ISSN: 2450-6869
eISSN:2719-6763
No. 22, 2025

DEFENCE SCIENCE REVIEW
http://www.journalssystem.com/pno/

DOI: 10.37055/pno/ 236062

From Frontline to Return Flow: A Systematic Review of Technologies Enabling Reverse Logistics in the Defence Sector

Muhammad Ahsan Javed[1,A-F]
ORCID 0000-0003-0119-9528

A - Research concept and design, B - Collection and/or assembly of data, C - Data analysis and interpretation, D - Writing the article, E - Critical revision of the article, F - Final approval of the article

[1]Foreign Trade, Istanbul Ticaret University, Turkey

Original article

Received: 2026-06-08

Revised: 2026-08-07

Final review: 2026-08-28

Accepted: 2026-09-06

Peer review: Double blind

Keywords: reverse logistics, military supply chain, defence logistics, PRISMA review, Industry 4.0 technologies.

Abstract

Objectives: To systematically review academic and institutional literature on technologies enabling Defence Reverse Logistics (DRL), examining which technology domains are active in DRL, what evidence supports their effectiveness, what limitations exist, and how these technologies interact within an integrated capability framework.

Results: Of 1,847 identified records, 68 sources met the inclusion criteria. Seven technology domains were identified: RFID/AIT, Blockchain/DLT, AI/ML, IoMT, Additive Manufacturing, Digital Twins, and Cloud/ERP. RFID and Cloud/ERP showed the highest maturity. AM had growing empirical support, while AI/ML evidence remained mainly conceptual and institutional. Six common barriers were identified: security classification, legacy infrastructure, workforce capability, certification, budget cycles, and coalition interoperability.

Conclusions: No single technology fully addresses DRL modernisation needs. Integrating technologies through the layered TEDRL framework may provide broader capabilities, although this proposition requires empirical validation. Full integration remains uncommon. TEDRL therefore provides a conceptual map for strategic DRL management and future empirical testing.

Corresponding author Muhammad Ahsan Javed Foreign Trade, Istanbul Ticaret University, Istanbul, Turkey; email: u23dbus806@istanbulticaret.edu.tr

1. Introduction

The famous quote, usually attributed to Napoleon Bonaparte, that ‘an army marches on its stomach’ is widely used to illustrate the importance of logistics in the defence sector. The logistical capability of a defence force is a major indicator of its operational capability. Considerable research has focused on the forward flow of products from the point of origin to the point of consumption. However, within research on defence supply chains, the reverse flow of products and materiel from the point of consumption to the point of origin has received considerably less attention. This reverse flow is referred to as Reverse Logistics (RL), which involves the backward movement of products or materiel in a supply chain for the purpose of recovery, repair, remanufacturing, or disposal.

Defence Reverse Logistics (DRL) comprises a cluster of activities that differ fundamentally from commercial RL activities in several respects. Moving military equipment from a combat or operational area involves significant risks that commercial logistics does not face. For example, items may be damaged in the battle zone, exposed to extreme weather conditions, or contaminated with hazardous materials. Therefore, weapons, ammunition, and classified military equipment and parts must follow strict security and tracking procedures. Furthermore, DRL does not primarily aim to recover monetary value; rather, it focuses on restoring the combat readiness and operational availability of assets (Walden, 2001).

The DRL also has a substantial impact on the economic dimension. Walden (2001) calculated that approximately twenty percent of all U.S. Army requisitions resulted in serviceable excess items becoming candidates for return to the wholesale system. Walden (2001), citing RAND research, noted that controlled substitution, local fabrication, local purchase, or higher-level assembly substitution fulfilled fifteen percent of all requisitions for dead-lined equipment, thereby highlighting the systemic gaps in the reverse supply pipeline. More recently, condition-based maintenance systems and circular economy elements have been incorporated into defence policy agendas and given high priority, moving DRL from a residual role in logistics to an important strategic area (Vasiliauskas et al., 2024).

The use of technology is becoming an integral part of DRL modernization. In the past ten years, digital technologies have become increasingly widespread across DRL functions, including real-time asset visibility through Radio Frequency Identification, forward repair through Additive Manufacturing, and the shift from reactive maintenance to predictive sustainment through Artificial Intelligence. To date, however, a critical, comprehensive, and evaluative synthesis of this landscape has yet to be provided in the academic literature. Individual technologies are generally studied separately, possible cross-domain integration effects are not sufficiently theorized, and the barriers to adoption receive less attention than benefits.

In summary, the fragmented nature of available literature related to DRL technologies, wherein most studies generally examine a single technology and its associated benefits, constitutes the research problem which the present study aims to address. The objective is to systematically identify, critically evaluate, and logically combine the available evidence on DRL-related technologies, and present an integrated capability framework. This paper tries to fill these gaps by conducting a PRISMA-guided systematic review and aims to answer three main research questions:

- What are the current domains of technology operating in defence reverse logistics?
- What evidence shows that they are effective, and what are their documented limitations?
- How do these technologies interact, and what possible integrated capability framework can be developed?

Moreover, since this study is a systematic review rather than hypothesis-testing primary research, it does not test a causal hypothesis. Instead, the TEDRL framework is advanced as a conceptual proposition for subsequent empirical validation. The introduction section of the paper is followed by the methodology, conceptual framework, seven technology-domain analyses, comparative synthesis including a maturity table, barrier analysis, the proposed TEDRL framework, research agenda, and conclusions.

2. Methodology

2.1 Search Strategy

Following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines, ScienceDirect, Google Scholar, and Emerald Insight were searched for potentially relevant sources. Additional searches were conducted through the Defense Technical Information Center (DTIC), the Naval Postgraduate School (NPS) research repository, the Air Force Institute of Technology (AFIT) repository, and relevant open-access defence and technology sources. The searches were conducted between January and May 2025.

Search strings were created as Boolean combinations of three clusters: (i) reverse logistics concepts: reverse logistics OR retrograde logistics OR closed-loop supply chain OR remanufacturing OR asset recovery OR end-of-life management; (ii) defence context: military OR defence OR defense OR armed forces OR DoD OR NATO logistics; and (iii) technology terms for each of the seven domains (e.g., for AI: artificial intelligence OR machine learning OR predictive maintenance OR predictive analytics). The date range was January 2001 to April 2025, with emphasis on 2015–2025.

2.2 Inclusion and Exclusion Criteria

Articles were included if they: (i) addressed a defence or military application context; (ii) discussed one or more specific technologies in relation to reverse, retrograde, or closed-loop logistics; (iii) were published in a peer-reviewed journal, peer-reviewed conference proceeding, government or institutional report (e.g., DTIC, NPS, AFIT), or official policy document; and (iv) were written in English. Articles were excluded if they addressed only commercial applications with no defence relevance, were vendor promotional materials or trade press without academic citation, were opinion pieces or editorials without empirical or systematic analytical content or were duplicates.

2.3 Screening Process and PRISMA

Figure 1 shows the detailed PRISMA flowchart.

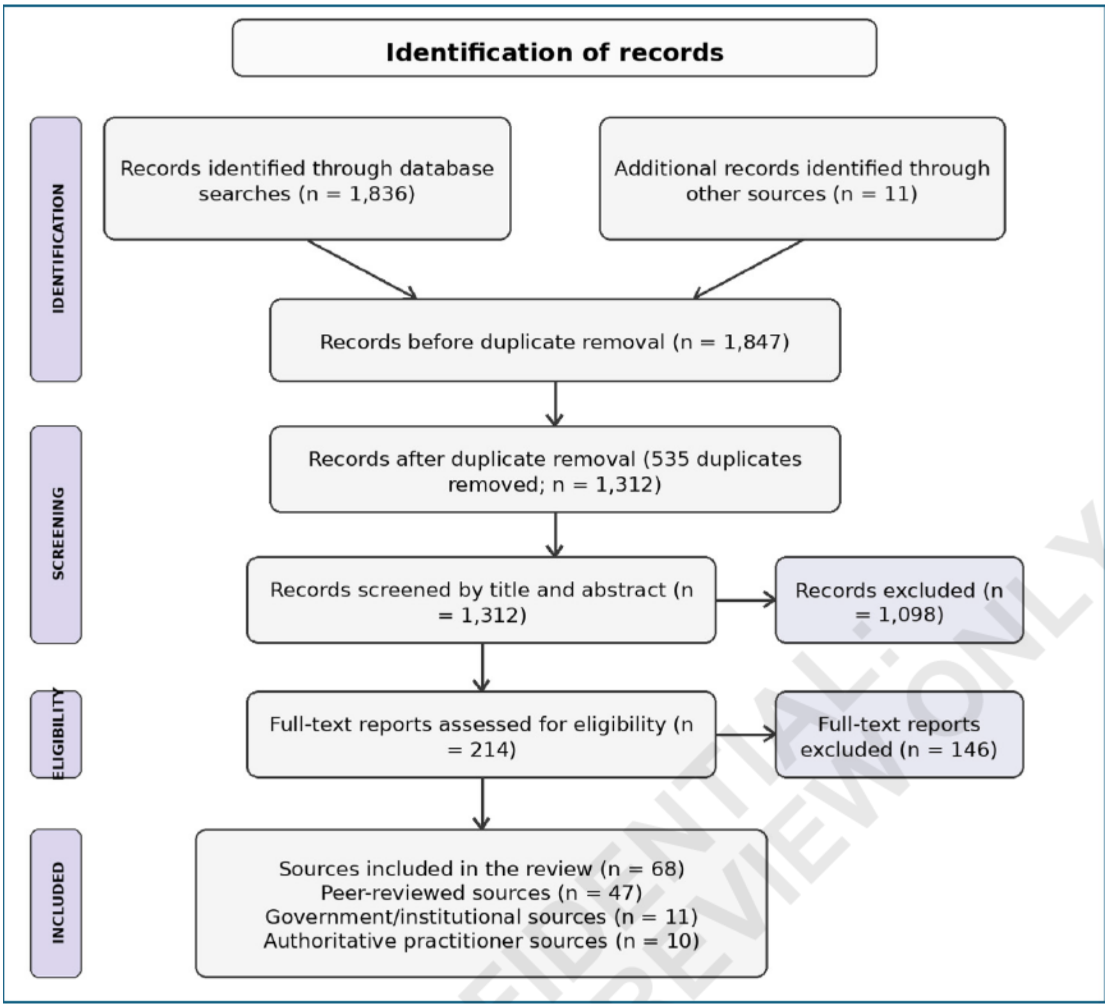

Figure 1. PRISMA Flow Diagram
Source: Author's own work

Initial database searches returned 1,836 records, and 11 additional records were identified through other sources, giving 1,847 records in total. After automated and manual duplicate removal (n = 535),1,312 unique records remained. Title and abstract screening reduced this number to 214 records. The 1,098 records excluded at this stage comprised commercial-only relevance with no defence application (n = 619), no reverse-, retrograde-, or closed-loop-logistics relevance (n = 84), non-English records (n= 83), and editorials or opinion pieces without analytical content (n = 312). Full-text review of 214 records resulted in a final corpus of 68 sources meeting all inclusion criteria. Of the 47 peer-reviewed sources, the majority were published in indexed Q1–Q3 journals; a small number (n = 3) appeared in lower-tier open-access venues, and their findings were treated as supplementary contextual evidence rather than primary claims. No vendor promotional sources were used as primary evidence for analysis.

2.4 Evidence-Source Classification

In order to organize the reviewed literature, the identified sources were grouped into four evidence source-based categories which included: peer-reviewed empirical studies, peer-reviewed conceptual or review studies, governmental or institutional documents, and authoritative practitioner sources (Table 1). It is pertinent to specify that these categories aim to distinguish the origin and research design of the evidence rather than explaining the methodological quality of identified sources. Keeping in view the directions of Durach et al. (2017) related to conduct of systematic review, each source was checked to see how the study was carried out, how clearly its evidence was reported, and how closely it related to defence reverse logistics. Moreover, grey literature **including** vendor websites, trade blogs, and unaffiliated practitioner sources), was used only for contextual triangulation and **not as** primary evidence **of effectiveness**.

Table 1. Evidence-Source Classification of Included Sources

Evidence Level	Description	Sources (n)
Level 1 - Peer-reviewed empirical	Journal articles with primary data (experiments, case studies, surveys)	28
Level 2 - Peer-reviewed conceptual/ review	Systematic reviews, frameworks, theoretical models in peer-reviewed venues	19
Level 3 - Government/ institutional	DTIC reports, NPS theses, DoD policy documents, NATO publications	11
Level 4 - Authoritative practitioner	Official military service publications, National Defense Magazine	10

Source: Author's own work

2.5 Data Extraction and Synthesis

Data were extracted from each included source according to technology domain, publication type, geographic or organisational setting, DRL function, reported outcomes, implementation limitations, and evidence level. Given the variability in study designs and outcome measures across the reviewed studies, statistical meta-analysis was not feasible. Evidence was therefore compared using thematic synthesis and a cross-domain comparison matrix. The TEDRL framework was developed by synthesising recurring technology functions into five roles: perception; trust and record; intelligence; simulation and planning; and execution. These roles were then analysed in terms of their reported functions and process dependencies to identify how they interact and the sequence in which they operate. The framework is therefore an abstraction and synthesis of the reviewed literature rather than an empirical model.

3. Conceptual framework: defence reverse logistics

Rogers and Tibben-Lembke (1999) defined reverse logistics as the process of planning, implementing, and controlling the efficient, cost-effective flow of goods and information from the point of consumption toward the point of origin for value recapture or proper disposal.

For the defence context, three qualifications are important: (i) the 'point of origin' can be thousands of kilometres away and within contested operational environments; (ii) 'value recapture' is not primarily financial recovery but the restoration of combat power; and (iii) 'proper disposal' is subject to arms-control treaties, classification requirements, hazardous-materials legislation, and environmental regulations.

The U.S. Army reverse pipeline has been described by Walden (2001) as having four major flows: lateral transfers between units, turn-ins to the supply system, theatre retrograde shipments, and excess and unserviceable (EUS) disposal. The Defense Logistics Agency coordinates across these flows, operating programmes for recycling, reutilization, and demilitarization. Vasiliauskas et al. (2024), in a peer-reviewed qualitative analysis of Lithuanian Armed Forces reverse logistics, found that military reverse logistics activities exist within closed-loop supply chain frameworks but are not yet systematically integrated with circular-economy objectives. This finding is also consistent with den Boer et al. (2020) in their Journal of Cleaner Production study on additive manufacturing in military and humanitarian supply chains.

4. Technology domain analysis

4.1 Radio Frequency Identification (RFID) and Automatic Identification Technology

4.1.1 Applications and Evidence

RFID uses electromagnetic fields to automatically identify tags on assets, enabling non-contact, nonline- of-sight tracking through the supply chain. In DRL, RFID is applied primarily to asset visibility in the retrograde pipeline, condition-code verification for returned items, and integration with global command-and-control systems. The U.S. Army Combined Arms Support Command (CASCOM, n.d.) and Bailey (2014) documented that RFID delivers fast, accurate, and flexible sustainment by replacing historically limited asset visibility with real-time tracking - addressing what the Army Command and General Staff College identified as the root cause of serviceable-asset loss in the reverse pipeline (Walden, 2001). Peer-reviewed empirical studies by Hellström and Wiberg (2010) and Chen et al. (2013) identified RFID as delivering improved inventory accuracy and reduced manual processing time across warehouse environments, with military applications showing particular gains in high-volume, complex environments (Bailey, 2014; CASCOM, n.d.).

Osman et al. (2024), in their study of RFID in army supply readiness, found that RFID-integrated army depot-management systems have the potential to significantly reduce errors, streamline warehouse processes, and improve supply readiness. Their qualitative analysis identified these as the primary areas of expected benefit, directly supporting DRL performance in asset recovery and reissue, although the study did not provide a controlled evaluation of causal effects.

4.1.2 Critical Evaluation and Limitations

Although RFID is mature, it is known to experience problems in defence deployments. The presence of electromagnetic interference in environments with high metal content, such as armoured vehicles, weapons-storage facilities, and shipboard environments, decreases the reliability of reads which forces the use of active-tag configurations with higher costs and maintenance requirements. The price of tags and reader infrastructure also remains high, especially for large inventories. Security concerns also arise from the transmission of location data for sensitive assets. The three critical success factors for implementing RFID-standardization, system integration, and change management are often underestimated, and this can lead to failure (Attaran, 2012). The Army's Global Combat Support System-Army (GCSS-A) programme, as documented by Walden (2001), illustrates the implementation risks of enterprise-scale RFID and logistics digitalization: the original programme configuration was cancelled in January 2001 due to cost overruns and schedule delays, with the fielding date moved from 1999 to 2004 for a revised iteration.

4.2 Blockchain and Distributed Ledger Technology

4.2.1 Applications and Evidence

Blockchain technology keeps transactions in an unchangeable, cryptographically secure distributed ledger, which keeps a record of transactions in a form designed to resist tampering and does not require a single trusted central authority. DRL is a blockchain-based solution that solves issues with information sharing between actors operating at different classification levels, counterfeit-parts detection, and proof of provenance. The DoD supply chain is one of the world's largest and most complex supply chains, and the need for secure and transparent tracking is a principal reason why blockchain is discussed for military supply chain management (Kostopoulos et al., 2025). The 2018 National Defense Authorization Act directed the Department of Defense to assess blockchain applications across offensive and defensive cyber, logistics, and critical infrastructure, reflecting institutional recognition of the technology's strategic relevance (U.S. Army, 2019).

Kostopoulos et al. (2025) based on a systematic review of 43 peer-reviewed articles, found that military blockchain research covers secure communication, integration with emerging technologies, supply-chain applications, and other defence uses. In DRL, blockchain may strengthen component provenance, maintenance-record integrity, and counterfeit-parts detection, although defence-specific effectiveness evidence remains limited. Mohril et al. (2021) proposed a blockchain-enabled maintenance-management framework for military equipment, in which smart contracts support more secure monitoring and validation with reduced human intervention.

A U.S. government pilot also used blockchain to manage and track inventory assets across a mobile workforce in near real time - a model with direct relevance, providing a potentially relevant model for retrograde asset management (U.S. Army, 2019).

4.2.2 Critical Evaluation and Limitations

While the blockchain literature in defence environments shows a number of advantages, it also identifies a number of tensions. Scalability is one of the core concerns: the trust properties of blockchain depend on consensus mechanisms, which have a computational cost that increases with network sizehus limiting throughput in high-volume logistics operations (Kostopoulos et al., 2025). Interoperability with legacy systems, which are the most widespread information systems in many defence organisations, is technically difficult and expensive. Energy use by proof-of-work consensus mechanisms is a sustainability issue, while proof-of-stake and permissioned-ledger architectures provide partial solutions (Lee & Kim, 2022). The lack of a common classification system among nations in multinational defence supply chains, combined with data-sovereignty requirements, creates jurisdictional challenges that blockchain alone cannot solve. Kostopoulos et al. (2025) point out that data integration for military logistics is extremely complex and time-consuming and that the cost-effectiveness of migration from existing systems has not been proven at scale.

4.3 Artificial Intelligence and Machine Learning

4.3.1 Applications and Evidence

AI and ML use pattern-recognition and optimization algorithms to analyze logistics data and are most widely used in logistics for predictive maintenance - predicting component failures and moving from reactive to proactive maintenance. In their chapter on AI Applications in Military Logistics Operations, published by Springer, de Castro et al. (2024) reported the use of AI in demand forecasting, route optimization, and predictive maintenance in military applications. Shin et al. (2019) pointed out three key AI applications in military logistics: predictive analytics, autonomous decision support, and demand forecasting, of which predictive analytics showed the highest potential for immediate impact. The Predictive Analytics and Decision Assistant (PANDA) is a U.S. Air Force product developed with C3 AI that uses ML to analyse aircraft-maintenance data on AWS GovCloud, predict component failures, and support repair-cycle planning (Amazon Web Services, 2023). Because this evidence is reported through a commercial technology-provider account rather than a controlled effectiveness study, it is treated here as Level 4 practitioner evidence.

de Castro et al. (2024) indicate that AI-based predictive-maintenance solutions in military logistics are helping to reduce unplanned retrogrades and component failures, contributing to both cost savings and improved operational security. Predictive logistics, as described in U.S. Army guidance (2023), applies ML to determine the time and place of need for fuel, ammunition, spare parts, and other materiel in order to pre-position them, thereby reducing forward and reverse pipeline congestion.

4.3.2 Critical Evaluation and Limitations

The academic literature identifies several limitations of AI in military logistics. First, explainability is a major obstacle: Kosasih et al. (2024) identify that many AI solutions in supply chains provide little to no explainability, which is a significant barrier to wider adoption, especially in military scenarios where decisions need to be “auditable and accountable”. Second, data quality and scarcity are inherent limitations: ML models need large, clean, and well-labelled training datasets that are often difficult to access because of classification requirements or differences in data-collection methods across systems (Samuels, 2025). Third, Kumar and Mallipeddi (2022) document cybersecurity threats in AI-powered logistics systems. Fourth, bias, transparency, trust, and legal accountability remain important challenges for the responsible use of AI in military systems (Schraagen, 2023).

These limitations become more serious when AI-enabled logistics is placed within the broader digitalization of military capability. In hybrid and cognitive conflict, maintenance data, training datasets, and model outputs may become targets for manipulation rather than only technical inputs. Data poisoning or model manipulation could quietly distort maintenance priorities and reduce readiness, while limited explainability can increase automation bias in decisions that must remain auditable. Marsili (2023, 2025) places such risks within hybrid conflict and the wider technological transformation of military capability, where military and non-military instruments operate across contested information environments; Johnson (2023) similarly stresses the continued need for human judgement in AI-supported command and control. Within DRL, data poisoning, model manipulation, and automation bias should therefore be treated as technical risks, while cybersecurity, data provenance, model assurance, and accountable human oversight should be regarded as operational requirements.

4.4 Internet of Military Things (IoMT) and Sensor-Based Monitoring

4.4.1 Applications and Evidence

The Internet of Military Things (IoMT) adapts commercial IoT technologies for defence, where sensors are mounted within vehicles, weapon systems, containers, and on individual soldiers to produce continuous condition and location information. In DRL, IoMT is applicable to condition-based maintenance because its sensor streams provide inputs for AI and digital-twin systems, and it offers real-time asset visibility for retrograde management. Kott et al. (2016) describe the Internet of Battle Things as a network of sensors and devices operating in a complex military environment. The DEVCOM Army Research Laboratory's IoBT programme represents institutional investment in networked sensors and other devices for battlefield logistics and sustainment (DEVCOM Army Research Laboratory, n.d.). Priority applications of IoMT include real-time equipment monitoring, supply-chain asset tracking, and vehicle-condition monitoring. The research challenges are those unique to the military, including intermittent connectivity, electromagnetic interference, adversarial jamming, and the need to combine sensor data with secure analytics. These conditions limit the direct transfer of performance claims from ordinary commercial IoT environments.

4.4.2 Critical Evaluation and Limitations

Security challenges are acute in the defence context. Al Kabir et al. (2023) report that the low-power hardware and heterogeneous architecture of IoT devices make them vulnerable and difficult to fix at scale. In a military context, compromised IoT sensors could provide operational information to an adversary, support denial-of-service attacks on logistics-management systems or degrade readiness through the injection of false condition data. Another important aspect is the lack of connectivity: military operations often take place in contested electromagnetic environments or austere theatres where bandwidth is limited or denied, and this is where the IoMT-dependent DRL systems are most required and least reliable. A third challenge is data volume and integration complexity. Many defence organisations still need to build the analytics infrastructure and data-integration pipelines required for effective IoMT deployment, while fragmented vendor standards create further interoperability problems in multinational coalition logistics.

In the digitalization of warfare, the IoMT sensing layer should be considered as a potential target to be attacked. The information for maintenance and retrograde decisions may be impacted by jamming, spoofing and false sensor data. The risk is particularly high because IoMT-based DRL systems can be most critical in an environment of contention in which communications may be the least reliable. Reliable sensors use therefore depends on several important conditions. These include sensor authentication, trustworthy data records, and the ability to operate during weak or interrupted communication (Marsili, 2025).

4.5 Additive Manufacturing

4.5.1 Applications and Evidence

Additive Manufacturing (AM) is a process that allows manufacturing of components from digital files, potentially on-demand spare-parts manufacturing at or near the point of need. The DRL implications are significant: AM can reduce the amount of parts that need to be moved backward for repair, reduce the need to maintain physical inventories of low-volume or obsolete parts in forward positions, and reproduce legacy components that are no longer commercially available. den Boer et al. (2020) conducted a peer-reviewed empirical study in the Journal of Cleaner Production (Level 1 evidence) on AM in military and humanitarian supply chains and reported that AM can influence the responsiveness and sustainability of the armed forces. Based on a systematic literature review, desk research, and semi-structured interviews with stakeholders from the Royal Netherlands Army and partner organisations, they recorded reduced lead times, lower stock requirements, and improved operational readiness, including the ability to print up to 70 different parts on demand.

Colorado et al. (2023) reviewed application of AM in military settings especially related to firearms, armour, ballistic structures, materials, and processing technologies. In 2021, the DoD Additive Manufacturing Strategy formalized AM as a defence capability and identified qualification, digital workflows, cybersecurity, and sustainment as important implementation concerns (U.S. Department of Defense, 2021).

The UK Ministry of Defence has also adopted an advanced-manufacturing strategy aimed at strengthening supply-chain resilience and improving access to obsolete or difficult-to-source components (UK Ministry of Defence, 2025).

4.5.2 Critical Evaluation and Limitations

den Boer et al. (2020) provide the most comprehensive critical analysis and identify three main barriers. First, cost: the purchase price of AM machines is high, and maintenance is more expensive than for traditional equipment. Second, intellectual property and security: digital part files create security and ownership risks, while outsourcing raises concerns in military operations. Third, certification: parts for safety-critical applications must undergo structural testing as conventional parts, which can take a long time, cost a lot and is still being established. In addition, production economics constrain AM when volumes are high, as low-volume production methods are still cheaper, and as den Boer et al. (2020) point out, the DRL advantage of AM is mainly found in low-volume, high-complexity, or obsolete-part applications.

4.6 Digital Twins

4.6.1 Applications and Evidence

Digital twins are dynamic virtual replicas of physical assets connected to their real-world counterparts via sensor-data sharing, which are constantly updated. Digital twins are used in DRL in three ways: asset-condition monitoring for maintenance decisions; fleet-level visibility to forecast maintenance requirements; and lifecycle management from procurement to in-service sustainment and disposal. In a peer-reviewed overview of digital-twin applications in the military domain, Mendi et al. (2022) categorize military digital-twin uses into equipment monitoring, logistics, and battlefield simulation, noting that digital twins can enhance operational preparedness and facilitate lifecycle management and predictive maintenance. Abd Wahab et al. (2024) conducted a systematic review of predictive maintenance and digital-twin technologies across several non-defence sectors. White and Ellington (2022) provided an institutional review of the adoption of digital twins within the Department of the Navy, tracing the concept from its early applications in product lifecycle management to possible future naval applications. Overall, the evidence remains largely institutional and conceptual rather than based on measured DRL performance outcomes.

4.6.2 Critical Evaluation and Limitations

In their systematic review, Abd Wahab et al. (2024) found that one of the drawbacks of these models is that they are based on insufficient theory and sometimes provide inaccurate behavioral predictions. Data quality is key: sensor data and historical records entering a digital twin determine the quality of its outputs, while the heterogeneous legacy systems in many defence organisations contain information that may be inconsistent or decades old. Standardization, interoperability, and cross-domain application remain major challenges as the technology scales from individual assets to multi-system simulations. Cybersecurity of the digital twin itself is also a concern because a twin that accurately mirrors a sensitive military system becomes an intelligence target. Initial investment in sensors, high-performance computing, and secure data networks is substantial, and military implementations remain limited relative to theoretical potential.

4.7 Cloud Computing and Enterprise Resource Planning Systems

4.7.1 Applications and Evidence

Cloud computing and ERP systems provide the information-management backbone integrating data from all other technology domains. ERP systems consolidate inventory management, maintenance records, procurement, transportation, and financial data into a single management platform; cloud deployment provides the scalability, accessibility, and resilience that defence organisations require. The U.S. Army's Logistics Modernization Program (LMP) - the Army Materiel Command's mission-critical-system for parts and equipment readiness - completed migration to the cARMY cloud environment in 2021. This migration was characterized as a transition from industrial age to information-age logistics management, with cloud architecture enabling improved data access across organisational levels (U.S. Army, 2021). Commercial defence ERP platforms also provide compliance, inventory-management, forecasting, and quality-management functions relevant to DRL. In the DRL context, cloud

ERP provides the data-integration layer without which RFID tracking data, IoMT sensor streams, and AI analytics cannot be translated into actionable maintenance and retrograde-management decisions.

4.7.2 Critical Evaluation and Limitations

Defence organizations face a unique set of challenges when implementing cloud ERP. Sensitive logistics data needs to be stored on cloud infrastructure in a classified environment, which complicates access to the cost-efficiencies of commercial cloud architectures and necessitates custom security settings. A constant challenge is legacy-system integration - the LMP migration from on-premises data centres illustrates the diverse legacy environment that most defence ERP modernization initiatives must overcome.

Another major difficulty is cybersecurity risk, especially when a logistics information system becomes a target of an adversary. When multiple countries share coalition logistics support but operate different classification and sovereign systems, ERP is not enough to resolve the resulting data-governance complexity.

5. Comparative synthesis

5.1 Technology Comparison Framework

Table 2 compares the seven technologies against five criteria: Technology Readiness Level (TRL, adapted from the NASA/DoD 1–9 scale), demonstrated DRL impact, primary barriers, evidence strength, and overall adoption readiness for DRL contexts.

Table 2. Technology Comparison Framework

Technology	TRL(Defence)	Primary DRL Impact	Key Barriers	Evidence Strength	Adoption Readiness
RFID/AIT	8-9	Asset visibility; retrograde tracking	EM interference; classification; cost	Strong (L1/L3)	High – most mature
AI/ML	6-7	Predictive maintenance; demand forecasting	Data quality; explainability; cybersecurity	Moderate (L2/L3)	Moderate - growing
Digital Twins	5-7	Condition monitoring; fleet management	Legacy data; standardization; cost	Moderate (L2/L3)	Moderate - early deployment
Additive Mfg.	6-8	On-demand repair; pipeline reduction	Certification; IP; per-unit cost at volume	Strong (L1/L3)	Moderate-High
Blockchain	4-6	Provenance; counterfeit prevention	Scalability; interoperability; governance	Moderate (L1/L2)	Low Moderate
IoMT	5-7	Real-time condition data; visibility	Cybersecurity; connectivity; standards	Moderate (L2/L3)	Moderate - provisional
Cloud/ERP	7-9	Data integration; process automation	Classification; legacy integration	Strong (L3/L4)	High - foundational

Source: Author's own work

Note: The stated TRL ranges are approximate author assessments made by the author based on the reviewed literature evidence and are not official programme ratings. L1–L4 refer to the evidence levels presented in Table 1 and do not represent a universal ranking of methodological quality.

It is evident from the framework (Table 2) that RFID/AIT and Cloud/ERP are comparatively more established and are widely used technologies in DRL since both show strong implementation base and high adoption-readiness. Similarly, AM technology is also progressing gradually, supported by Level 1 empirical evidence despite certification and production-economics barriers. On the other hand, AI/ML is progressing rapidly however, within the defence settings its evidence lies mainly in Level 2 and Level 3 rather than Level 1 controlled evaluation. Presently, blockchain remains in the lower-to-moderate range due to scalability and governance-related hinderances. Digital twins and IoMT fall at the lower end as compared to other technologies. Although their functions are relevant to DRL, however, their defence-specific outcome evidence remains limited at present.

Another notable observation is that the evidence is also uneven across the geographical settings with major portions of documented implementation coming from U.S. programs like GCSS-A, LMP, PANDA, and the Department of Defense additive-manufacturing initiatives. Although some documented evidence exists for European countries, including Lithuanian reverse-logistics practice, Dutch and French AM cases, and the UK advanced-manufacturing programme, this evidence is narrower in scope and technology-specific (den Boer et al., 2020; UK Ministry of Defence, 2025; Vasiliauskas et al., 2024). Globally, defence organisations differ in their acquisition systems, classification rules, available resources, and certification requirements. Therefore, readiness assessments may lack generalisability and may not apply equally to European, resource-constrained, or multinational defence organisations. Furthermore, evidence of technology integration is still limited as far as multinational DRL is concerned. The closest evidence comes from the related digital infrastructure programs such as DARPA's SHARE initiative which successfully demonstrated secure data sharing in real time across different classification levels between the U.S. and its allied forces. This shows that coalition level interoperability can be supported through data-level security and tactical-edge systems (DARPA, 2023). However, this program did not examine the reverse-logistics outcomes. Therefore, the evidence shows that interoperability mechanisms are practically possible but the confirmations regarding the effectiveness of a complete multinational TEDRL framework cannot be established.

5.2 The TEDRL Framework

Based on the comparative analysis and the functional coding described in Section 2.5, this paper presents the Technology-Enabled Defence Reverse Logistics (TEDRL) framework, which is a conceptualization of the seven technology domains as layered capabilities of an integrated digital ecosystem:

- Layer 1 - Perception: RFID/AIT and IoMT sensors deliver real-time asset identification and condition information - the source of the data needed by the other capabilities.

- Layer 2 - Trust and Record: Blockchain and secure Cloud/ERP infrastructure provide trustworthy data storage, transaction records, and information-sharing mechanisms.
- Layer 3 - Intelligence: AI/ML algorithms analyze sensor data and historical information to provide predictive-maintenance insights, demand predictions, and optimization suggestions.
- Layer 4 - Simulation and Planning: Digital Twins can represent assets and fleets dynamically and simulate them before real events occur, allowing proactive maintenance planning and lifecycle management.
- Layer 5 - Execution: Additive Manufacturing enables on-demand production close to the point of-need, thereby potentially reducing the dependence on the extended supply chain routes and the volume of parts moved backward, subject to design approval and certification.

This multi-layer approach is based on the finding that none of the technologies is a complete solution for DRL modernization, but each layer builds on and facilitates the others. The framework helps to explain why partial deployments, which are typical in practice, may provide limited results: Layer 3 (AI) without Layer 1 (sensors) has no suitable real-time data, while Layer 5 (AM) requires validated demand, design, and certification inputs. Individual technologies do not automatically become a systemic capability; they need to be integrated. However, the proposition that a complete five-layer system produces better performance than partial deployment has not yet been empirically tested.

6. Cross-cutting barriers to technology adoption

Six barriers recur across technology domains and are identified as the primary constraints on DRL modernization. First, security-classification constraints affect all seven domains. RFID location data, IoMT sensor streams, blockchain records, AI training data, digital-twin models, and ERP databases all potentially contain operationally sensitive information that must be managed within classified environments, increasing cost and complexity and limiting access to commercial off-the-shelf solutions. Second, legacy-infrastructure fragmentation is documented across RFID (Walden, 2001), digital twins (White & Ellington, 2022), and ERP (U.S. Army, 2021). Most defence organisations operate heterogeneous information environments spanning decades of technological generations, making integration technically challenging and expensive. Third, workforce-capability gaps constrain all technology domains. den Boer et al. (2020) identify AM-specific training needs, Schraagen (2023) discusses human understanding and accountability in military AI, and Mendi et al. (2022) note digital-twin management skill requirements. Defence logistics workforces are not yet broadly equipped with data literacy, AM operations, or AI interpretation skills. Fourth, AM is affected by certification and qualification requirements and, to a lesser degree, AI. Qualifying 3D-printed safety-critical military parts is lengthy, costly, and still developing. Similar explainability requirements apply to AI systems used in safety-critical maintenance decisions (Kosasih et al., 2024). Fifth, the structural tension between the multi-year defence acquisition cycles and the pace of technological change, especially in AI, blockchain, and AM. Total-cost-of-ownership analysis of specific DRL technologies remains underexplored. Lastly, interoperability in coalition environments is more challenging than in ordinary commercial environments. NATO and other coalition logistics arrangements involve countries with different classification systems, ERP platforms, AM certification standards, and data-governance processes, and no single technology can resolve these differences on its own.

Table 3. Mapping of Cross-Cutting Barriers onto the TEDRL Framework

Barrier	Layer 1	Layer 2	Layer 3	Layer 4	Layer 5
Security classification	Direct	Direct	Direct	Direct	Direct
Legacy-infrastructure fragmentation	Indirect	Direct	Direct	Indirect	Not evident
Workforce-capability gaps	Indirect	Indirect	Direct	Direct	Direct
Certification / qualification	Not evident	Not evident	Indirect	Not evident	Direct
Budget-cycle misalignment	Indirect	Indirect	Direct	Direct	Direct
Coalition interoperability	Direct	Direct	Indirect	Indirect	Direct

Source: Author's own work

Note. 'Direct' means that corresponding barrier operates at that TEDRL layer; Indirect' refers to the situation in which the barrier affects the layer through its connection with another layer; 'Not evident' means that there is no clear direct effect identified.

The table depicts that security classification barrier impacts all five layers. Legacy-infrastructure fragmentation impacts Trust and Record (Layer 2), and Intelligence (Layer 3) layers, while Certification is most serious in Execution (Layer 5) layer. Coalition interoperability mainly affects the Perception and Trust and Record layers, but it can also create problems in planning and execution. The analysis therefore shows which barriers matter and where they are most likely to occur in the TEDRL framework.

7. Research agenda

The following directions for future research are identified in this review:

- First, empirical research on the effect of the deployment of DRL technology on specific measures of performance such as retrograde cycle time, serviceable-asset recovery rate, and maintenance cost per equipment hour is required. Existing literature consists mainly of cross-sectional and conceptual studies; before-and-after performance data would strengthen the evidence. When making decisions related to deployment, priority should be given to Layer 1 and Layer 3 wherein sensing and predictive analytics are usually discussed but are rarely linked to measured DRL outcomes.

- Second, there is a need for research on the effects of multi-technology integration. The theoretical synthesis proposed in the present study presents an ideal view of TEDRL; empirical studies should identify exactly which layers are integrated, compare partial and multi-layer configurations, and measure system-level performance. Such studies would directly test and refine the framework.
- Third, the DRL literature and evidence base reviewed in the present study is heavily weighted toward U.S. military experience. Keeping the present study as base, more comparative studies are needed especially focusing on European, Asia-Pacific, and developing-nation defence sectors including multinational military coalition logistics, in order to test the transferability of the proposed framework.
- Fourth, the responsible use of AI in DRL needs dedicated further research. Bias, transparency, explainability, and legal responsibility remain unresolved issues in military AI. These issues are especially critical once AI is used for maintenance decisions that may affect safety (Schraagen, 2023). Thus, future research should focus on Layer 3 and on the quality and security of the data from Layers 1 and 2.
- Fifth, the intersection of DRL and circular-economy policy particularly the integration of military reverse logistics with national circular-economy strategies, as documented by Vasiliauskas et al. (2024) for the European context deserves targeted empirical and policy research. Future research should also strive to analyze the impact of Trust and Record and Execution-layer requirements on reuse, remanufacturing, demilitarization,
and disposal decisions.

8. Conclusions

This paper, by conducting a systematic literature review, examined a total of seven technologies which are actively being used or considered in defence-sector reverse logistics activities. These included RFID/AIT, Blockchain/DLT, AI/ML, IoMT, AM, Digital Twins, and Cloud/ERP. PRISMA-based search and screening protocol identified 68 sources, of which 69.1% were peer-reviewed academic publications, while the remainder consisted of reports from government institutions and authoritative practitioner sources.

The findings show that each of the studied technologies can deliver some degree of support for defence reverse logistics, but there are also limitations and implementation barriers associated with each technology. RFID and Cloud/ERP systems show the most mature-implemented capabilities, while AM is gaining prominence with growing empirical evidence but remains constrained by certification and production economics. AI/ML is also developing rapidly, although its defence evidence remains mainly Level 2 conceptual and Level 3 institutional evidence. Blockchain is still at an early stage of adoption in the defence sector because of governance, interoperability, and scalability challenges. Digital Twins and IoMT stand in the middle, with clear potential but mainly conceptual and institutional evidence rather than strong Level 1 evaluation.

The most significant contribution of this study is the proposed layered TEDRL framework, which organises the technologies as interconnected capabilities rather than considering each technology in isolation. The reviewed evidence suggests that integration may provide broader capabilities, but it does not establish that a complete TEDRL architecture produces superior performance.

This integrated framework is also rarely found in practice. The primary barriers to technology integration include legacy infrastructure, lack of workforce capability, certification requirements, and coalition interoperability. Therefore, defence organisations need to manage their forward and reverse supply chains effectively, and the TEDRL framework can provide a conceptual map to aid this process, rather than an established model or universal prescription.

References

Abd Wahab, N. H., Hasikin, K., Lai, K. W., Xia, K., Bei, L., Huang, K., & Wu, X. (2024). *Systematic review of predictive maintenance and digital twin technologies: Challenges, opportunities, and best practices*. *PeerJ Computer Science, 10*, e1943. https://doi.org/10.7717/peerj-cs.1943

Al Kabir, M. A., Elmedany, W., & Sharif, M. S. (2023). Securing IoT devices against emerging security threats: Challenges and mitigation techniques. Journal of Cyber Security Technology, 7(4), 199-223. https://doi.org/10.1080/23742917.2023.2228053

Attaran, M. (2012). *Critical success factors and challenges of implementing RFID in supply chain management*. *Journal of Supply Chain and Operations Management, 10*(1), 144-167.

Chen, J. C., Cheng, C.-H., Huang, P. B., Wang, K.-J., Huang, C.-J., & Ting, T.-C. (2013). Warehouse management with lean and RFID application: A case study. The International Journal of Advanced Manufacturing Technology, 69, 531-542.https://doi.org/10.1007/s00170-013-5016-8

Colorado, H. A., Cardenas, C. A., Gutierrez-Velazquez, E. I., Escobedo, J. P., & Monteiro, S. N. (2023). Additive manufacturing in armor and military applications: Research, materials, processing technologies, perspectives, and challenges. Journal of Materials Research and Technology, 27, 3900-3913. https://doi.org/10.1016/j.jmrt.2023.11.030

de Castro, B. A., Pochmann, P. G. C., & Neves, E. B. (2024). Artificial intelligence applications in military logistics operations. In Á. Rocha, C. H. Fajardo-Toro, & J. M. R. Rodríguez (Eds.), Developments and advances in defense and security: MICRADS 2023 (pp. 89-100). Springer. https://doi.org/10.1007/978-981-99-8894-5_8

den Boer, J., Lambrechts, W., & Krikke, H. (2020). Additive manufacturing in military and humanitarian missions: Advantages and challenges in the spare parts supply chain. Journal of Cleaner Production, 257, 120301. https://doi.org/10.1016/j.jclepro.2020.120301

Durach, C. F., Kembro, J., & Wieland, A. (2017). A new paradigm for systematic literature reviews in supply chain management. Journal of Supply Chain Management, 53(4), 67-85. https://doi.org/10.1111/jscm.12145

Ekström, T. (2025). Supply chain resilience: An empirical exploration of barriers and enablers in military settings. Scandinavian Journal of Military Studies, 8(1), 119-136. https://doi.org/10.31374/sjms.350

Hellström, D., & Wiberg, M. (2010). Improving inventory accuracy using RFID technology: A case study. Assembly Automation, 30(4), 345-351. https://doi.org/10.1108/01445151011075807

Johnson, J. (2023). Automating the OODA loop in the age of intelligent machines: Reaffirming the role of humans in command-and-control decision-making in the digital age. Defence Studies, 23(1), 43-67. https://doi.org/10.1080/14702436.2022.2102486

Kosasih, E. E., Papadakis, E., Baryannis, G., & Brintrup, A. (2024). A review of explainable artificial intelligence in supply chain management using neurosymbolic approaches. International Journal of Production Research, 62(4), 1510-1540. https://doi.org/10.1080/00207543.2023.2281663

Kostopoulos, N., Stamatiou, Y. C., Halkiopoulos, C., & Antonopoulou, H. (2025). Blockchain applications in the military domain: A systematic review. Technologies, 13(1), 23. https://doi.org/10.3390/technologies13010023

Kott, A., Swami, A., & West, B. J. (2016). The Internet of Battle Things. Computer, 49(12), 70-75. https://doi.org/10.1109/MC.2016.355

Kumar, S. K., & Mallipeddi, R. (2022). Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. Production and Operations Management, 31(12), 4488-4500. https://doi.org/10.1111/poms.13859

Lee, S., & Kim, S. (2022). Blockchain as a cyber defense: Opportunities, applications, and challenges. IEEE Access, 10, 2602-2618. https://doi.org/10.1109/ACCESS.2021.3136328

Marsili, M. (2023). Hybrid warfare: Above or below the threshold of armed conflict? Honvedsegi Szemle - Hungarian Defence Review, 150(Special Issue 1-2), 36-48. https://doi.org/10.5281/zenodo.7557494

Marsili, M. (2025). Dal campo di battaglia al metaverso: La nuova frontiera delle operazioni militari. Libreriauniversitaria.it Edizioni.

Mendi, A. F., Erol, T., & Dogan, D. (2022). Digital twin in the military field. IEEE Internet Computing, 26(5), 33-40. https://doi.org/10.1109/MIC.2021.3055153

Mohril, R. S., Solanki, B. S., Lad, B. K., & Kulkarni, M. S. (2021). Blockchain-enabled maintenance management framework for military equipment. IEEE Transactions on Engineering Management, 69(6), 3938-3951. https://doi.org/10.1109/TEM.2021.3099437

Osman, M. K., Mohamad, E., Husain, R., & Kamarudin, N. (2024). Evaluating the importance of radio frequency identification (RFID) in warehouse operations for army supply readiness. International Journal of Academic Research in Business and Social Sciences, 14(10), 521-538. https://doi.org/10.6007/IJARBSS/v14-i10/23121

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hrobjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71

Rogers, D. S., & Tibben-Lembke, R. S. (1999). Going backwards: Reverse logistics trends and practices. Reverse Logistics Executive Council.

Samuels, A. (2025). Examining the integration of artificial intelligence in supply chain management from Industry 4.0 to 6.0: A systematic literature review. Frontiers in Artificial Intelligence, 7, 1477044. https://doi.org/10.3389/frai.2024.1477044

Schraagen, J. M. (2023). Responsible use of AI in military systems: Prospects and challenges. Ergonomics, 66(11), 1719-1729.

https://doi.org/10.1080/00140139.2023.2278394

Shin, K., Lee, J. K., Kang, K. H., Hong, W., & Han, C. (2019). The current applications and future directions of artificial intelligence for military logistics. Journal of Digital Contents Society, 20(12), 2433-2444. https://doi.org/10.9728/dcs.2019.20.12.2433

Vasiliauskas, A. V., Ivanauskas, S., & Ciziuniene, K. (2024). Challenges of ensuring reverse logistics in a military organization using outsourced services. Sustainability, 16 (11), 4569. https://doi.org/10.3390/su16114569

Other Sources

Amazon Web Services. (2023, December 14). The U.S. Air Force improves aircraft readiness with AI and predictive maintenance solutions. https://aws.amazon.com/blogs/publicsector/the-us-airforce-improves-aircraft-readiness-with-ai-and-predictive-maintenance-solutions/

Bailey, K. (2014, May 14). Real time asset visibility is leading the way for retrograde. U.S.Army. https://www.army.mil/article/125914/real_time_asset_visibility_is_leading_the_way_for_retrograde

DARPA. (2023, June 22). Ensuring reliable communications between U.S., allied partners at the tactical edge. https://www.darpa.mil/news/2023/communications-tactical-edge

DEVCOM Army Research Laboratory. (n.d.). Internet of Battlefield Things (IoBT) Collaborative Research Alliance. https://arl.devcom.army.mil/cras/iobt-cra/

UK Ministry of Defence. (2025). Defence advanced manufacturing strategy. https://www.gov.uk/government/publications/defence-advanced-manufacturing-strategy

U.S. Army Combined Arms Support Command. (n.d.). In-transit visibility. https://cascom.army.mil/G_Staff/cdi/esd/itv/index.htm

U.S. Army. (2019). Blockchain for military logistics.

https://www.army.mil/article/227943/blockchain_for_military_logistics

U.S. Army. (2021). LMP becomes third Army ERP program to migrate to the cloud. https://www.army.mil/article/249516

U.S. Army. (2023). Future of Army logistics: Exploiting AI, overcoming challenges, and chartingthe course ahead. https://www.army.mil/article/267692

U.S. Department of Defense. (2021). Department of Defense additive manufacturing strategy. https://www.cto.mil/wp-content/uploads/2021/01/dod-additive-manufacturing-strategy.pdf