Deloitte.

A report from the
Deloitte Center for Government Insights

Using digital supply networks to combat systems confrontation warfare

MAKING AN IMPACT THAT MATTERS since 1845

The Future of Warfighting

The Deloitte Center for Government Insights is undertaking a yearlong research project focused on helping defense organizations prepare for the next 15 years of defense challenges. While defense challenges are ever shifting, our research has identified interoperability—within militaries, within government, between nations, and within industry—as being key to meeting uncertain threats.

Through more than 60 experts representing 12 countries across North America, Europe, and Asia, this research will produce more than a dozen insights articles offering ways of improving interoperability across key military areas. Research will detail how specific defense organizations can improve interoperability across defense challenges based on country-level expertise. The four leading defense challenges assessed from strategy documents of the 12 countries include near-peer warfare, grey zone threats particularly from technology, limited scale warfare, and defending the rules-based international order. The goal is to not only promote discussion at the international and intra-national levels, but demonstrate, in part, how greater interoperability can occur.

Visit www.deloitte.com/futureofwarfighting to access the Future of Warfighting collection and the interactive Interoperability index.

Future of Warfighting Interoperability Index

In focus: Resilient Operations

FIGURE 1

The demands of interoperability vary with defense challenge

Assessed level of interoperability needed

Gray zone threats | Near-peer/peer warfare | Defending rules-based international order | Limited-scale warfare

	1 Baseline	2 Joint/Service	3 Intranational	4 Intercountry	5 Systemic
Development and acquisition	• Repeatable, transparent acquisition processes	• Ability to own and share technical data for select acquisition programs (e.g., via digital or model-based systems engineering) • DevSecOps, Agile, or other iterative models of production used for select software development • Mechanism for joint requirements development/coordination (e.g., JROC in the United States) • Standards for joint interoperability of key systems • Services have access to technical baseline data • Flexible acquisition processes operating at the speed of technology	• Ability to own and share technical data for all major acquisitions (e.g., via digital or model-based systems engineering) • DevSecOps, Agile, or other iterative models of production used for all software development • Mechanism for efficient and timely intragovernment coordination • Open architectures to ensure better interoperability even of proprietary systems • Services have access to live data from systems • Enhanced and inclusive mechanism for government/industry coordination • Shared curriculum to educate leaders on emerging technology	• Ability to rapidly share technical details between/among government and industry to allow for distributed production (e.g., using common digital engineering tools) • Open architectures with international standards to ensure better interoperability even of proprietary systems • Mechanism for coordinating international rapid acquisition coordination • Mechanism for international authentication of trusted vendors and sharing of IP • International program for tech education and advancement	• Ability to share consumption/use data from tactical edge to inform network of international producers (e.g., common digital thread) • Allies iterative development of shareable systems • Mechanism for coordinating defense innovation with allies and partners
Resilient operations	• National forces can move to a conflict, sustain and protect themselves, and apply force to an adversary	• Common operational standards for common tasks such as air support • Ability to leverage other services'/central military capabilities for transport, fires, or logistics • joint capabilities to protect integrity of force, including from industrial threats (e.g., suppliers or knowledge of suppliers)	• Shared appreciation of problem sets across government • Understanding the capabilities that industry/government can bring to bear • Process to leverage those capabilities form industry/government	• Shared understanding of allied forces' incentives, risks, and goals • Common operating picture for allied/partner/commercial military-relevant capabilities • Shared international standards for key components (types of fuel, size of pallets, radio encryption, data formats, permission, etc.)	• Ability to seamlessly drive tactical data between countries, agencies, and even industrial bases to coordinate responses • Integrated information systems that can share data according to need and clearances • Ability to visualize and tap into military, allied, capabilities in real time at the tactical level
Workforce, skills, and culture	• Defined and accountable organizational culture in defense organizations • Recruitment sufficient to maintain desired end-strength and contemporary skills	• Talent management to account for individual workforce skills and needs • Capacity to quickly organize cross-functional teams • Agile hiring policies to attract and retain top talent in emerging skills • Change in mindset from "know it all" to "learn it all" • Joint standards for use of automation	• Talent management for interagency assignments • Shared skills and experiences between government and industry via rotation and new talent models • Government, industry, and academic collaboration to shape talent pipeline • Clearly defined inherently government functions and understanding of comparative advantage for all other functions	• Talent management that takes into account allied skills and capabilities • Shared skills and experiences between ally and partner industry, academia, and government • Create cross-functional allied/partner teams and automation	• Cultivate a culture of shared defense across nations, industry, and militaries • Workforce where military/civilians can leave and return to service • Shared understanding among allies/partner of appropriate use of human vs. automation (e.g., AI ethics principles)
Decision-making	• Secure, reliable information systems • Trustworthy data • Timely data collection and analysis • An understanding of policy and legal boundaries/ permissions	• Coordinated architectures for interservice information management systems • Timely access to mission-relevant joint data • Joint leadership development curriculum tailored to the spectrum of defense priorities • Culture of trust to enable faster decision-making	• Common operating pictures for key issues shared across government agencies • Information management systems capable of bidirectional sharing of data operating in both connected and disconnected modes • Timely access to interagency mission-relevant data • Process for coordinating tasks based on agency legal/policy authorities • Interagency leadership development curriculum tailored to shared-mission areas	• Information and data management for seamlessly sharing information with allies/partners according to their clearance and immediacy of need without manual processes • Ability to visualize impacts to national interests across social, political, economic, and other dimensions (e.g., via narrow-scope AI tools) • Process for coordinating tasks based on international legal/policy authorities • International leadership development curriculum tailored to specific mission areas	• Ability to coordinate international response to threat in minutes or hours • Automated information and data management system for combined common operating picture tailored to mission need and permissions (e.g., via general-purpose AI tools) • Shared culture of trust/risk-taking • Adaptable policy and legal permissions for combined operations

During WW2 the US and its allies lost 3,500 allied merchant ships, 175 allied warships, and 72,200 naval and merchant seamen providing supplies to Europe from North America. The need to supply the European theater via the Atlantic made the Atlantic Ocean a fierce battle ground. As fierce as the Battle of the Atlantic was, it was largely contained to the Atlantic Ocean where German U-Boats and bombers could attack supply lines. Despite the incredible losses, they would have been far worse had the German military been able to attack the factories, trains, and workforce in North America that produced the supplies.

Today, supplying a military caught in a peer fight would expose each factory, ship, train, plane, truck, ally, partner, and even the workforce no matter where they are located. That's because the future of warfare is likely to see systems-confrontation campaigns[1], which use physical, digital, and electronic warfare means to interfere with the physical and digital systems that a modern logistical process relies on. Through systems confrontation strategies a modern military's logistical processes can be stalled before they even start. For instance, a ransomware attack could stop oil distribution, or a disinformation campaign could convince large segments of the workforce that it's unsafe to be at work.

Article elements

- Logistics interoperability
- Near-peer/peer warfare
- US perspective

Key topics

- Systems warfare
- Digital supply networks
- Digital thread technologies

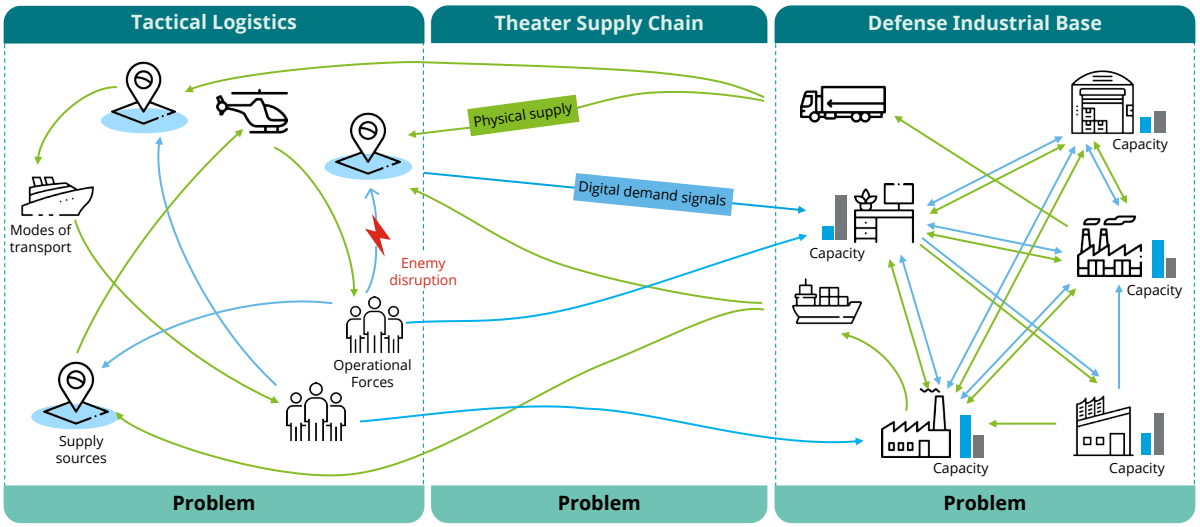
To complement digital attacks, systems confrontation warfare also leverages physical attacks through conventional munitions that sink ships, shoot down planes, or destroy supply depots. In all, modern combat logistics must be prepared to endure attacks in all operational domains[2] and across allies, industry, and government agencies to rapidly design, produce, and deploy combat resources.

The best guarantee for sustaining combat logistics against an adversary waging system confrontation warfare is creating interoperable physical-digital supply networks. Unlike fragile, linear supply chains, digital supply networks offer many redundant ways to connect demand with supply and mobility at the tactical edge or production capacity in the industrial base. Commercial industry has been leveraging digital supply networks for years, but not at the scope and scale needed for systems confrontation warfare. To meet the needs of this type of warfare, militaries need to create digital supply networks not just within their armed services, but also with its allies, partners, and even industry.

Combat logistics in a "systems" world

In 1959, Read Admiral Henry Eccles defined the functions of a logistics system as "the bridge between the economy of the Nation and the tactical operations of combat forces."[3] Like any bridge, logistics must have firm foundations on either side, meeting the different needs of both the industrial economy and tactical forces. This can be challenging because tactical forces and the defense industrial base face very different challenges. At the tactical edge, the challenge is one of capabilities finding the right supplies and the right transport at the right time to keep operations moving. In the industrial base, the problem is one of capacity—ensuring that producers have enough capacity to make what is required when it is required.

This means the digital supply networks must serve two very different purposes: it must coordinate capabilities at the tactical edge and coordinate capacity in the industrial base.



Connect demand to the right sources of supply and the right mobility to move it—all from different services and allied nations—in as near–real time as possible, and do so in a contested information environment.

Provide the physical and digital infrastructure to connect tactical logistics and the defense industrial base.

Coordinate the capacity of different types of production across the defense industrial base to ensure fast, reliable production of even entirely new materiel.

Coordinating capabilities at the tactical edge

Tactical forces need the right supplies moved by the right transport at the right time. It is a complicated problem, but not an unprecedented one. Gig transportation apps solve a similar problem, matching the many riders with unique transit demands to many drivers with unique locations and drive times. Digital supply networks for combat logistics would work on a similar principle to network together allied and partner capabilities to inform commanders what supplies are available and what transportation near the front can deliver them. To be sure, militaries have connected supplies with nearby transportation for decades. What makes digital supply networks different is the way they leverage smart algorithms, significant data management, sharing across partners, an ability to operate in connected and disconnected modes, and joint view of the battle space that integrates operational and logistical pictures to inform and speed operations while reducing patterns the adversary could take advantage of.

Using other sources of data ranging real-time consumption rates to weather, operational and intelligence data, could allow commanders to proactively resupply units with exactly what they need and when and where they need. Such an approach would introduce new levels of flexibility and adaptability while reducing the concentration of troops and supplies that were typical for past logistics efforts but only make juicy targets today.

Coordinating capacity in the industrial base

In addition to delivering troops supplies, warfare can also demand entirely new items, whether theater specific vehicles, radio parts, new body armor, or countless other items deemed necessary by operational requirements. This creates challenges for the industrial based. Since the precise needs of a conflict cannot be predicted, there is no guarantee that the firms best positioned to design or manufacture the needed equipment are available when needed. They may already be committed to a different high priority project or not have sufficient design capability to meet the timelines. Overcoming these challenges requires coordinating industrial capacity.

Coordinating capacity is not just about finding a manufacturer to produce a new radio or vehicle, it's also knowing not only where all the necessary materials will come from to make the item in the first place, but their sufficiency in the supply pipeline. This inevitably extends to allies and partners given the complexity of global supply chains today. Digital supply networks can provide the necessary level of coordination. Shared standards for digital thread tools and data can create a single source of digital truth from design through production and sustainment for key parts or even whole vehicles. The common standards can allow for rapid coordination between government and industry and among industry players. For example, if a new threat emerges at the tactical edge, government can quickly share the requirements for a solution with a large number of industry participants. Those participants can then not only distribute production among them based on who has capacity, but also break the product into component parts for parallel production with full confidence that all the parts will work together. This process can also be adjusted in real-time. If one producer is disrupted by a cyber attack, they can shift production to another, making the entire industrial base more responsive and more resilient.

Making necessary changes

While the concept of digital supply network may be new, the tools necessary realize it are not. In fact, they have been fueling the Fourth Industrial Revolution around the world. Still, to realize digital supply network at this scale requires new levels of military, government, and industry interoperability from the tactical edge to the defense industrial base.

1. **Interoperability in tactical data across military services and allies:** Delivering supplies to troops at the tactical edge requires data interoperability within militaries and between them. That is certainly not a new concept, but when facing a peer adversary, systems combat logistics requires interoperability be expanded beyond certain programs or applications and sit as the foundation of military logistics. Specifically, it will require the ability to seamlessly drive tactical data within and between militaries and other government organizations. It will also require integrated information systems that can share data across the joint and combined force based on need and clearance level. Finally, it will require the ability to visualize and tap into military and allied capabilities in real time.

2. **Interoperability in digital engineering across military and industrial base:** At the DIB level, interoperability is about being able to design, produce, and innovate across militaries, government, and industry partners. Here shared standards and the technologies of the digital threat, like computer-aided design, product lifecycle management, manufacturing execution systems and more, must be adopted by all actors required to supply and sustain a wartime effort. Otherwise the speed, flexibility, and resilience afforded by system combat logistics breaks down. For example, if militaries, government, and industry partners are not able to coordinate during the development of new innovative items, those products cannot be produced across the supply network.

3. **Digital backbone to connect tactical edge to industrial base:** Connecting the tactical edge to the defense industrial base requires a common digital backbone, or a single digital platform that combines operational and logistical data from the tactical edge to the military and enterprise data in the industrial base. There are several existing platforms within industry that manage data between produces, logisticians, and customers. Large e-commerce sites are an example; they sell their own products and act as a hub to connect other producers with consumers.

Logistics remains challenging, and it certainly becomes more fragile while under fire. Bringing allies and technology partners together through wargames is the last critical element. The goal of practice should be to test the connections and their resiliency between both technology and people that are the foundation of interoperability. The focus should not be on achieving a stagnate end state but the development of a system of military logistics that evolves as technology and adversaries do.

Through digital supply networks, modern militaries can deny adversaries the ability to disrupt wartime logistics and force opponents to reevaluate the likelihood of their victory. In this way, a resilient combat logistics system cannot only help a nation be prepared for war but may actually help deter one as well.

Endnotes

1. A Joint Warfighting Concept for Systems Warfare | Center for a New American Security (en-US) (cnas.org)
2. Gen. Hyten On The New American Way of War: All-Domain Operations - Breaking Defense Breaking Defense - Defense industry news, analysis and commentary
3. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp4_0ch1.pdf?ver=2020-07-20-083800-823
4. https://asianmilitaryreview.com/2018/10/the-mrap-story-learning-from-history/

Author

Alan Estevez
Specialist Executive, National Security and Logistics
United States
alanestevez@deloitte.com

Kelly Marchese
Lead Principal, Supply Chain and Network Operations
United States
kmarchese@deloitte.com

Adam Routh
Defense, Security & Justice Sector Research Lead
Center for Government Insights
United States
adrouth@deloitte.com

Joe Mariani
Senior Research Manager,
Center for Government Insights
United States
jmariani@deloitte.com

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organization") serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 312,000 people make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms or their related entities (collectively, the "Deloitte organization") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

© 2021. For information, contact Deloitte Touche Tohmatsu Limited.