Contested Logistics Impact on Joint Warfighting

Gartner Mission Solutions Perspectives

March 2026

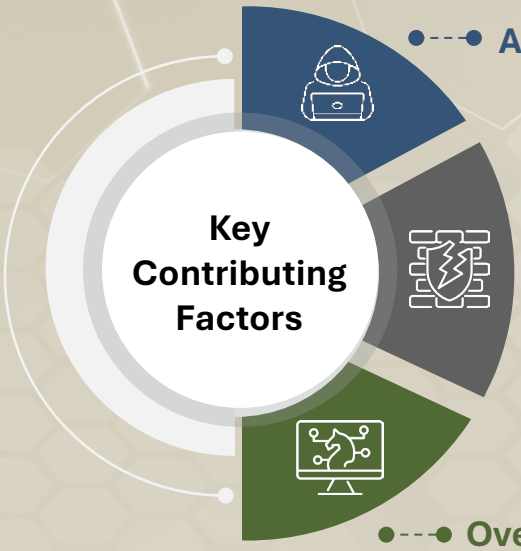
Gartner®

Contested Logistics

Definition

Contested logistics refers to the operational and strategic challenges faced by the Joint Logistics Enterprise (JLEnt), a multi-tiered matrix of global logistics providers (military, defense and supporting industrial base organizations) when adversaries actively seek to disrupt, deny, or degrade logistics operations across all domains — land, air, maritime, space, and cyberspace.

Contested logistics assumes that supply chains are under threat from kinetic, cyber, and informational attacks — from the homeland to the combined or joint operations area — resulting in globally integrated joint warfighting operations that are increasingly demanding logistically. Key Contributing Factors for Exploiting Vulnerabilities, Denial, Disruption, or Degradation of Operations include:



Adversarial Intent

Deliberate and pervasive adversarial actions, undertaken by a diverse array of threat actors, including nation-states, cybercriminals, hacktivists, and malicious insiders. These actions involve concurrent and sometimes coordinated efforts.

Multi-Domain Threats

Vulnerabilities span physical and digital domains often in a blended approach that concurrently utilizes more than one threat vector — such as supply chain, cyber, electromagnetic spectrum, and human elements.

Over-reliance on Fragile Supply Chain Capabilities

Pre-Contested Sources: Dependence on supply chains optimized for uncontested, cost-efficient operations, which can not withstand exposure to today's multi-domain adversarial threats.

Aging technological infrastructures: Burdened by substantial technical debt from legacy systems, processes, etc. that present inherent vulnerabilities and hinder resilient sustainment.

Shifting Global 'Partner' Context: Great power competition, global tensions, and economic warfare negatively impact industrial capacity, and supply chain resilience.

Gartner

Contested Logistics Under Pressure

Time-Critical, Deliberate, and Unified Response Needed

New Trade Policies
Increased the cost of imported goods and disrupted global supply chains will require a focus on agility, compliance, and technology to offset higher operational costs.

Changing Environmental/Social/Governance (ESG) Regulations
Meeting new dynamic and evolving regulatory complexities can lead to significant operational changes and investments.

Data/Information Control
Adversarial threats jeopardize the accuracy, security, and reliable flow of data throughout supply chains.

Geopolitical Tensions & Transition for Power
Global conflicts disrupting access to resources, energy, trade, as well as rising challenges for superpower status.

Talent Scarcity
A mismatch between the skills required and what the available workforce offers.

Technological Advancements/Disruptors
New investment in innovations that fundamentally change how goods are moved, stored, and managed, leading to dramatic increases in efficiency, transparency, and customer satisfaction. (e.g., Artificial Intelligence [AI]).

Gartner

Contested Logistics — A Multi-Echelon Supply Chain

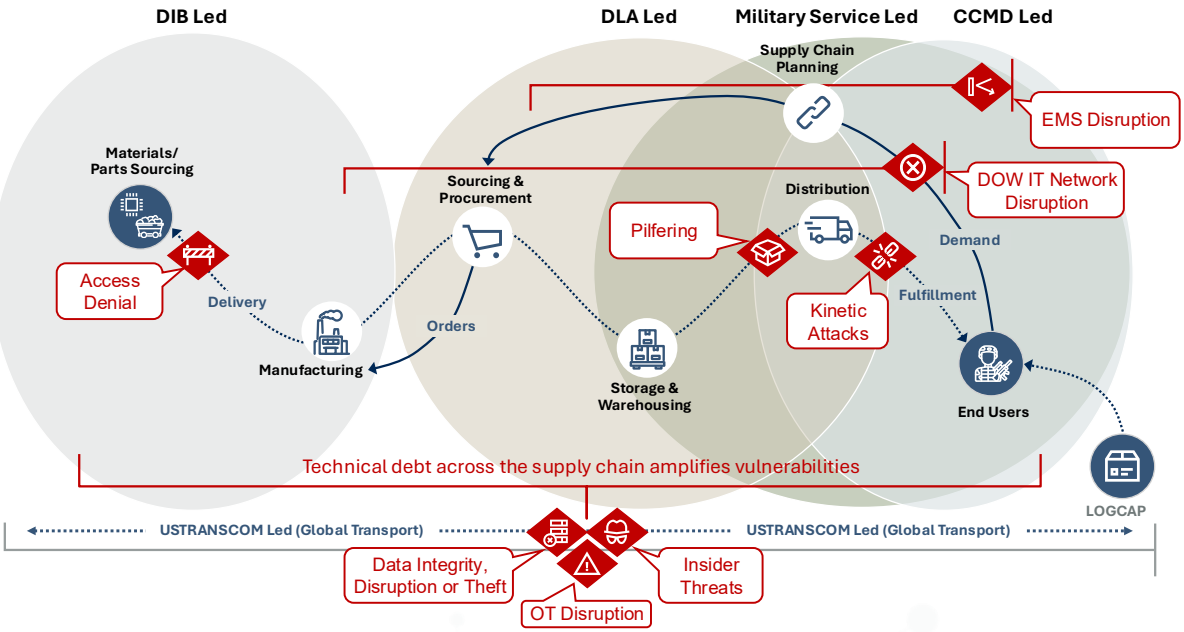
The Contested logistics environments are complex ecosystems composed of multiple stages, distributions points, suppliers, organizations and partners, each with their unique technologies, cultures, and processes across multiple operational domains — Land, Sea, Air, Space, and Cyberspace. Degradation of capabilities can occur anywhere within the network as material, money, and information moves bi-directionally. **There is no single entity that has end-to-end control and visibility of all supply chain operations which can lead to exploitable vulnerabilities by adversarial nation states, cybercriminals, hacktivists, and insiders with ill intent or seeking personal gain, etc.**

Note: The 2026 National Defense Authorization Act will likely formally designate the U.S. Transportation Commend as the "lead" for mitigating vulnerabilities and risks associated with contested logistics for the Department of War.

Pain Points & Threat Vectors

Today the warfighter faces a disparate set of threats complicated by traditional supply chain vulnerabilities with emerging threat vectors in contested environments creating a complex and high-risk landscape.

A High-Risk Landscape: Deliberate adversarial action in contested logistics environments amplify "traditional" Supply Chain vulnerabilities.



Traditional Supply Chain Vulnerabilities

These foundational weaknesses are exacerbated under contested conditions.

- **Increasing Logistics Demand & Complexity:** Growing mission requirements and multi-domain operations strain existing logistics frameworks.
- **Resource-Constrained Environments:** Limited access to critical materials, transportation assets, and personnel impedes responsiveness.
- **Limited of End-to-End Visibility:** Fragmented systems and data silos hinder real-time decision-making and situational awareness.
- **Data Integrity & Lineage Issues:** Inaccurate or manipulated data compromises planning, forecasting, and trust in systems.
- **Siloed Asset & Resource Management:** Disconnected vendor and supplier ecosystems increase risk and reduce agility.
- **Vendor & Supplier Risk:** Overreliance on single-source or foreign suppliers introduces geopolitical and operational vulnerabilities.
- **Workforce & Resource Limitations:** Talent shortages and overextended personnel reduce adaptability and resilience.
- **Dynamic & Uncertain Regulation:** Rapidly evolving compliance landscapes challenge continuity and legal assurance.
- **Tech Debt & Legacy Systems:** Outdated infrastructure limits integration, scalability, and cybersecurity posture.
- **Environmental Impacts:** Climate events and sustainability pressures disrupt supply routes and asset availability.

Contested Logistics Threat Vectors

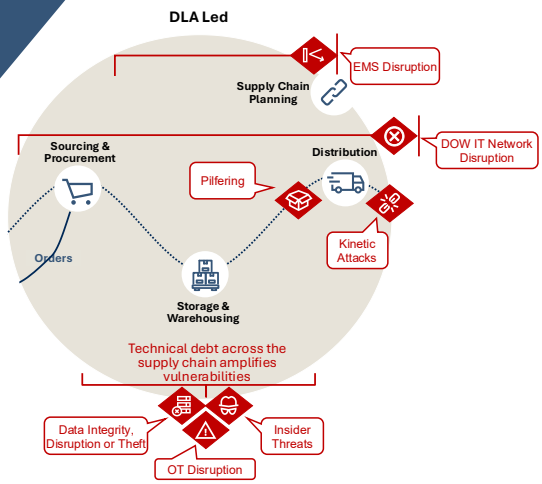
In adversarial environments, these threats directly target logistics operations:

- **Cyber-Attacks & Network Disruptions:** Targeted attacks on logistics IT systems can paralyze operations and corrupt data.
- **Kinetic Attacks:** Physical strikes on supply nodes, transport assets, or infrastructure degrade capability.
- **Access Denial (Anti-Access/Area Denial — A2/AD):** Adversaries restrict movement and access to critical regions, delaying or halting supply flows.
- **Pilfering & Theft:** Opportunistic or organized theft of supplies undermines mission readiness.
- **Insider Threats:** Compromised personnel or contractors pose risks to operational security and continuity.

*Note: **LOGCAP** logistics and life support services provided by host-nations necessary to sustain deployed forces in theater (primarily U.S. Army).*

Stakeholder Vignette 1

To effectively address supply chain vulnerabilities and threat vectors associated with contested logistics, it is essential to understand the capabilities that are at risk for each Stakeholder in the ecosystem. DLA is subject to the following major threats: EMS and DOW Network Disruptions, Kinetic Attacks, Pilfering, Cyber Attacks (Data Integrity, Disruption or Theft), Operational Technology (OT) Disruption, and Insider Threats.



Defense Logistics Agency (DLA)

'Drive and Sustain Warfighter Readiness'

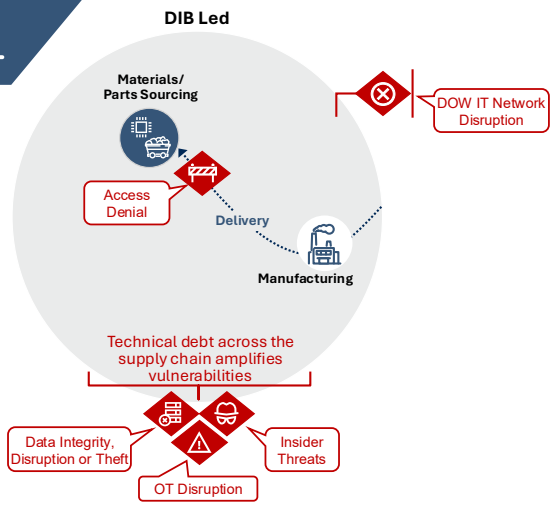
A combat support agency responsible for end-to-end management of eight global supply chains and a worldwide network with 24 distribution centers, essential for sustaining U.S. forces across all operational domains, managing everything from spare parts to uniforms, subsistence, medical supplies, and fuel. DLA also enables the full life cycle support of weapon system capabilities. Embeds liaisons within Combatant Commands and teams within service industrial sites.

DLA's Capabilities at Risk — Disruptions Can Impact:

- **Acquisition and Procurement:** Procurement of a vast range of items, from raw materials to commercially available goods like food and medical supplies, for the Department of War (DOW).
- **Supply Chain Management:** Oversight of the end-to-end supply chain for missions, including inventory management, warehousing, packaging, and transportation of supplies.
- **Global Distribution:** Operations of a global network of distribution centers to provide storage and delivery services wherever U.S. forces have a significant presence.
- **Disposal Services:** Management of the disposal of excess military equipment and property, including hazardous waste, through reutilization, resale, and demilitarization programs.
- **Energy support:** Management of the supply chain for petroleum, alternative fuels, and renewable energy, providing fuel for land, sea, air and space operations.
- **Weapon Systems Life Cycle:** Support for weapon systems and its ability to provide the vast array of consumable repair parts and other materials needed for development, maintenance and readiness.
- **Innovation Leader:** The ability to positively influence and incentivize Suppliers through the acquisition process to incorporate new technologies, advancements, and security measures.
- **Cyber Defenses:** The ability to operate and defend information systems and networks to prevent or mitigate cyberattacks that could disrupt logistics or compromise data.
- **Resilience: Ability to** anticipate, mitigate, adapt to, and recover from disruptions to maintain continuity and minimize negative impacts on operations, customers/end users.

Stakeholder Vignette 2

The DIB, partners in solutioning, advancement in technologies, and providing a more robust supply chain are subject to the following major threats: Access Denial, Cyber Attacks (Data Integrity, Disruption or Theft), OT Disruption, and Insider Threats.



Defense Industrial Base (DIB)

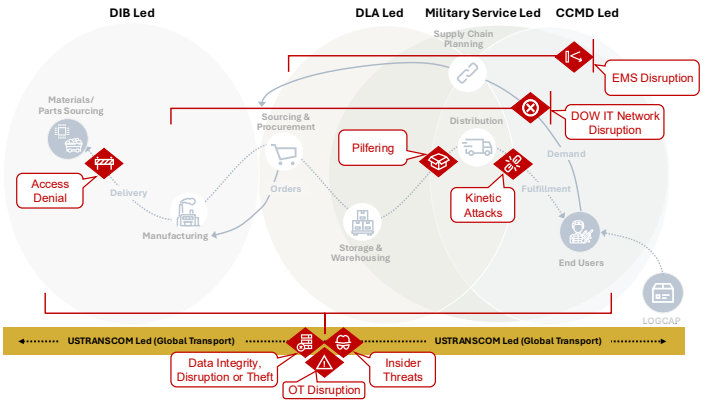
Vendors are a critical component of the DOW's team that secures U.S. Interests around the world. The DIB is often called the 5th Component. The DIB's ability to scale and support worldwide deployments is based on maintaining a healthy and robust supply chain, with deep understanding of risks and supplier's health and resiliency.

DIB Capabilities at Risk — Disruptions Can Impact:

- **Capacity Management:** Ability to support manufacturing and production capacity to surge for meeting rapidly emerging requirements.
- **Innovation Partner:** The acceleration of technological innovation to develop new solutions for advancements in manufacturing, improvements in demand forecasting, hardening cybersecurity infrastructure, etc.
- **Cyber Defenses:** The ability to operate and defend information systems and networks to prevent or mitigate cyberattacks that could disrupt logistics or compromise data.
- **Resilience:** Anticipating, mitigating, adapting to, and recovering from disruptions to maintain continuity and minimize negative impacts on operations, customers/end users.

Stakeholder Vignette 3

USTRANSCOM, an essential Combatant Command (CCMD) partner in global mobility for project and sustainability of joint forces, is subject to the following major threats: EMS and DOW Network Disruptions, Kinetic Attacks, Pilfering, Cyber Attacks (Data Integrity, Disruption or Theft), OT Disruption, and Insider Threats.



U.S. Transportation Command (USTRANSCOM)

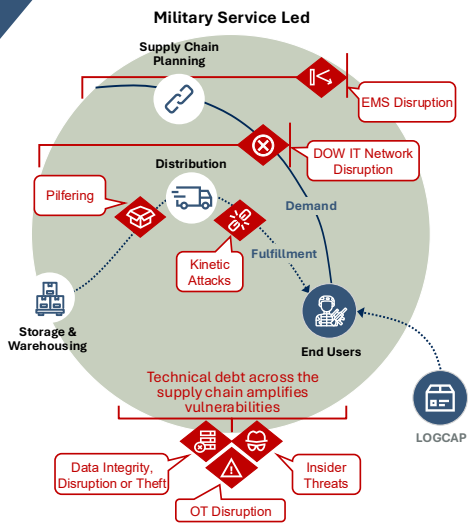
The CCMD charged to project, maneuver, and sustain the forces globally, possessing the expertise, authorities, and real-time awareness to accomplish assigned missions. Collaborates with DLA on providing integrated transportation services to support delivery of supplies.

USTRANSCOM Capabilities at Risk — Disruptions Can Impact:

- **Global Transportation:** Synchronization of global mobility capacity and planning across the Joint Deployment and Distribution Enterprise (JDDE), the broad network of military, commercial, and government partners that work together to move troops and equipment globally.
- **Mobility Resilience:** Ability to minimize the effects of cyber threats on commercial transportation providers, limiting the JDDE's ability to maintain alternative transportation routes and its ability to optimize relations with transportation agencies and commercial partners.
- **Technology & Innovation:** The development of new requirements, the ability to influence designs, and provide oversight, as well as integrate support for new technologies to improve operations.
- **Visibility & Analytics:** Data interoperability and in-transit visibility (ITV), which would give warfighters real-time location information on supplies, weapons systems, and other materials.
- **Cyber Defenses:** The ability to operate and defend information systems and networks to prevent or mitigate cyberattacks that could disrupt logistics or compromise data.

Stakeholder Vignette 4

Logistics providers under the control of Military Services procure services and goods in the contested logistics environment are subject to the following major threats: EMS and DOW Network Disruptions, Kinetic Attacks, Pilfering, Cyber Attacks (Data Integrity, Disruption or Theft), OT Disruption, and Insider Threats.



Military Services

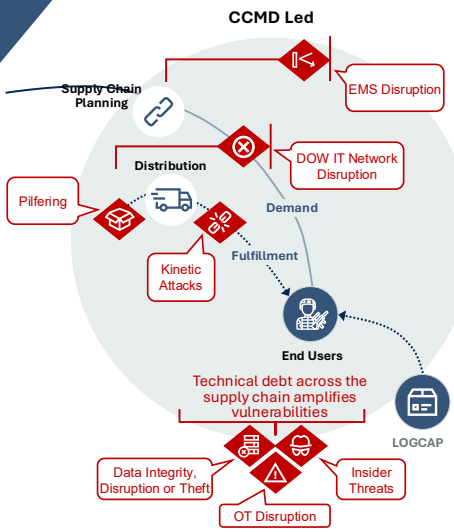
Military service branches, or defense agencies that purchase or request supplies.

Customer Capabilities at Risk — Disruptions Can Impact:

- **Demand Forecasting & Requirements Definition:** Accuracy in what is needed, when, and in what quantities. This includes specifying mission-critical items like fuel, ammunition, medical supplies, or spare parts.
- **Contracting & Procurement:** Coordination with DLA to manage acquisition processes, including vendor selection, contracting, and compliance with regulations (e.g., Federal Acquisition Regulation).
- **Funding & Resource Allocation**: Decision making for budgets and allocation of resources to support logistics operations.
- **Strategic Planning:** The shaping of logistics strategy, including pre-positioning of supplies, contingency and digital scenario planning, and risk mitigation in contested environments.
- **Technology & Innovation Partner:**
  - The responsible adoption of emerging technologies, (e.g., the integration of AI, autonomous systems, additive manufacturing (3D printing), and predictive analytics into logistics operations).
  - Innovation in acquisition models (e.g., agile contracting, rapid prototyping) to accelerate delivery in contested environments.
  - Collaboration efforts with Industry & Academia to fund and develop solutions tailored to contested logistics (e.g., resilient supply chains, expeditionary energy solutions).
- **Cyber Defenses:** The ability to operate and defend information systems and networks to prevent or mitigate cyberattacks that could disrupt logistics or compromise data.
- **Resilience:** Anticipating, mitigating, adapting to, and recovering from disruptions to maintain continuity and minimize negative impacts on operations, customers/end users.

Stakeholder Vignette 5

CCMDs, their partners across Host Nations and Logistics Civil Augmentation Program (LOGCAP) are subject to the following major threats: EMS and DOW Network Disruptions, Kinetic Attacks, Pilfering, Cyber Attacks (Data Integrity, Disruption or Theft), OT Disruption, and Insider Threats.



Combatant Commands (CCMDs)

'Deter and win wars, protect U.S. interests, and ensure security cooperation with allies and partners'

A unified U.S. military unit with broad, continuing missions executed by eleven (11) commands with forces from different military branches which are organized by either a specific geographic area or functional specialty. Responsible for executing and sustaining military operations. Some CCMDs act in the capacity both as a Partner (e.g., USTRANSCOM) and Customer/End User.

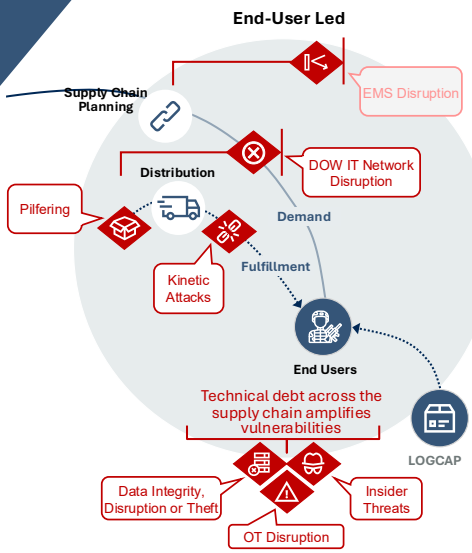
CCMDs Capabilities at Risk — Disruptions Can Impact:

- **Resilience:** Ability to develop and coordinate implementation of plans that can sustain forces even when traditional supply routes and facilities are targeted. This includes prepositioning supplies, leveraging local and/or host nation support (HNS) resources, and reducing overall demand through innovative technologies. LOGCAP coordination to quickly tap into civilian contractor resources when military units and host-nation support are unavailable or insufficient.
- **Visibility & Analytics:** Ability to create a common operational picture of logistics for each military operation by tracking supply usage, predicting needs, and simulating scenarios to identify vulnerabilities.
- **Technology & Innovation: In the capacity** as a Customer/ End User and a partner with DLA, the DIB, and others, the ability to influence the design of new advancements. As a trusted Partner, CCMDs ability to provide oversight and integrate new technologies for improved supply chain and logistics operations.
- **Security:** Ability to effectively collaborate with DLA to protect the global defense supply chain. This includes defending against cyber threats to industrial control systems and transportation networks.
- **Cyber Defenses:** The ability to operate and defend information systems and networks to prevent or mitigate cyberattacks that could disrupt logistics or compromise data.

Gartner

Stakeholder Vignette 6

Customers (aka Warfighters or onsite operations) receiving supplies to actively sustain forces are subject to the following major threats: EMS and DOW Network Disruptions, Kinetic Attacks, Pilfering, Cyber Attacks (Data Integrity, Disruption or Theft), OT Disruption, and Insider Threats.



Customers/End Users

The individual warfighting unit of action (e.g., tactical unit, ship, aircraft, vehicle, satellite, soldier/airman/sailor/marine, etc.) under operational control of CCMDs who uses or consumes the delivered goods and services.

End User Capabilities at Risk — Disruptions Can Impact:

- **Operational Feedback & Adaptation:** Real-time feedback about the performance, suitability, and reliability of logistics support as conditions change rapidly In contested environments.
- **Inventory Management & Last-Mile Execution:** The tracking, handling, and distribution of supplies at the tactical edge — often the most vulnerable and complex part of the supply chain. Additionally, executing the final delivery of supplies from a forward logistics node to the point of use, as well as managing risks like theft, spoilage, or enemy interference during last-mile delivery.
- **Innovation at the Tactical Edge:**
  - Innovates with field-level problem solving by repurposing materials, modifying equipment, or creating ad hoc solutions when standard logistics fail.
  - Providing feedback loop for new innovations to inform iterative improvements in logistics systems and technologies.
- **Cyber Defenses:** The ability to operate and defend information systems and networks to prevent or mitigate cyberattacks that could disrupt logistics or compromise data.
- **Resilience:** Anticipating, mitigating, adapting to, and recovering from disruptions to maintain continuity and minimize negative impacts on operations, customers/end users.

Key Contested Logistics-related Capabilities

Capability Matrix

The following Capability Matrix, provides a framework to assess the participation and interdependencies of all stakeholders involved in Contested Logistics space. It outlines the core capabilities required to plan, execute, and enable the movement and support of military/operational forces in environments where adversaries actively disrupt logistics operations across all domains, including air, land, sea, space, and cyberspace.

Capabilities

● Command & Participation ◒ Participation ○ Limited Participation

Activity	DLA	DIB	USTRANSCOM	Military Services	CCMD	Customers/ End Users
Holistic Management of Contested Logistics Ecosystem			**Owner**			
▪ Supply Chain Design & Implementation	●	◒	●	◒	◒	◒
▪ Acquisition & Procurement (Includes Supplier Management)	●	●	●	●	●	●
▪ Logistics & Distribution	●	◒	●	◒	●	◒
▪ Execution in Theater	◒	◒	●	◒	●	●
▪ Technology & Innovation	●	●	●	●	●	●
▪ Visibility & Analytics	●	●	●	●	●	●
▪ Cyber Defenses	●	●	●	●	●	●
▪ Resiliency	●	●	●	●	●	●

Major Takeaways:

- **Entry Points:** Each stakeholder has unique leverage points — where a small change can produce significant and lasting effects, (e.g., DLA in supply chain hardening, USTRANSCOM in mobility resilience).
- **Coordination Gaps:** Limited full end-to-end visibility and siloed operations increase vulnerabilities (e.g., Holistic Management).
- **Strategic Alignment:**
  - Each stakeholder must be accountable for hardening cyber defenses, employing coordinated resiliency plans, as well as visibility and analytics capabilities which are critical for proactively managing and overcoming active threats to disrupt supply chains.
  - Development of a joint doctrine and shared threat models are essential for unified response.

Gartner

Next Steps — Call to Action

Urgent action is needed as drivers, gaps in capabilities, and threat vectors will heavily impact Contested Logistics over the next three to five years. These unique challenges and opportunities demand attention to maintain adversarial and strategic advantage with a resilient integrated warfighting logistics capability.

Prioritize

Establishing Holistic Supply Chain Risk Management

- Create a unified governance framework that integrates joint, interagency, commercial, and allied logistics efforts.
- Designate a lead organization or joint task force to oversee contested logistics planning, risk mitigation, and capability development.
- Implement a federated logistics architecture that enables decentralized execution with centralized coordination across domains and theaters.

Strengthen Cyber Defense & Resiliency

- Stakeholders harden logistics networks and platforms against cyberattacks, spoofing, and data manipulation.
- Test for degraded, denied, and disconnected environments, including contested cyber and space domains.
- Integrate zero-trust architectures and AI-enabled anomaly detection into logistics IT and OT systems to ensure continuity under attack.

Visibility & Analytics Across the Ecosystem

- Deploy real-time, multi-domain logistics systems that integrate stakeholder data sources (e.g., versus siloed view).
- Invest in predictive analytics and digital twins to simulate disruptions and optimize contingency planning.
- Illuminate “dark spots” in the supply chain using advanced sensors, blockchain, and autonomous reporting tools.

Technology & Innovation

- Establish contested logistics innovation hubs to rapidly prototype and design for scale new technologies (e.g., use of autonomous resupply systems, additive manufacturing, expeditionary logistics kits. etc.) for guaranteed delivery regardless of conditions, crashing lead times, and reductions in the cost to serve.

Acquisition, Procurement & Cost Optimization

- Foster agile acquisition pathways to enable secure and faster services and integration of technologies.

Gartner

Partnering with Gartner

Gartner's Mission Solutions provides cross-industry expertise, scalable solutions and implementations for Contested Logistics.

We can be your partner where you are in your journey.

Fundamentals
Evaluation & Strategic Alignment

Applications
Acceleration & Innovation

Optimization
Operate & Evolve

Hardening Supply Chains	Acquisitions, Procurements & Cost Opt.	Speed & Efficiency	Supply Chain Risk Management	Technology & Innovation
Simulation Exercises and Tabletops	Cost to Serve	Supplier Assessments	Supply Chain Strategy & Implementation Plan	AI Integration Design
Minimally Viable Supply Chain	Vendor Ecosystem Assessment	Business Process Reengineering	Maturity Assessment	Digital Twin Design
Disaster Recovery	Waste Reduction	Technology & Automation Assessment	Third-Party Risk Management	Tool Assessment & Rationalization
Business Continuity			Control & Visibility: Metrics & Dashboards	DevSecOps
Resilience			Operating Model Modernization	Data Security
Preemptive Cybersecurity			Policy & Standards Development	
			Insider Threat	

Gartner is poised to address the need for holistic management of Contested Logistics environment and the maturity of capabilities customized and delivered to meet mission needs. Please coordinate with your Gartner Managing Partner.

Gartner

With Gartner, defense leaders gain the clarity and confidence to make informed decisions that directly support the warfighter — where it matters most.

Gartner's Approach

Gartner provides a comprehensive suite of tailored mission solutions, delivery models and tools that are customizable and scalable across AI, Cybersecurity, Supply Chain and Technology Innovations to help re-design operations in today's contested environment. Gartner's approach draws on business technology insights both globally and contextualized for defense, delivered by seasoned practitioners with extensive experience across the warfighting Contested Logistics environment.

Benefits: Unlock Mission-Ready Supply Chain Excellence

Gartner drives consistent, scalable success — empowering defense operations in high-stakes environments. Our expert solutions and insights build resilient and secure supply networks to:

- Withstand disruption
- Maximize operational efficiency and cost-effectiveness
- Accelerate logistics responsiveness a
- Mitigate risks across the supply chain ecosystem
- Integrate purpose-fit technologies and innovation

Gartner

Gartner Point of Contact

Gartner
John Fitzgerald
Senior Managing Partner
Federal Mission Solutions
Phone: +1 703 963 0302
Email: john.fitzgerald@gartner.com

Gartner
Tim Galginaitis
Senior Managing Partner
Federal Mission Solutions
Phone: +1 571 379 1713
Email: tim.galginaitis@gartner.com

Gartner
Tom Schneider
Expert Partner
Federal Mission Solutions
Phone: +1 703 338 1645
Email: thomas.schneider@gartner.com

Gartner
Mary Ann Wagner
Managing Partner
Gartner Consulting
Phone: +1 703 346 7723
Email: maryann.wagner@gartner.com

Appendix

Stakeholder Focus Areas — *Illustrative Use Cases*

When logistics operations incorporate new processes, advanced technologies, a skilled workforce, and innovative solutions, they showcase the transformative warfighting impact of synchronized logistics in achieving mission outcomes.

This section presents a series of illustrative vignettes that highlight stakeholders' critical logistics capabilities and provide a sense of "What good looks like…", as required for agility, transparency, and security in sustaining warfighter operations in contested logistic environments across land, air, maritime, space, and cyberspace domains.

- Joint Logistics Element: European Theater of Operations
- Microelectronics Manufacturer Operations & Global Supply Chain
- Aerospace Manufacturer's Global Supply Chain
- U.S. Transportation Command: Global Transport Provider

Gartner

Joint Logistics Element: European Theater of Operations

Illustrative Use Case

A joint logistics element sustains U.S. and allied forces in Europe during the Ukraine conflict. An adversary employs cyber attacks, kinetic strikes, and information operations to disrupt supply chains across land, sea, and air domains. The mission demands agile procurement and delivery of ammunition, medical supplies, and fuel, overcoming sanctions and contracting hurdles while leveraging AI-driven logistics planning and resilient, space-enabled asset tracking.

DLA's Role: DLA rapidly procures ammunition, medical supplies, and fuel to U.S. and allied forces, leveraging agile contracting models, AI-enabled risk assessments, and secure logistics platforms. Using predictive analytics and AI tools, DLA streamlines RFP analysis, vendor selection, and contract execution under time-sensitive sanctions and operational conditions.

Outcomes:

- AI-enabled inventory forecasting to improve demand planning
- Enhanced cyber resilience
- Integrated logistics dashboards for real-time visibility, decision support, threat simulation and predictive analytics leveraging digital twins
- Synchronized, efficient, and secure logistics operations across the joint force

Acquisition, Procurement and Cost Optimization	▪ **Market Intelligence and Supplier Insights:** Employe up-to-date analysis on supplier capabilities, market trends, and emerging threats, enabling DLA to make informed, rapid procurement decisions ▪ **Training and Change Management:** Provide training resources and change management support to help DLA personnel adapt to new procurement processes and technologies ▪ **Incentivized Suppliers:** Provide both monetary and non-monetary incentives for suppliers to accelerate Integration of space-hardened technologies and AI-enhanced logistics software
Supply Chain Risk Management	▪ **Risk Management and Resilience Planning:** Leveraged AI-powered digital twins to monitor critical assets, predict failures, optimize supply chain logistics, enhance cybersecurity, assessed and mitigated supply chain risks, including those specific to contested environments (cyber threats, access denial, vendor instability) ▪ **Regulatory and Compliance:** Tracked regulatory changes to ensure DLA's rapid procurement activities remained compliant, even as regulations evolve in contested environments
Technology & Innovation	▪ **Technology Optimization:** Evaluated and identify procurement technologies (e.g., e-procurement platforms, supply chain visibility tools, AI-driven analytics) that could automate and expedite procurement tasks ▪ **Modernizations for Improved Supply Chain Risk Management:** – AI-enabled inventory forecasting and automated warehousing – Integrated supply chain platforms for tracking shipments across domains – Integrated logistics dashboards for real-time visibility and decision support ▪ **Effective Integrations:** Integrate new systems with legacy DLA infrastructure to promote smooth adoption and rapid impact
Hardening Supply Chains	▪ **AI Tools for Cyber Defenses:** Relieve burden on stretched cybersecurity/IT resources while proactively managing risks with AI Threat Detection & Response, Automated Vulnerability Scanning, Intelligent Access Control, Autonomous Incident Response, and AI Enhanced Endpoint Protection ▪ **Leveraging Partners:** In collaboration with DISA and U.S. Cyber Command: – Defend logistics information systems and operational technology (OT) networks from AI-driven cyberattacks and signal spoofing – Conduct cyber posture assessments and simulated threat scenarios – Maintain secure communications via satellite-based VPNs and zero-trust architectures ▪ **Resilience Planning:** – Utilize real-time threat intelligence to anticipate disruptions – Utilize AI to dynamically reroute supplies and optimize transport under threat – Activate distributed logistics nodes and autonomous resupply systems
Speed & Efficiency	▪ **Best Practices and Process Optimization:** Benchmark and implement best practices for agile procurement processes, including streamlined sourcing, contract management, and supplier onboarding

Gartner

Microelectronics Manufacturer: Operations & Global Supply Chain

Illustrative Use Case

A large U.S. microelectronics manufacturer producing advanced semiconductors for defense systems relies on a global supply chain dominated by foreign sources for critical raw materials and outsourced wafer fabrication, exposing it to supply disruptions and downstream cybersecurity threats. To mitigate these risks, the manufacturer must rapidly diversify suppliers across allied nations, harden digital networks with real-time threat monitoring, and scale up domestic chip fabrication and raw-material processing facilities.

DIB's Role: Acts as an integral part of defense logistics, providing the research, design, production, delivery, and sustainment of critical military systems and materials. In this use case, the DIB supports strategic investment in domestic surge capacity and operational continuity under multi-domain supply chain pressure through proactive supply chain risk management and resilience.

Outcomes:

- Accelerated investment in domestic production capacity
- Secure and resilient logistics support despite adversarial disruption
- Diversified sourcing of critical materials to reduce geopolitical risk through third-party risk management
- Validated industrial surge model for future contested logistics scenarios

Supply Chain Risk Management	▪ **Capacity Management:** – Mapped and documented multi-tiered supplier relationships – Reallocate resources across a global manufacturing network to meet urgent demand, supported by operating model modernization – Utilize AI-driven demand forecasting to prioritize production based on operational needs – Invest in new suppliers in new locations to broaden multi-region availability of critical parts – Activated surge production lines for munitions, tactical gear, and communications systems – Map and document multi–tiered supplier relationships – Management and planning of raw material sourcing
Hardening Supply Chains	▪ **Cyber Defenses:** – Resilience testing to simulate and mitigate cyberattacks on production and distribution systems – Partner with DOW cyber teams to harden networks and secure data exchange – Implement Zero-Trust architecture, data security, and real-time threat monitoring across ICS ▪ **Resiliency:** – Diversify supply sources and prepositioned critical components in secure locations – Adapt production schedules and delivery routes in response to real-time threat intelligence – Build alternative logistics networks – Maintain continuity through redundant facilities, secure cloud-based logistics platforms, and interoperable systems
Technology & Innovation	▪ **Advancements:** – Accelerate development of modular, rapidly deployable systems tailored for contested environments – Collaborate with DLA and CCMDs to integrate advanced manufacturing techniques (e.g., additive manufacturing) and digital twin design for scenario planning – Enhance logistics planning with predictive analytics and AI-enabled supply chain modeling

Aerospace Manufacturer: Global Supply Chain

Illustrative Use Case

During a global pandemic, a major aerospace OEM faces challenges in sourcing critical avionics and structural components from its global network of suppliers as workforce shortages, regional lockdowns, and evolving airport curfews disrupt cargo flights and ocean shipments. With each country enforcing different health mandates and travel bans, supplier delivery schedules became erratic, making it nearly impossible to guarantee on-time part availability for scheduled assembly-line production. To mitigate these risks, the manufacturer begins investing domestic surge capacity, diversifies its supplier base, and deploys real-time supply-chain risk monitoring to sustain continuous operations.

DIB's Role: Acts as an integral part of defense logistics, providing the research, design, production, delivery, and sustainment of critical military systems and materials. In this use case, the DIB aerospace manufacturer supports both strategic surge capacity and operational continuity under geopolitical and adversarial pressure.

Outcomes:

- Achieved resilient logistics support despite global disruption
- Accelerated domestic investment in secure production facilities and diversified supply chains
- Enhanced interoperability and coordinate with key partners (DLA, USTRANSCOM, and CCMDs)
- Validated industrial surge model for sustained production and rapid responsiveness

Supply Chain Risk Management	▪ **Capacity Management:** – Utilize AI-driven demand forecasting and digital scenario planning to mitigate volatile demand signals – Invest in new suppliers, informed by robust vendor ecosystem assessment and third-party risk management – Activate surge production lines supported by operating model modernization – Ensure supply chain visibility by mapping multi-tiered supplier relationships and applying control and visibility metrics
Hardening Supply Chains	▪ **Cyber Defenses:** – Implement Zero-Trust architecture and real-time threat monitoring across ICS – Secure information systems and networks using robust data security protocols to protect critical data integrity – Conduct Simulation Exercises and Tabletops to test defenses against supply chain cyberattacks ▪ **Resiliency:** – Diversify supply sources and implemented redundancy planning – Adapt production schedules and delivery routes in response to real-time threat intelligence – Build alternative logistics networks – Maintain continuity through an optimized supply chain supported by secure, cloud-based logistics platforms
Technology & Innovation	▪ **Advancements:** – Enhance logistics planning using predictive analytics and customized AI integration for supply chain modeling – Accelerate secure capability development and deployment utilizing DevSecOps practices – Collaborate with DLA and CCMDs on advanced manufacturing techniques (e.g., additive manufacturing) and digital twin design for strategic components

U.S. Transportation Command: Global Transport Provider

Illustrative Use Case

A joint force requires rapid force projection and sustainment into contested Indo-Pacific region under persistent Anti-Access/Area-Denial (A2/AD) threats across extended supply and communication lines. Adversarial electronic warfare, cyber-attacks, and kinetic strikes target key logistics nodes and lines of communication across the maritime and air domains. The mission demands rapid, distributed logistics capabilities to penetrate the A2/AD environment and maintain resilient supply lines.

USTRANSCOM's Role: Coordinates and executes rapid strategic sealift and airlift into contested littorals as the DOW lead for contested logistics (per 2026 NDAA, pending). In coordination with geographic CCMDs, ensures mobility resilience by utilizing dispersed port hubs, alternative routes, and sea-basing concepts to mitigate interdiction risk. Defends transportation systems against kinetic, cyber, and electronic warfare threats while synchronizing efforts with DLA and CCMDs to support sustained force projection into the theater

Outcomes:

- Rapid force projection into a contested theater with minimal disruption
- Resilient mobility operations utilizing dispersed nodes across military and commercial domains
- Enhanced synchronization and coordination with DLA, CCMDs, and commercial partners
- Validated model for distributed strategic mobility in future multi-domain operations (MDO) and conflict scenarios

Technology & Innovation	▪ **As a Customer/End User:** Develop and refine requirements for logistics platforms, including autonomous logistics system, including unmanned vessels and expeditionary drones ▪ **As a Partner:** Provide integration support for new technologies into existing transport and logistics frameworks, especially multi-modal command and control (C2) systems
Hardening Supply Chains	▪ **Cyber Defenses:** – Secure information systems used in maritime/air movement coordination – Identification and mitigation of cyberattacks targeting transportation infrastructure, including port operations and terminal systems – Collaborate with DLA and CCMDs to implement zero-trust architectures and AI-enabled threat detection across the logistics enterprise ▪ **Mobility Operations & Data Governance** – Implement cyber threat mitigation measures for commercial transportation providers and establish protocols for managing alternative routes – Strengthen collaboration with transportation agencies and partners to ensure continuity of operations – Enhance data management and governance to improve access to and quality of logistics data, and to protect infrastructure from adversarial threats ▪ **Resiliency:** – Implement alternative routing strategies using allied infrastructure and commercial corridors – Collaborate with DLA and other partners, to harden systems against cyber threats and maintain operational continuity – Establish redundant distributed logistics nodes and sea-based capabilities to penetrate A2/AD environments
Supply Chain Risk Management	▪ **Visibility & Analytics:** – Integrate multi-domain sensors and interoperable data platforms to monitor the movement of critical maritime and air cargo – Provide warfighters and mission planners with real-time location data on supplies and equipment – Ensure visibility across terrestrial and maritime logistics chains, coordinating movements despite jamming and spoofing

Gartner