SEPTEMBER 2023

THE RACE FOR DATA SUPREMACY

Achieving decision advantage to deter future conflicts

OXFORD ECONOMICS

Report Sponsored by IBM

The race for data supremacy: Achieving decision advantage to deter future conflicts

Victory in future wars will increasingly depend on which side most swiftly gathers strategic insights from data and is able to deploy them, from headquarters and the tactical edge and throughout the battlespace in real-time combat conditions. Without an urgent transformation in the military's ability to synthesize and distribute information through a secure data architecture, the US and its allies could lose their ability to deter or win potential conflicts as rival nations develop their own capabilities.

"If I can own the data on the battlefield, then I'm five steps ahead," says former US Air Force Major General Robert Wheeler, one of several leaders across NATO and the Five Eyes nations interviewed for this paper. "I need this data timely, I need it accurate, and I need it across the battlefield."

Yet the US military and its allies in NATO and Five Eyes[1] have not moved quickly enough to make these essential capabilities available. And as the revolution in data science, sensors, autonomous assets, and Artificial Intelligence (AI) continues, the risks of losing decision advantage multiply. With data sources rapidly proliferating, agile software and integrated information delivery systems, like a data fabric architecture, will transform deterrence and create decisive advantages for the forces that deploy the best data fastest. The only question is who will seize this strategic high ground.

The pace of transformation is daunting. Other nations, including China and Russia, continue to invest heavily in emerging and disruptive technologies. In some areas, like electronic warfare, facial recognition, and certain IT hardware, they may be developing meaningful advantages. Indeed, many observers believe that the capability gap the NATO allies traditionally enjoyed relative to potential adversaries could be eroding.[2] And as the use of enterprise-level generative AI to unlock insights and fortify decision advantage advances, the demand for a robust data fabric to manage the kinds of data being propagated will become ever more critical.

While military hardware and well-trained troops will remain essential, defense officials must broaden their focus on warplanes, ships, and artillery to include superiority in the processing, analysis, governance, and deployment of data as key measures of combat readiness. And when information flows at the speed of light, many of the current systems of command and control are too plodding to gather and communicate pertinent data that can identify and neutralize emerging threats.

"A disruptive jump in generational capabilities is what is needed today if we're going to go up against China," Wheeler warns. The networks of the future will have to integrate weapons platforms from across all services and allies, from space to undersea, and "find, fix, track, target and destroy multiple targets in near real time, while on the move."

The conflict in Ukraine has demonstrated how an agile military using commercially available satellite communications, mobile internet towers, low-cost drones, cellphone videos and open-source software can fuse data relatively seamlessly and carry out

[1] i.e., Australia, Canada, New Zealand, the United Kingdom, and the US.
[2] https://cepa.org/comprehensive-reports/elevating-our-edge-a-path-to-integrating-emerging-and-disruptive-technologies.

precise combat operations. Ukraine was able to develop its data-driven warfighting assets quickly, but replicating that success across multiple large military establishments will be a bigger job. "Most NATO countries might need around 10 years to forge similar progress at 10 times the price and with less functionality," says Nico Lange, chief of staff for the German Defense Ministry until 2022.[3] And a conflict with China would likely be far more complex and dispersed across a far larger geographic footprint.

To accelerate development of expertise in data-driven combat and match the speed of technological advances taking place in the commercial world, defense organizations must put aside the "not invented here" mindset common in the defense industry and collaborate more intensively. Classification and security remain crucial, but military leaders could benefit by taking cues on data management and digital innovation from the private sector, where companies thrive on competition and rapid iteration.

Industry also has a role to play, as contractors and developers can do far more to improve interoperability of the various data types—including metadata—collected. Agreeing to some basic standards could help defense agencies rapidly improve the usefulness of their data, much of which is not being used effectively.

Collecting, cleansing, securing, and extracting significance from data is difficult work, and sharing it across several countries and continents is a challenge even in peacetime—and these systems need to function under combat conditions where normal communications networks and access to the cloud will be impeded.

How can the US and its allies move quickly to create sustainable decision advantage? Key steps include the following:

- **Develop a shared master strategy** for data governance, architecture, deployment, and use. This will require more willingness, earlier, for the US military and its alliance partners to communicate and collaborate on an ongoing basis to develop true interoperability.
- **Create a joint allied taskforce, including industry, focused on data system integration** that can rapidly develop a comprehensive data architecture to govern multi-domain operations consistent with the US military's Joint All Domain Command and Control (JADC2)/Multi Domain Integration initiatives.
- **Build a standard for data integration** that builds on hybrid cloud and data fabric technologies and that uses dynamic data architectures that are backward compatible and widely accessible. This will likely involve moving to a Software as a Service (SaaS) model, using more off-the-shelf hardware, and decreasing reliance on specialized built-to-purpose software.
- **Start with small systems and scale up,** not with giant, complex systems that take years to deploy. Incorporate the "minimum viable product" model used in the private sector to speed testing of new systems, and then scale.
- **Consider new recruiting and on-boarding options aimed at attracting top IT talent** into the military's ranks to translate high-level visions of data integration into on-the-ground reality.
- **Use private sector innovations and resources** in a purposeful way that respects national interests.
- **Encourage industry to be more open** to allowing employees to work with government defense agencies for dedicated periods.

Making all of this happen is a formidable challenge, but there are no alternatives in a dangerous world with near-peer rivals and unpredictable asymmetric enemies. While data is critical for every phase of defense strategy, from planning and readiness to deterrence, this paper focuses primarily on the imperatives, opportunities, and challenges of creating decision advantage by getting the right data to and from commanders to the tactical edge using data fabric architectures.

[3] Nico Lange, "How to Beat Russia: What NATO armed forces in NATO should learn from Ukraine's homeland defense." https://www.globsec.org/what-we-do/publications/how-beat-russia-what-armed-forces-nato-should-learn-ukraines-homeland.

Planning for an uncertain future

In the two decades since the September 11 attacks, the US and its NATO allies focused primarily on counterinsurgency campaigns in combat zones like Afghanistan and Iraq. As a result, "we underinvested in command and control for 20-odd years," said Lt. General Michael Vetter, Director General Cyber/IT and Chief Information Officer at the German Ministry of Defense in Berlin.

The war in Ukraine opened many eyes to the potential for conventional warfare to explode suddenly between militaries with advanced weaponry. Amid a changing geopolitical environment, allied defense establishments have rapidly begun to adapt to the new realities of preparing for potential conflicts against well-resourced, technologically advanced peer or near-peer competitors, who also boast top-tier weapons and sophisticated data capabilities.

Acknowledging this changing strategic landscape, the Pentagon and NATO have identified the information domain as the next battlefront in conventional warfare. War planners now recognize that advanced processing and data analysis—and the ability to rapidly communicate data to the edge—can yield decision advantage should conflict arise.

To reflect this new thinking, in March 2022 the Pentagon articulated a Joint All Domain Command and Control (JADC2) framework. The Pentagon has defined JADC2 as a "warfighting necessity" and "an approach for developing the warfighting capability to sense, make sense, and act at all levels and phases of war, across all domains, and with partners, to deliver information advantage at the speed of relevance."[4] The allies have programs with similar objectives in place.

Yet achieving decision advantage using advanced Information Technology requires much higher levels of interoperability across systems, more robust data sharing, and redundancies to ensure data can be delivered after networks are compromised in combat. "Being able to own the data on the battlefield with a non-traditional approach with edge processing that is secure… even when networks are compromised… that is where we need to be going," Major Gen. Wheeler said.

Implementing such strategies will require a major transformation in military culture and mindset.

[4] US Department of Defense, "Summary of the Joint All Domain Command and Control Strategy," March 2022.

Rethinking war and deterrence

The need to develop common standards across the services that align the US military with its allies in NATO and Five Eyes poses a huge test for large organizations that have traditionally created their own technological solutions to resolve issues each believes are service-specific.

Currently the US Army has unveiled Project Convergence, the Navy has announced Project Overmatch, and the Air Force has awarded contracts for its Advanced Battle Management System (ABMS), while the Marine Corps has acknowledged in its most recent Force Design 2030 update the service's legacy command-and-control systems are stove-piped and need to be modernized.[5]

And while it is well recognized that the needs of fighter pilots are not the same as those of submarine commanders, the need for interoperability among systems will only grow in importance. A recent study by the Government Accounting Office (GAO) noted that the Defense Department has not yet determined exactly what existing and future desired capabilities will be needed to realize its vision for JADC2 and was in the process of identifying a variety of implementation challenges.[6]

The military services will need to move away from a focus on hardware-centric solutions to upgrades that incorporate a Software as a Service model to encourage new levels of data-sharing and interoperability that can operate at the speed of mission. A recurring theme across interviews with defense experts is that a system of plug-and-play interoperability cannot take hold if each service branch or NATO ally takes its own route toward developing a data architecture.

"The central challenge is creating true interoperability across each of the services and with partners and allies," said Rear Admiral (ret.) William Metts, former INDOPACOM Director for Intelligence. "We tend to operate with and from different IT communications networks, and historically those communications networks have not enabled the sharing of information easily."

Metts says the military needs to consider leveraging the technological innovations being pioneered in private industry to rapidly integrate data across services and partners. In its initial iteration, many of the services focused on the communications component of JADC2, said Rear Adm. Eric Ruttenberg, reserve director for Maritime Operations, United States Pacific Fleet and a former chief engineer, Naval Information Warfare Systems Command. "It took us about two years to understand that it's not the networks that are so important, it's the ones and the zeros—the data—that goes over that network that's critical."

In addition, achieving military advantage based on information technology demands a new kind of data architecture, where data housed in a variety of locations and formats can be cleansed, sifted, and distributed even while maintaining needed security classifications. Likewise, a data-centric capability demands redundancies at the edge through virtualization, to overcome network disruptions that would likely take place during combat. In a data-centric system of defense, agility, resilience, speed, and mobility may well prove decisive.

"That's why data fabric is critical," Ruttenberg said. "Because that's what's going to drive not only the resiliency that we need in networks, but also in how we develop and deliver applications that sit on the network."

[5] https://defensescoop.com/2023/06/05/force-design-2030-c2-data.
[6] US Government Accountability Office, "Battle Management: DOD and Air Force Continue to Define Joint Command and Control Efforts" GAO-23-105495, published January 2023.

What is data fabric?

Data fabric is an architectural framework that aims to provide a unified and consistent view of data across different systems, platforms, and data sources within an organization. It focuses on creating a centralized data layer that connects various data silos and enables seamless data access and integration across the enterprise at scale.

Data fabrics pull together data from legacy systems, data lakes, data warehouses, SQL databases, and apps to provide a holistic view created from a variety of data sources.

Some key features of a data fabric include the following:

- Virtualization techniques to abstract the underlying data sources and provide a unified interface for accessing and querying data.
- Integration of disparate data sources by establishing connections, transforming data formats, and ensuring data consistency.
- Governance mechanisms to ensure data quality, security, and compliance across the organization.
- Observability, including tools and processes for managing data workflows, data pipelines, and data transformations.

Maj. Gen. Rob Collins, the Army's program executive officer for command, control, communications–tactical (PEO C3T), described data fabric this way:

"We have to make sure that we've got a fabric that can ingest all the data, make sure it is understandable, it's interoperable, and it's trusted. Then, on the other end, we have to make sure it's discoverable," Collins said. "We're now trying to pivot toward a more federated data environment. You can discover data, you can exchange data based on the need for that data, and you're able to articulate and mark data to the attribute level."[7]

[7] https://federalnewsnetwork.com/cme-event/federal-insights/ask-the-cio-army.

While time is short to develop a shared data architecture, there is growing awareness that the Western allies need a secure data fabric architecture that can link a variety of data sources across multiple hyper scalers and on-premise centers, in multiple data formats, while controlling access, protecting secrecy, and preserving sovereignty.

"Data is a strategic resource, and we need to really get our act together to make better use of all the data that's within the organization," Lt. General Vetter said. "We must find instruments to bring structured and unstructured data together, and we need to provide a common operational picture, especially on the NATO level, to coordinate joint effects. This would be a huge step forward."

Success factors for a changing mission

The emerging paradigms of data-centric warfighting will demand other changes in the Pentagon's long-standing methods of operations.

Traditionally, storing and archiving data was considered a cost of operation, not a strategic asset, notes retired Air Force Major General Brian Dravis, who was a senior leader at Defense Information Systems Agency (DISA) and director of the Joint Service Provider organization within the Pentagon. "Data literally was much more of a liability than an asset," he said, because enormous amounts of old data had to be stored and archived in server farms that demanded electricity to keep them cool, staff to maintain the facility, and protocols to ensure the data remained secure, even if much of it was never actually used.

Today's aspiration, by contrast, "is to flip that upside down," Dravis said, and "use things like machine learning, AI, automation, all of those rapidly evolving attributes to leverage the insights from that data to get you to a place where you can actually use it for decisional advantage." The challenges of this transformation are immense. "It's not a trivial thing to move from a massive anchor that is literally a cost center, into being a decisional advantage attributable thing that you have high confidence in."

Creating a unified, interoperable data architecture would also allow military services to actually make use of the volumes of data it already collects, from both structured and unstructured data sources, and create governance tools to make sure the data being analyzed is accurate.

As currently configured, experts say, a vast majority of data cannot be adequately mined for meaning. "I wouldn't be surprised if greater than a 90th percentile of the data, particularly the unstructured data, is not providing value to the commanders who face strategic and operational-level decisions," said Dravis. "We need to be able to make good decisions faster than our enemies."

Likewise, differences in classifications systems across US military services and between the US and its allies can serve as a barrier to true interoperability.

The same challenge confronts the UK, says Dr. Timothy Robinson, chief data architect for the Ministry of Defense. Various services work in silos, and are "very risk averse," when it comes to changing processes to boost interoperability. "Our data is messy and complex, and we can't get it out to the user quickly enough," he said. Interoperability isn't necessarily considered a priority, because "people just don't want to actually let the data out of their zone of control."

To better analyze the enormous amounts of data it collects, the services will increasingly rely on machine learning and advanced AI systems. But experts note additional steps are required to ensure the data being analyzed is reliable, authentic, and accurate, so new standards of data governance and grooming will also be needed. "You need a guarantee of the authenticity of the data that informs machine learning, and therefore AI and automation that leads to decision superiority, Dravis said. "Data provenance is often overlooked, but it's becoming increasingly important."

Implementing these new data requirements will require another change in mindset: moving from a system where operations, cryptographic, and classification systems are updated through hardware to systems that can be defined and updated via software, much as the software running a Tesla electric vehicle is updated over the air via Wi-Fi. Open-mission software that is backwards—as well as forward—compatible can update command and weapons systems more rapidly and at lower costs.

Working more closely with allies

The Ukraine conflict has also reinforced the notion that US defense forces must work more closely with their NATO and Five Eyes partners. Yet issues regarding data-sharing and interoperable data architecture and even adopting common definitions of data among the allies are not yet fully resolved.

Major Stephen Nelson, program director for the NATO Next Generation modeling and simulation division, notes that not all NATO nations have agreed on a common set of terrain names for vast areas of the sea between the Mediterranean and the Black Sea. "Can we develop a terrain data model that all 31 nations, and potentially 32, can agree upon?" he asks.

Moreover, while European nations may share data regarding potential enemy—so-called "red team"—threats, "nations are also jealous about sharing their blue team information. So, we probably have less of a realistic look at blue data than we actually do on red data."

In organizing a comprehensive multi-domain approach, "you have to have data that's flowing both ways," Nelson said. "So, what you're going to see with NATO" and other allies "is nations can access NATO data, but it's not a bidirectional gate. And they're only going to give so much back."

Leaders in Europe are anxious to align with US efforts at creating deep data interoperability, but also must take steps to shore up their internal operations.

In Germany, "interoperability is one of our top priorities, and with regard to data and data standards we are one of the most outspoken advocates of the federated mission network approach within NATO to make sure that we have standards, protocols in place that enable us to work together and share information even if we are operating on different information systems," General Vetter explained.

Vetter argues that the German defense forces can be more agile in their decision-making and implementation of new data management architectures because they lack the scale of the US military.

However, "once the Americans would decide on a common architecture, and would agree on the plan to implement it, we will be surprised how quickly they will be doing this. It takes some time until the American machine is up and running. But when it's running, you'd better get out of the way."

Dutch Air Force Colonel Talitha Born, deputy director for information-driven decisions, says while the Dutch military endorses the idea of a data fusion architecture that can lead to multi-domain authoritative decision-making, more investment must be made in the basic information backbone as well as in the mindset governing NATO allies. "We need cognitive dominance as NATO. We need to invest in information integration across the board," she said. "Sound initiatives are on their way, yet we still have a long way to go."

From concept to implementation

The Ukraine conflict has dramatized the need for NATO member countries to invest more to address shortcomings in managing their own data architecture, Col. Born noted, even as they await a more unified definition from the US military.

While the Dutch military is investing heavily in strengthening its data backbone and developing greater integration of data streams that were formerly fragmented, it recognizes the necessity to follow whatever data architecture the US Pentagon eventually settles on. "We cannot close our eyes on this," she said. "It's crystal clear that we must follow the US in certain ways because our weapons systems come from the US in large part. So you cannot ignore the opportunity to embrace the possibilities of an F-35, and only the Americans have that."

Among data experts interviewed, there is a growing recognition that getting mission-critical data to the edge will require data virtualization and redundant communications networks, even using 5G or 6G technologies when more conventional cloud-based networks are disrupted. But some worry whether the services have the talent necessary to help build these systems.

Robinson, of the British MOD, fears that a real deficit in technical skills within the military's own IT services will make it difficult for his government to actually implement the utopian vision of data sharing articulated at senior command levels. "We can't match the private sector pay, so we don't get the best people coming in," he says, while those who become well trained are often transferred to other divisions within too short a time.

Many also express the traditional complaint that the way military services acquire new technologies hampers their ability to stay on the cutting edge. "There are no venture capitalists in the Defense Department," Dravis said. The Pentagon needs to "find a way to iterate and test new concepts without having to jump through all the security hoops for development."

Maj. General Wheeler notes that, in addition to a lack of data engineering talent within the Pentagon to implement new paradigms around data architecture, the procurement officers who must approve acquisition also lack sufficient technical background. "The acquisitions people don't have operational experience using these systems," he noted. "When the guy that's buying this stuff doesn't understand how it will be used, it becomes a problem."

This is especially true when it comes to data fabric, which is becoming better understood as a foundational data architecture to allow rapid dissemination of mission-critical data.

"I'm framing it as 'time to value for data,'" MOD's Robinson said.

"It's about being able to get your hands on the data you need much more quickly and to move it around more quickly. But that means you must build the pipelines to do it, and you have to be able to build those pipelines quickly," which means developing low-code solutions and data visualizations.

In the new world where interoperability, resilience, mobility, and speedy decision-making are becoming "must have" assets to deter conflict, experts agree that a multi-domain data fabric architecture, combined with a distribution system that offers multi-level

security protocols, can rapidly improve the data landscape at the edge. This agile new architecture can also yield cost savings when advanced commercial technologies, already deployed, are adapted to the security needs of the military.

And while the military must directly confront its need to quickly establish greater interoperability, its private-sector partners in the defense, communications, and IT industries should also take more concrete steps to lower barriers for data sharing among hyperscalers, and between various software database and operational suites.

This array of sophisticated systems "requires you to change the way you do business," Maj. General Wheeler said. "But the only way we're going to survive and prevent the next fight, hopefully never have to fight it—and if we have to fight it, win it—is by having these kinds of fabrics. So, this is not anything that's futuristic. It is just getting people together to understand it."

Calls to action

To accelerate true data interoperability and enable decision advantage at the tactical edge, defense officials in the US and its NATO and Five Eyes allies should consider the following:

- **Treat data as seriously as any weapons system.** Create a classification of "data officers" that mirrors the responsibility of weapons control officers.

- **Prioritize the establishment of a joint data task force** to establish a unified data architecture that will govern multi-domain operations for the US and its allies in NATO and Five Eyes.

- **Convene a military-civilian working group to collaborate with key IT partners,** including cloud providers and software companies, to develop standards of interoperability that can accelerate data sharing, using commercial technologies while still maintaining necessary level of cryptographic and data security principles.

- **Place a greater priority on issues around data governance and reliability.** As the conversation around AI will inevitably accelerate, so will the need to ensure that all data sources are authentic and reliable.

About Oxford Economics

Oxford Economics is the world's foremost independent economic advisory firm. We specialize in evidence-based thought leadership, forecasting, and economic impact analysis. Headquartered in Oxford, with offices around the world, we employ more than 400 people, including over 250 economists, industry experts, and business editors. The rigor of our analysis, caliber of staff, and best-of-class global economic models and analytical tools make us a trusted resource for decision-makers. Oxford Economics has a worldwide client base of over 2,000 corporations, financial institutions, government organizations, professional firms, and universities. Visit www.oxfordeconomics.com to learn more.

About IBM

IBM is a leading provider of global hybrid cloud and AI, and consulting expertise. We help clients in more than 175 countries capitalize on insights from their data, streamline business processes, reduce costs and gain the competitive edge in their industries. More than 4,000 government and corporate entities in critical infrastructure areas such as financial services, telecommunications and healthcare rely on IBM's hybrid cloud platform and Red Hat OpenShift to affect their digital transformations quickly, efficiently and securely. IBM's breakthrough innovations in AI, quantum computing, industry-specific cloud solutions and consulting deliver open and flexible options to our clients. All of this is backed by IBM's legendary commitment to trust, transparency, responsibility, inclusivity and service. Visit www.ibm.com for more information.

OXFORD ECONOMICS

Report Sponsored by IBM