Deloitte.

A report from the
Deloitte Center for Government Insights

Military interoperability in the intelligent age of 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.

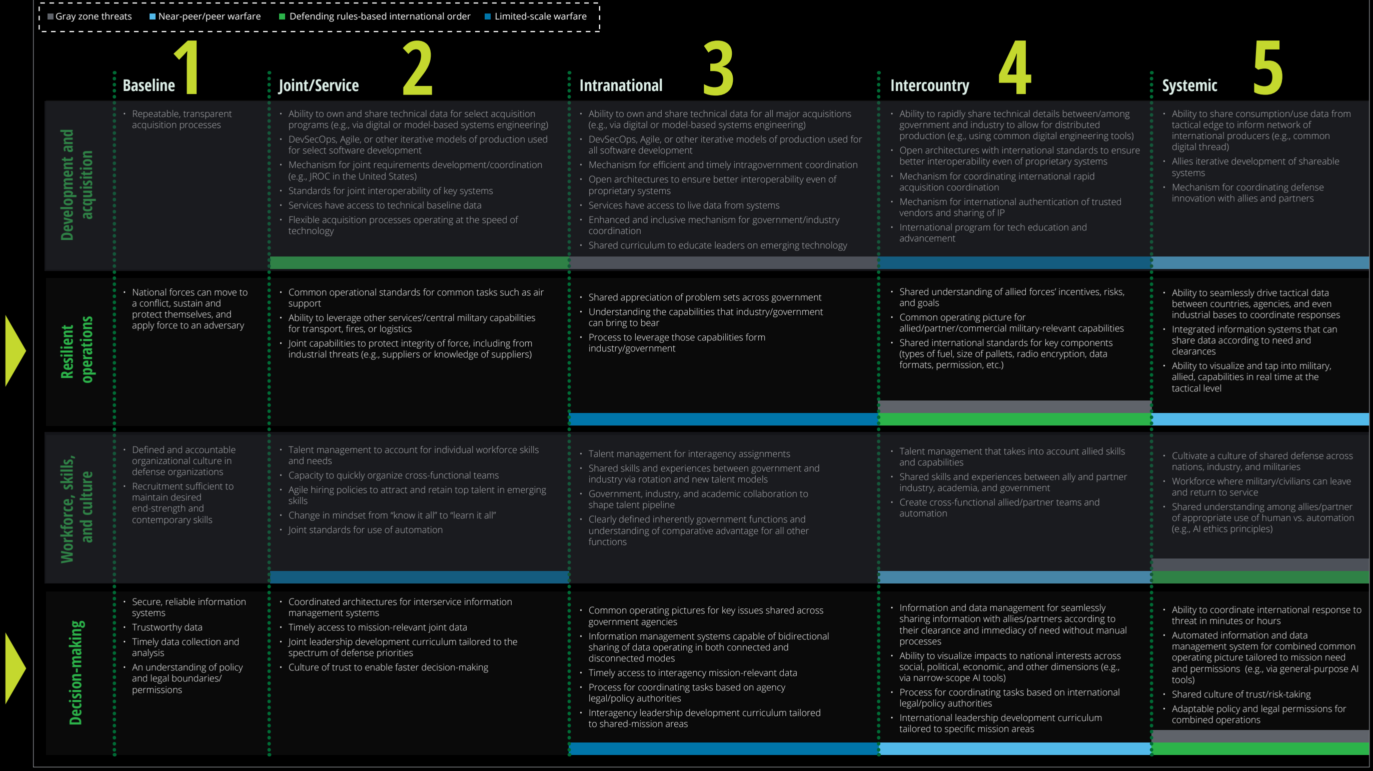
Future of Warfighting Interoperability Index

In focus: Resilient Operations and Decision-making

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

	Baseline 1	Joint/Service 2	Intranational 3	Intercountry 4	Systemic 5
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

A Future of Warfighting publication by Deloitte UK

Interoperability has become the cornerstone of successful military operations and the critical element for future military effectiveness against threats ranging from grey zone disinformation campaigns, to defending the rules-based international order, and peer warfare. Future conflict success will require rapid pace, precise understanding, quick decisions, and coordinated effects to disrupt enemy activity. Interoperability between departments, agencies, allies, and domains will deliver critical outcomes to achieve campaign goals faster at strategic and operational levels.

There is just one problem: current military interoperability is highly people intensive, and people are slower than machines. It takes enormous teams to create interoperability environments, staff the processes for effective integration, and create the tools and products that deliver the results. For example, completing a multinational 24-hour Air Tasking Order can require hundreds of people to plan and interact across domains, forces, and services, and the process is continuously repeated. It is a demanding and time-consuming activity that needs to be accurate and trusted or else the mission may fail.

Article elements

- Intelligent interoperability
- UK perspective

Key topics

- Intelligent Age Warfare
- Automated interoperability
- Common data and common tools

But is that the best use of human talent? Analyzing data points, deconflicting with other militaries, and planning logistics simply to provide air operations? And can such human-centric processes provide an advantage on a future battlefield suffused with data and where decisions need to be made faster than ever before? Arguably, no. To make interoperability the strategic and operational advantage we need it to be, we must automate more of it.

Combining automation and interoperability isn't new. Outside the military we are witnessing significant reductions in human activities in the current Intelligent Age as machines and automation replace human talent. Intelligent organizations are enhancing people with AI, where machines support all decisions, improving trust between humans and machines and their outcomes. But more than just automation, digital supply networks merge smart tools, like AI, with integration. Smart factories and production facilities are connected across borders in a manner increasingly necessary to keep pace with the rate of consumption and trade today. The combination of Intelligent Age machines, like AI, with Intelligent Age practices, like digital supply networks, has changed global commerce, and it can change warfare too.

We can see from industry examples that combining automation with interoperability requires the following:

- **Common data:** If stakeholders make their data discoverable according to access rights or classification, and that data is in common formats, then military partners can use that data to create automated tools that benefit all. For example, digital supply networks often rely on shared standards that allow production facilities and material suppliers to speak the same digital language. Without that common language, the digital supply network would be less digital or, in other words, less automated.

  For the military this means repurposing Information Age data-rich environments into practical, automated interoperability tools and processes. Modern militaries are endeavouring to exploit these data pools at a faster pace, but in isolation. Most still see data as a function by itself rather than a conduit to more significant interoperability gains. The military needs to move from the Information Age thinking to Intelligent Age thinking by deliberately linking interoperability with data.

- **Common tools/platforms:** Common data is necessary but not sufficient by itself. Common data can mean that patterns speak the same language, but it doesn't mean that they can act in the same way. To turn a common language into common outcomes requires common tools. Disparities in tools can reduce the efficiency of a partnership down to the lowest common denominator. For example, in a digital supply network a manufacturer of devices may have the tools to adjust production in real-time based on demand, but unless the manufacturer's parts supplier also has the tools to ramp-up production based on demand, the manufacturer won't have the necessary materials to increase production regardless of its tools or demand. Common platforms for data sharing, tool development, and use allow military and civilian partners to quickly share not just data, but entire tools that allow whole networks to operate at the same speed.

  For defense groups this starts by reducing complexity and conflict across organizations with an increased commonality of data, tools, and processes. Even simple interoperability and automation will fail without shared common platforms. Military time and effort need to be devoted to improving interoperability as well as improving tool functionality.

Joining automation and interoperability will afford two key advantages. First, people's time will be freed up to ensure that the valuable human elements of integration such as trust, relationships, assurance, and allyship can be emphasized by individuals. These are all skills where machine learning struggles and fails. Equally, automated processes and tools working across domains, departments, and national information systems will complete faster decisions, blending insight with intelligence to deliver greater combined effectiveness.

Making it real

Turning current military interoperability practices into the ones necessary for Intelligent Age warfare requires addressing changes across people, process, and technology.

People

Culturally, Defense should adopt wide recognition that both increased integration and automation are the future to improving the delivery of military effects and outcomes. Too many military leaders see these two measures as separate options. Militaries need to align integration with automation consciously across all domains and services and partners, including industry; and fight hard to prevent isolated thinking or secluded developments.

Process

To be an interoperable organization, Defense should scale its automation processes across and outside itself, recognizing that there is more power beyond its own organizational processes. The default military plan is to create an insular 'uber-programme' to define, design, and deliver everything at once. But such a process poses a major risk to interoperability and automation because they are detached from outside innovations and efforts. The true need is for an incremental, agile process that enables programmes to establish shared tools and procedures in a way that connects them with other programmes in other organizations. Together, a more agile and inclusive process can tap into shared knowledge to permit new innovations and collective change.

Technology

Defense should assess the value of technologies based on how compatible they are in a plug-and-play system. Interoperability and automation do not often work on isolated technologies. Even the most advanced 5th-generation aircrafts will offer limited advantage if they are disconnected from a broader automated interoperability architecture. Early identification of shared opportunities and development solutions across the MOD and with allies and partners can aid in finding or developing plug-and-play technologies that enable a more automated interoperability.

Intelligent Age warfare needs an innovative approach to interoperability. It needs an approach that folds in automation across key functions and domains. To do this requires simplifying and reduce toolsets, allowing for development of solutions on commonly understood platforms rather than bespoke and outdated single-purpose systems. It needs a mindset that prioritizes the principles of interoperability first, from concept design through to delivery of effect. Above all, it means applying thinking for the Intelligent Age, rather than the Information Age.

Author

Tony Reeves
Lead Partner, Digital Defence
United Kingdom
treeves@deloitte.co.uk

Deloitte.

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.