicating that forecasting, visibility, and additive manufacturing offer large benefits while autonomy, digital twins, and blockchain lag in readiness. The article concludes that technological promise will be realized only if forces pair innovation with robust data, secure networks, adapted doctrine, trained personnel, and resilient architectures designed for contested environments.

Keywords: military logistics, emerging technologies, supply chain resilience, additive manufacturing, autonomous sustainment

INTRODUCTION

Logistics has long been described as the foundation of military power. Campaigns are enabled or constrained by the ability to move people, equipment, fuel, ammunition, food, and medical supplies to where they are needed and to maintain equipment in fighting condition. Classical works on military logistics stress that sustainment shapes strategy as much as tactics do (Kress, 2002). Joint doctrine likewise treats logistics as an integrated enterprise spanning supply, maintenance, transportation, distribution, and health services, all of which must function together across strategic,

operational, and tactical levels (Joint Chiefs of Staff, 2019). The strategic environment is changing the demands placed on this enterprise. Forces are expected to operate over greater distances, in dispersed formations, and in environments where adversaries can threaten ports, airfields, roads, networks, and supply lines. Traditional logistics models built on large stockpiles, predictable routes, and centralized planning are increasingly vulnerable. At the same time, a wave of digital and physical technologies, often discussed under the heading of Industry 4.0, is transforming commercial supply chains (Barreto, Amaral, & Pereira, 2017; Ivanov, Dolgui, & Sokolov, 2019). These technologies promise real-time visibility, accurate prediction, local production, and automated movement of goods. Translating commercial advances into military practice is not straightforward. Defense logistics must function in austere and contested conditions, handle classified and mission-critical items, and integrate with legacy systems across services and allied nations. Failure carries consequences measured not only in cost but also in lives and mission outcomes. Moreover, the same connectivity and automation that deliver efficiency can introduce new vulnerabilities to cyber attack and electronic warfare. The adoption of emerging technologies must therefore be guided by a clear understanding of both opportunities and risks. This article offers a structured examination of the role of emerging technologies in transforming military logistics and support systems. Drawing on the supply chain management, operations research, and defense studies literature, it proceeds through thematic sections that address conceptual foundations, forecasting, asset visibility, additive manufacturing, autonomous sustainment, data integrity, contested logistics, workforce and doctrine, and interoperability and policy. A summary then consolidates the principal findings and recommendations for planners, technologists, and policymakers.

Conceptual Foundations of Military Logistics and Support Systems:

Military logistics encompasses the planning and execution of the movement and maintenance of forces, including the acquisition, storage, distribution, maintenance, and disposition of materiel, the transport of personnel, the provision of facilities and services, and medical support. Unlike commercial supply chains, which generally optimize cost and customer service under stable conditions, military systems must optimize effectiveness under uncertainty, adversary action, and rapidly changing demand. Christopher (2016) emphasizes agility and responsiveness as central supply chain capabilities, and these qualities are even more significant when demand is driven by unpredictable operational events. A useful way to think about military logistics is as a layered network of nodes and links. Strategic nodes such as national depots and industrial bases connect through strategic lift to theater nodes such as ports and staging areas, which in turn connect through operational distribution to forward units. Each layer has its own constraints and vulnerabilities, and delays or losses at one point propagate through the network. This ripple effect, studied extensively in supply chain research (Ivanov, Dolgui, & Sokolov, 2019), explains why visibility, flexibility, and redundancy are valued attributes and why emerging technologies that improve them attract attention. Support systems extend beyond materiel flow. They include equipment maintenance, base operating support, energy supply, medical evacuation, and the information systems that coordinate all of these activities. Transformation of logistics therefore cannot be limited to a single technology or function; it requires attention to the whole sustainment architecture. The concept of sustainment as a system of systems, whose performance depends on the interaction among people, processes, infrastructure, and technology, provides the conceptual frame for the technology discussions that follow.

Artificial Intelligence and Demand Forecasting:

Artificial intelligence is among the most promising technologies for logistics because so many logistics decisions depend on prediction. Machine learning models can forecast demand for spare parts, fuel, and consumables by learning from historical consumption, operating tempo, equipment condition, and environmental factors. Compared with traditional statistical methods that assume stable averages, these models can capture nonlinear patterns and respond to changing conditions. Baryannis and colleagues (2019) survey applications of artificial intelligence to supply chain risk management, showing its potential for early detection of disruption and for improved decision making under uncertainty. Beyond forecasting, artificial intelligence supports optimization of routes, loads, schedules, and inventory positioning. Algorithms can evaluate large numbers of alternatives and recommend plans that balance speed, cost, and risk, and they can re-plan rapidly when conditions change. In a military context this might involve adjusting convoy routes in response to threats, reallocating scarce transport capacity among competing priorities, or recommending the pre-positioning of stocks ahead of anticipated operations. Natural language tools may also help staff process large volumes of reports, requisitions, and technical documentation. Challenges are considerable. Military demand data may be sparse, since operations are infrequent and unique, and historical data may not represent future conflict conditions. Models may fail unpredictably when circumstances differ from training data, and adversaries may deliberately manipulate inputs. Decision makers need to understand the confidence and rationale behind recommendations in order to rely on them appropriately. Artificial intelligence should therefore be treated as decision support rather than decision replacement, with human oversight, rigorous testing, and fallback procedures when systems are degraded or unavailable.

Internet of Things and Real-Time Asset Visibility:

The Internet of Things refers to networks of sensors, tags, and devices that collect and exchange data about physical objects and their surroundings. In logistics, technologies such as radio frequency identification, satellite and cellular tracking, and condition sensors provide continuous information on the location, status, and condition of containers, vehicles, equipment, and supplies. Ben-Daya, Hassini, and Bahroun (2019) review how these technologies improve visibility, traceability, and coordination across supply chains. For military forces, the long-standing problem of not knowing what is where, often described as lost visibility in transit, is directly addressed by such tools. Asset visibility yields several benefits. It reduces duplication and shortage by allowing planners to find and redirect existing stocks, shortens the time needed to locate critical items, and supports accurate accounting. Condition sensing on cargo, such as temperature monitoring for medical supplies and munitions, helps protect quality and safety. Combined with predictive analytics, visibility data feed forecasting and maintenance planning, creating a more integrated picture of sustainment. A common operational picture of logistics, shared with commanders, allows support considerations to be integrated into operational planning in a timely way. Implementation problems include connectivity, power, and security. Austere and contested environments may lack the networks needed to transmit tracking data, and emissions from tags and devices may reveal the location and movement of forces to adversaries. Cost and standardization also matter, since inconsistent tags and data formats across services and nations impede integration. Designers must therefore consider low-signature approaches, store-and-forward architectures, and secure protocols, accepting that visibility must be balanced against operational security and that some information may be deliberately withheld or delayed.

Additive Manufacturing and Distributed Spare Parts Production:

Additive manufacturing, commonly known as three-dimensional printing, builds objects layer by layer from digital designs. For logistics, its appeal lies in the potential to produce certain parts on demand near the point of need, reducing dependence on long supply lines and extensive inventories. Khajavi, Partanen, and Holmstrom (2014) analyze the spare parts supply chain and show that additive manufacturing can reduce inventory and lead times for low-volume, high-value, or obsolete parts, which closely resembles the profile of many defense spares. Ageing equipment for which original suppliers no longer exist is an especially attractive application. Military applications range from fabrication of non-critical components and tools in forward locations to repair and production of more demanding metallic parts in depots and on ships. Digital part libraries allow designs to be stored securely and transmitted to any qualified printer, turning inventory into data. This approach could shift logistics from moving objects to moving information, with major implications for the footprint and vulnerability of supply chains. It also supports adaptation, since designs can be modified rapidly to address emergent needs, such as protective equipment or modifications to field equipment. Barriers include qualification and certification, since a printed part must meet the same safety and performance standards as a conventionally made one; control of intellectual property and technical data; availability of materials and power; and training of personnel. Quality can vary with machine, material, and process, so assurance methods are needed. Cybersecurity of design files is also critical, as tampering could introduce defects. A realistic approach therefore begins with lower-risk parts, builds qualification evidence progressively, and develops standards and governance before extending to critical components.

Autonomous Vehicles, Drones, and Robotics in Sustainment:

Autonomous and uncrewed vehicles offer ways to move supplies with reduced risk and workforce requirements. Ground vehicles in convoy configurations, aerial drones for last-mile delivery and resupply, and uncrewed surface and underwater vessels for maritime transport are being explored. These systems are particularly attractive for dangerous routes, contaminated environments, and dispersed units that are difficult to reach by conventional means. By removing human drivers and pilots from exposure to threats, they can also reduce casualties and allow personnel to be assigned to other tasks. Robotics and automation are also changing warehousing and depot operations. Automated storage and retrieval systems, robotic pickers, and autonomous guided vehicles are increasingly common in commercial distribution centers and could improve the speed and accuracy of military depots (Barreto, Amaral, & Pereira, 2017). In maintenance facilities, robots may assist with inspection, handling of hazardous materials, and repetitive tasks. Exoskeletons and robotic assistants may reduce physical strain on logisticians who move heavy loads, supporting endurance and reducing injury. Limitations include payload and range, since many drones can carry only small loads over limited distances; vulnerability to weather, jamming, and attack; and the difficulty of operating autonomously in complex environments with civilians and obstacles. Regulation, safety certification, and rules for operating in shared airspace and roadways add further complexity. Human oversight remains necessary, and designs that combine uncrewed and crewed assets, with humans supervising several machines, are more likely to be effective in the near term than fully autonomous networks.

Blockchain, Digital Twins, and Data Integrity:

Blockchain and related distributed ledger technologies provide shared, tamper-evident records of transactions. In supply chains they have been proposed to improve traceability, authenticity, and trust among parties that do not fully trust one

another. Min (2019) discusses how blockchain can enhance supply chain resilience through transparency and secure information sharing, and Saberi and colleagues (2019) explore its relationship to supply chain management more broadly. For defense, potential uses include tracking the provenance of parts to counter counterfeits, recording maintenance and custody histories, and securing contracts and transactions. Counterfeit and substandard parts are a recognized risk in defense supply chains, and a trusted record of origin and handling could help detect them. Similarly, secure records of configuration and maintenance could support audit and airworthiness assurance. However, blockchain is not a universal remedy. It does not guarantee that the data entered are accurate, it can be slow and energy intensive, and many applications can be served by conventional secure databases. Adoption should therefore be based on a clear problem that distributed trust genuinely addresses, rather than on technological enthusiasm. Digital twins and simulation complement these tools by creating virtual representations of supply networks, facilities, and equipment. Planners can use them to test the effects of disruption, alternative basing, or changes in demand before committing resources. Combined with live data, they can support continuous assessment of sustainment risk. Realizing this potential requires reliable data, validated models, and integration with planning tools, and it raises the same questions of security and trust that apply to all connected systems. Data integrity, in the sense of accuracy, completeness, and protection from manipulation, is the common foundation for each of these technologies.

Resilience and Contested Logistics:

Contested logistics refers to the condition in which adversaries can attack or disrupt sustainment throughout the depth of operations, including in the homeland, at ports and airfields, in transit, and at forward locations. Chopra and Sodhi (2004) argue that supply chain risk should be managed through deliberate strategies such as redundancy, flexibility, and attention to both disruption and operational risks. In the military setting these ideas translate into dispersed stocks, multiple routes and modes, local sourcing, and the ability to continue operating when networks are degraded. Emerging technologies can both strengthen and weaken resilience. Distributed manufacturing, autonomous delivery, and predictive analytics can reduce dependence on vulnerable nodes and enable rapid adaptation. Conversely, heavy reliance on networked systems creates single points of failure, and cyber attack or electronic warfare could disable the very tools that forces depend on for planning and movement. Resilient design therefore requires graceful degradation, with systems able to function in reduced modes and with manual or alternative procedures available, as well as security measures that assume that parts of the network will be compromised. Signature management is another consideration. Large logistics footprints and predictable supply patterns reveal intentions and are easy to target, whereas smaller, dispersed, and more irregular flows are harder to detect and attack. Technologies that reduce the volume that must be moved, such as local production, improved energy efficiency, and more accurate demand forecasting, contribute to a smaller signature. Exercises and wargames that realistically represent logistics attacks are essential for revealing weaknesses and testing the performance of new technologies under stress.

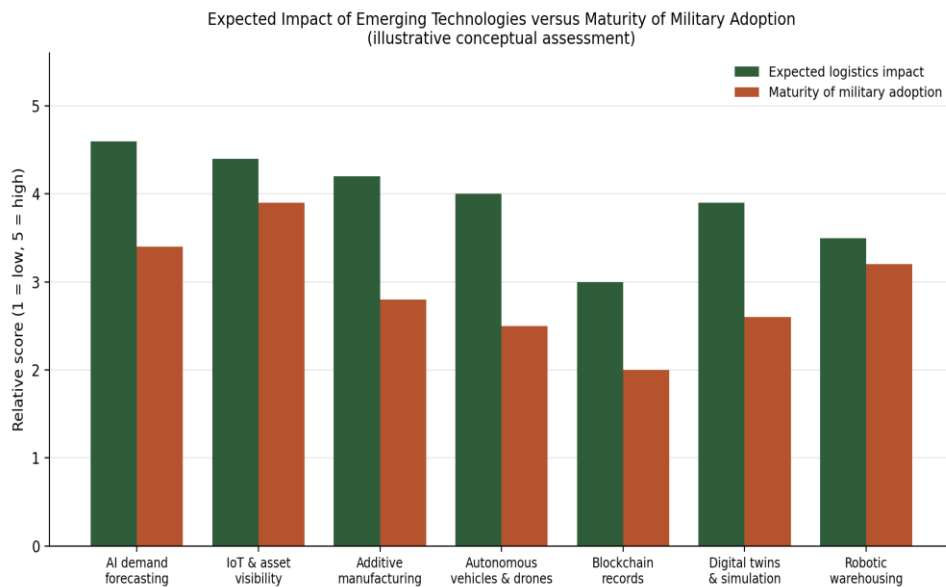
Workforce, Doctrine, and Organizational Adaptation:

People remain central to logistics performance, and the introduction of advanced technology changes the skills required. Logisticians must be able to interpret analytic outputs, manage digital systems, and understand data quality, while retaining the ability to improvise when technology fails. New roles are emerging, including data analysts, additive manufacturing technicians, and operators of uncrewed systems. Education and training need to evolve accordingly, integrating technical literacy into professional military education and offering career paths that attract and retain technically skilled personnel. Doctrine and organization must also adapt. Concepts of operations should describe how technologies are integrated into planning and execution, how authority is delegated to automated systems, and how responsibilities are shared among logistics, operations, and technical communities. Traditional boundaries between maintenance, supply, and transportation may become less meaningful as integrated data and analytics allow end-to-end management. Organizations that cling to stovepiped processes will struggle to capture the benefits of technologies that depend on cross-functional information sharing. Cultural factors can accelerate or impede change. Logistics organizations are often risk averse for good reason, since failure has serious consequences, yet excessive caution can delay beneficial adoption. Experimentation in exercises and low-risk settings, with structured feedback from users, helps build confidence and refine tools. Leadership commitment, clear metrics, and incentives aligned with readiness and sustainment outcomes encourage adoption. Involving logisticians early in design ensures that technologies address real needs and fit the realities of operations, rather than imposing solutions developed without understanding of the working environment.

Interoperability, Policy, and Future Research Directions:

Modern operations are generally multinational, so logistics systems must work across national boundaries. Differences in standards, data formats, equipment, and procedures can create friction, and shared use of emerging technologies requires agreement on interoperability, data sharing, and security. Alliances have developed standards for logistics information and interoperability, and extending these to new technologies, such as additive manufacturing and autonomous systems, will be necessary. Common approaches to part qualification, digital design exchange, and secure

data sharing would allow partners to support one another more efficiently. Policy questions accompany these technical issues. Governments must decide how to balance the efficiency of commercial solutions with the need for security and assured access in crisis, how to manage dependence on commercial suppliers and cloud services, and how to protect industrial bases and technical data. Procurement approaches need to support rapid adoption and iteration of technology while maintaining accountability and standards. Legal frameworks for the use of autonomous and uncrewed systems in logistics, including liability and safety, require clarification, especially where systems operate near civilians. Future research should address the validation of artificial intelligence in logistics under sparse and shifting data, the resilience of networked logistics under cyber and electronic attack, the qualification of additively manufactured parts, and the integration of autonomous systems with human logistics workforces. Empirical evaluation through exercises and field trials, with transparent metrics, is needed to separate demonstrated benefit from promotional claims. Interdisciplinary collaboration among logisticians, engineers, data scientists, and policymakers will be essential if emerging technologies are to deliver sustainment that is faster, more resilient, and more efficient.



Summary:

Emerging technologies are poised to transform military logistics and support systems by improving prediction, visibility, local production, automated movement, and decision support. The review indicates that artificial intelligence, Internet of Things tracking, and additive manufacturing offer particularly high expected benefit, while autonomous vehicles, digital twins, and blockchain show considerable potential but remain less mature in military practice. The technologies reinforce one another, since visibility data feed forecasting, forecasting guides production and positioning, and secure records and models support planning and assurance. The conceptual graph in this article illustrates the relationship between expected impact and maturity of adoption, and it should be read as an illustrative framework rather than a measurement. Recommendations include prioritizing investments where benefit and feasibility are both high, building secure and resilient data architectures, designing for degraded and contested conditions, developing standards for qualification and interoperability, and investing in people, doctrine, and experimentation. If pursued together, these measures can allow future forces to sustain operations over longer distances and in more demanding environments, while reducing vulnerability and cost.

References:

- Barreto, L., Amaral, A., & Pereira, T. (2017). Industry 4.0 implications in logistics: An overview. *Procedia Manufacturing*, 13, 1245–1252.
- Baryannis, G., Validi, S., Dani, S., & Antoniou, G. (2019). Supply chain risk management and artificial intelligence: State of the art and future research directions. *International Journal of Production Research*, 57(7), 2179–2202.
- Ben-Daya, M., Hassini, E., & Bahrour, Z. (2019). Internet of things and supply chain management: A literature review. *International Journal of Production Research*, 57(15–16), 4719–4742.

- Chopra, S., & Sodhi, M. S. (2004). Managing risk to avoid supply-chain breakdown. *MIT Sloan Management Review*, 46(1), 53–61.
- Christopher, M. (2016). *Logistics and supply chain management* (5th ed.). Pearson.
- Ivanov, D., Dolgui, A., & 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.
- Joint Chiefs of Staff. (2019). *Joint publication 4-0: Joint logistics*. U.S. Department of Defense.
- Khajavi, S. H., Partanen, J., & Holmström, J. (2014). Additive manufacturing in the spare parts supply chain. *Computers in Industry*, 65(1), 50–60.
- Kress, M. (2002). *Operational logistics: The art and science of sustaining military operations*. Kluwer Academic Publishers.
- Lee, J., Bagheri, B., & Kao, H.-A. (2015). A cyber-physical systems architecture for Industry 4.0-based manufacturing systems. *Manufacturing Letters*, 3, 18–23.
- Min, H. (2019). Blockchain technology for enhancing supply chain resilience. *Business Horizons*, 62(1), 35–45.
- Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, 57(7), 2117–2135.