Image source: Gorodenkoff via iStock

WHITEPAPER

Achieving Decision Dominance in U.S. Military Operations

EVERFOX

“The complexity of modern warfare requires the coordination of disparate military branches, units, and allied forces, each with its own systems, protocols, and often, cultures.”

Achieving Decision Dominance in U.S. Military Operations

Decision dominance—the ability to make faster, better decisions than adversaries through integrated, multi-domain operations—is crucial to addressing persistent threats from near-peer adversaries. The Department of Defense (DOD) and its industry partners are diligently working on the primary challenges that influence decision dominance.

The following pages explore some of these myriad challenges in achieving decision dominance as well as potential solutions.

Data management and sharing

Data is the backbone of every decision—good data leads to effective decision-making, and incomplete data creates blind spots. Achieving true decision dominance requires consolidation of real-time data that is often spread across a multitude of different components, services, systems and people.

The DOD generates more than 22 terabytes of data daily, primarily for IT systems[1]. Developing standardized data-sharing interfaces and robust network capabilities is critical to have any hope of extracting actionable intelligence from that much data. The Joint All-Domain Command and Control (JADC2) initiative aims to address these data management and sharing issues but will require significant transformational changes within the DOD, including modernizing networks and data management systems[2]—with the result of increasing interoperability, shortening the sensor-to-shooter timeline, and enhancing decision dominance.

In June 2024, the Pentagon's Chief Digital and Artificial Intelligence Office (CDAO) announced another concept that would aid the DOD in managing and sharing data—the Open Data and Applications Government-owned Interoperable Repositories (Open DAGIR). Open DAGIR offers an approach to scaling data, analytics, and Artificial Intelligence (AI) capabilities. According to the CDAO, it will be a "multi-vendor ecosystem with supporting business models that enables industry and government to integrate data platforms, development tools, services, and applications in a way that preserves government data ownership and industry intellectual property."[3] The DOD will initially use the Open DAGIR ecosystem to support the data infrastructure and applications that will enable JADC2.

Image source: Liubomyr Vorona via iStock

Key Data Management and Sharing Challenges

Legacy Systems
Many existing systems are outdated and incompatible with modern data-sharing technologies, leading to inefficiencies and delays in critical information dissemination.

Standardization
A lack of standardized data-sharing protocols across military branches hampers interoperability and coordinated decision-making.

Network Capabilities
Upgrading network infrastructure to support real-time data sharing is essential but requires substantial investment and strategic planning.

Potential Solutions

Network Modernization
Investing in the latest networking technologies to enhance data transmission speeds and reliability.

Standardized Protocols
Developing and implementing universal data-sharing protocols across all military branches to ensure seamless interoperability.

Advanced Data Management Systems
Deploying data management systems capable of handling large volumes of data efficiently and securely.

Image source: Standret via iStock

Technological integration

Integrating advanced technologies such as AI, machine learning (ML), and 5G communications into DOD systems is essential for achieving decision dominance—these are the technologies that make analyzing and disseminating massive amounts of data quickly possible. The challenge lies not in getting buy-in on these technologies, but rather in the timing of implementation and the need for them to integrate with other systems. With the colossal number of formats, networks and systems that data is spread across, integration becomes a daunting task.

To address this challenge, projects like the U.S. Army Futures Command's Project Convergence are experimenting with and implementing these technologies. For example, the Project Convergence Capstone 4 experiment is integrating an extensive communications network[4]. The Capstone 4 mission scenarios are helping the military identify challenges and opportunities to improve integration of new technologies and tactics into network communications to accelerate data exchanges, which will ultimately support real-time decision-making.

Integration Challenges

Research and Development
High costs and long development timelines can delay the deployment of critical technologies.

Technological Compatibility
Ensuring new technologies are compatible with existing systems and platforms is a complex and ongoing challenge.

Training and Adoption
Adequate training for personnel to effectively utilize new technologies is essential for maximizing their potential.

Potential Solutions

Investment in R&D
Increasing funding for research and development to accelerate the introduction of new technologies.

Interoperability Standards
Establishing clear standards for technological integration to ensure new tools can work seamlessly with existing systems.

Comprehensive Training Programs
Developing extensive training programs to ensure all personnel can effectively use new technologies.

Cybersecurity and data security

Faster networks sharing actionable data must also be secure and capable of deterring extremely sophisticated adversaries. The use of AI and ML introduces new vulnerabilities that adversaries could exploit. Building a secure and resilient network infrastructure is crucial to ensuring the integrity of decision-making processes. The threat from near-peer adversaries as they explore their own decision dominance will continue to evolve.

The CDAO's Open DAGIR initiative is one step toward accelerating the adoption of secure data practices and AI to generate decision advantages. In addition, DOD's 2024 Defense Industrial Base Cybersecurity Strategy calls for public-private cybersecurity collaboration[5]—a key initiative to benefit from private sector innovation.

Moreover, the DOD's commitment to a zero-trust security architecture by 2027 involves leveraging AI to streamline implementation processes and ens ure continuous security enhancements[6].

Cybersecurity and Data Security Challenges

Evolving Threats
Cyber threats are constantly evolving, requiring continuous updates to security protocols and technologies.

AI and ML Vulnerabilities
The integration of AI and ML introduces new attack vectors that adversaries can exploit.

Resource Allocation
Ensuring sufficient resources are allocated to cybersecurity efforts is crucial for maintaining a robust defense posture.

Potential Solutions

Continuous Monitoring and Updating
Implementing systems for real-time monitoring and regular updating of cybersecurity protocols.

Secure AI/ML Practices
Developing best practices for the secure implementation of AI and ML technologies to mitigate vulnerabilities.

Dedicated Cybersecurity Resources
Allocating dedicated resources and personnel to focus on cybersecurity initiatives.

Operational complexity and interoperability

The complexity of modern warfare requires the coordination of disparate military branches, units, and allied forces, each with its own systems, protocols, and often, cultures. In June 2024, the Pentagon released Fulcrum—the DOD's Information Technology Advancement Strategy[7]. The Fulcrum strategy aims to create a more integrated and cohesive fighting force by addressing interoperability challenges through standardization, joint training, unified systems, and strong cybersecurity measures. It is a blueprint to drive interoperability and integration in information technology across the DOD and emphasizes ensuring future capabilities align with warfighter needs.

In addition, programs like the Missile Defense Agency's Command Control Battle Management and Communications (C2BMC)—which dynamically integrates and coordinates ballistic missile defense assets to increase system performance throughout the battlespace—aim to provide a unified strategic view of the battlespace. While integrating these systems across different domains has been a formidable task, there is hope that Fulcrum will provide the roadmap needed.

Operational Complexity & Interoperability Challenges

Diverse Systems and Protocols
Different branches and allies use varying systems and protocols, complicating efforts to achieve interoperability.

Operational Coherence
Coordinating operations across multiple domains and forces is complex and requires advanced planning and communication.

Technology Integration
Integrating new technologies into existing frameworks without disrupting operations is a significant challenge.

Potential Solutions

Unified Command Systems
Developing and implementing unified command systems that can integrate data and operations from multiple branches and allies.

Interoperability Training
Conducting joint training exercises to improve interoperability and operational coherence among different forces.

Advanced Planning Tools
Utilizing advanced planning and simulation tools to better coordinate multi-domain operations.

Image source: Gorodenkoff via iStock

Final thoughts

Looking ahead, the future of U.S. national security hinges on the continuous pursuit of innovation to drive decision dominance. As the nature of warfare evolves, so must the DOD's approach to managing data, integrating advanced technologies, securing cyberspace, and achieving interoperability. The challenges are significant, but they are not insurmountable.

To stay ahead of near-peer adversaries, the U.S. military must continue to embrace a forward-thinking mindset, investing in cutting-edge research and development to harness the full potential of AI, machine learning, and advanced communications. By building robust and resilient networks, the military can ensure the integrity and speed of decision-making processes, even in the face of sophisticated cyber threats.

Interoperability across disparate military branches and allied forces will be critical, requiring concerted efforts to standardize systems and protocols. Innovative programs and initiatives, such as JADC2 and Project Convergence, will play pivotal roles in achieving seamless integration and operational coherence.

Ultimately, maintaining decision dominance will require unwavering commitment to collaboration with industry partners, leveraging their expertise and capabilities to drive technological advancements. By fostering a culture of innovation and continuous improvement, the U.S. military can secure its strategic advantage and ensure national security in an increasingly complex and contested global landscape. The road ahead demands resilience, adaptability, and a relentless focus on technological superiority, but with these elements in place, the U.S. can navigate the challenges and seize the opportunities of the future.

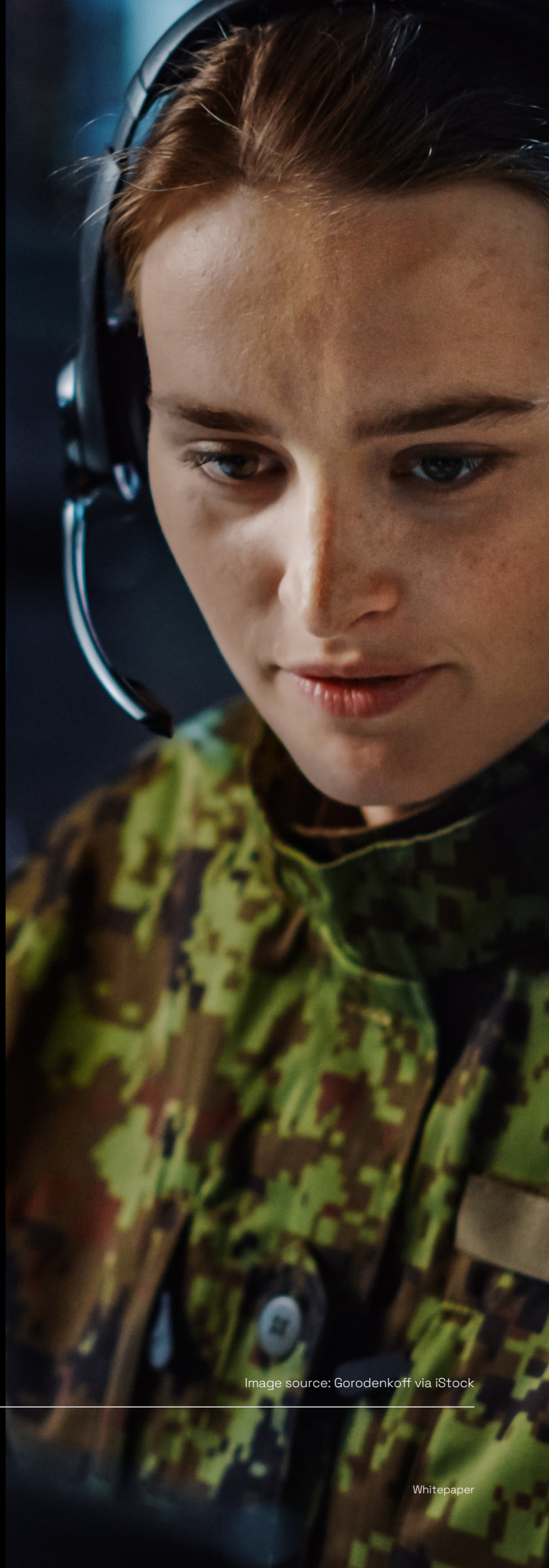

Image source: Gorodenkoff via iStock

Citations

1 - Rinderer, Egon. “Democratize Data for Decision Dominance.” National Defense. October 13, 2023. https://www.nationaldefensemagazine.org/articles/2023/10/13/democratize-data-for-decision-dominance

2 - LTC Brittany Lloyd, USA, & 2LT Jeremiah Rozman, PhD, USA. “Achieving Decision Dominance Through Convergence: The U.S. Army and JADC2.” AUSA. February 2022. https://www.ausa.org/publications/achieving-decision-dominance-through-con- vergence-us-army-and-jadc2

3 - Press Release: “CDAO Announces New Approach to Scaling Data, Analytics and AI Capabilities.” Department of Defense. May 30, 2024. https://www.defense.gov/News/Releases/Release/Article/3791829/cdao-announces-new-approach-to-scal- ing-data-analytics-and-ai-capabilities/

4 - Army Spc. Jackson Gray, 24th Theater Public Affairs Support Element. “Network Capability Provides Successful Start to Project Convergence Capstone 4.” Department of Defense. March 1, 2024. https://www.defense.gov/News/News-Stories/Ar- ticle/Article/3692858/network-capability-provides-successful-start-to-project-convergence-capstone-4/

5 - Defense Industrial Base Cybersecurity Strategy 2024.” Department of Defense. March 21, 2024. https://media.defense.gov/2024/Mar/28/2003424523/-1/-1/1/DOD_DOB_CS_STRATEGY_DSD_SIGNED_20240325.PDF

6 - Woolf, Tony. “How DOD Can Maintain Zero-Trust Momentum.” FedTech. April 19, 2024. https://fedtechmagazine.com/article/2024/04/how-dod-can-maintain-zero-trust-momentum

7 - Clark, Joseph. “DOD Releases Strategy to Achieve IT Integration, Interoperability.” DOD News. June 25, 2024. https://www. defense.gov/News/News-Stories/Article/Article/3817169/dod-releases-strategy-to-achieve-it-integration-interoperability/

Achieving Decision Dominance in U.S. Military Operations

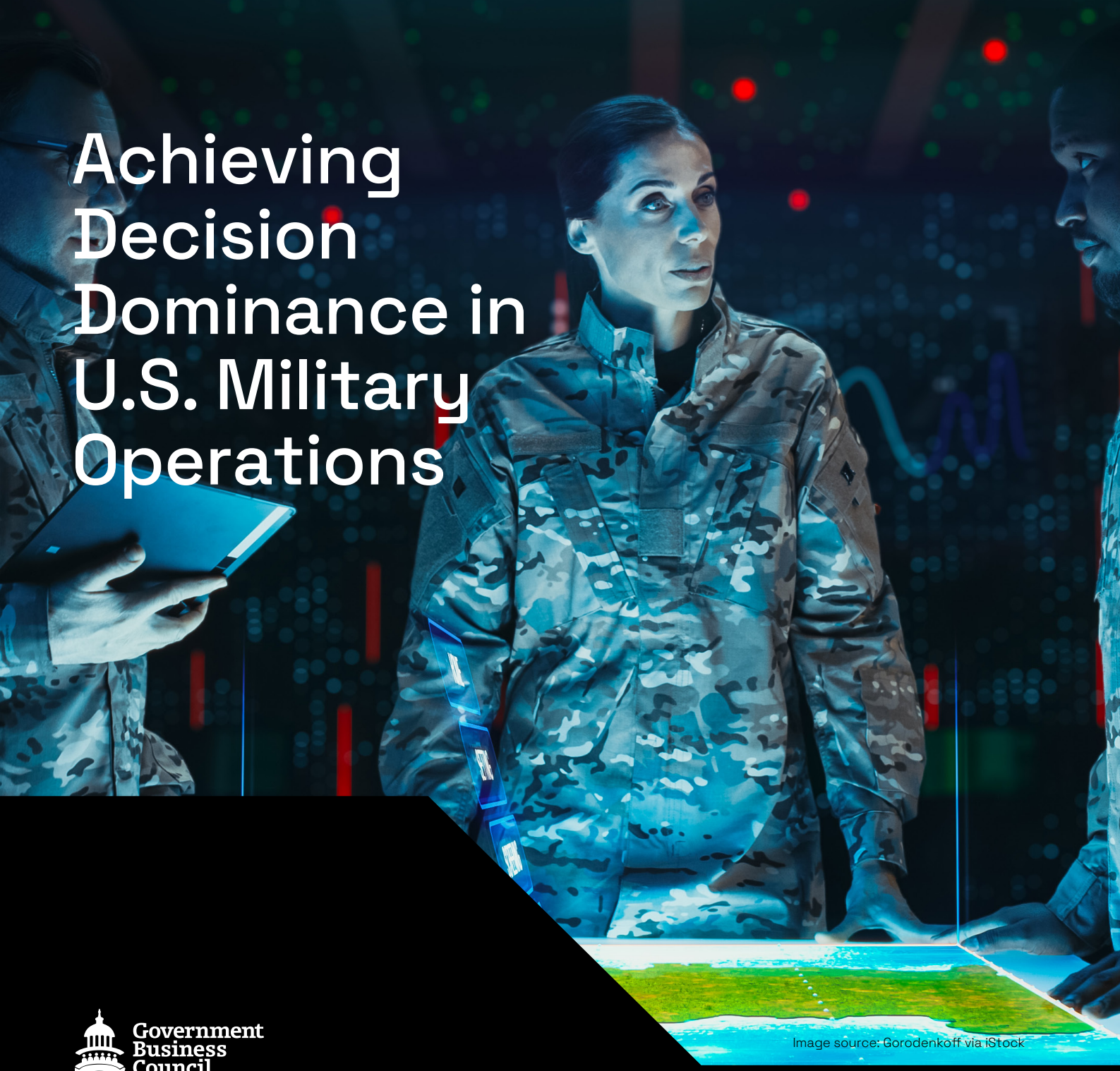

Image source: Gorodenkoff via iStock

Government Business Council

About Government Business Council

As GovExec's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of Government Executive's 50 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision-makers from across government to produce intelligence-based research analysis.

For more information, email us at research@govexec.com or visit our website at govexec.com/insights.

About Everfox

Everfox, formerly Forcepoint Federal, has been a trailblazer in defense-grade cybersecurity for more than two decades. Leading the way in delivering innovative, high-assurance solutions. But we're just getting started.

Learn More

www.everfox.com

EVERFOX

GUIDE

Unlocking Your Data's Value

with Trusted Thin Client Multi-Enterprise Spanning Architecture (MESA)

Image source: Jacob Wackerhausen via iStock

Image source: Dragos Condrea via iStock

Unlocking your data's value with Trusted Thin Client Multi-Enterprise Spanning Architecture (MESA)

Data is of vital importance to the United States and its allied partners. It goes without saying that superiority cannot be guaranteed without the ability to collect, process, and exchange data in an active conflict.

As the number of mission partners increases, so does the volume of data. While this helps enhance readiness, the surge of data has put a lot of pressure on existing digital infrastructure, revealing friction points.

For example, the U.S. Armed Forces must be able to quickly and securely share data with its mission partners on a global scale. During Talisman Sabre in 2023, the need for rapid data sharing was apparent, with Maj. Simon Stanton, Army G6 Signal Officer for the Australian Defence Force (ADF), emphasizing the importance of rapid data sharing among mission partners as joint partners in the region must conquer the tyranny of distance if active conflict were to arise.

"Traditionally, having to switch between information systems in my local environment versus information systems in a partner environment could take minutes, hours or days, and that's time that could be spent focusing on the mission," said Christopher Finch, Everfox Solutions Architect.

Everfox's role in enhancing combat readiness

Everfox TTC, otherwise known as Everfox Trusted Thin Client, seeks to solve this issue via the creation of a Multi-Enterprise Spanning Architecture (MESA) solution capable of scaling to meet global mission demands while establishing secure on-demand access to information systems in multiple enterprise networks. MESA enables real-time collaboration among mission partners without requiring users to switch back and forth between local or partner information systems.

"MESA establishes access and security controls between separated enterprise networks where each owner can say, *'I'm going to publish access to this particular information through the MESA architecture and give this authorized user the ability to subscribe to it,'*" said Finch.

The types of separated enterprises TTC MESA can connect include those deployed across the Joint Worldwide Intelligence Communication System (JWICS), the Secret Internet Protocol Router Network (SIPRNet), the Non-classified Internet Protocol Router Network (NIPRNet), and any other environment in the FVEY community (e.g. MPE SABRE) that exists within its own isolated network segment.

By consolidating to a single multi-enterprise access platform, each enterprise owner retains sovereignty over their local information systems while gaining the ability to collaborate at the speed of the mission. Moreover, TTC MESA leads to greater cost-savings as enterprise owners don't have to invest significant dollars into dedicated infrastructure to support each multi-enterprise collaboration requirement.

With TTC MESA, the mission is front and center.

"For example, if an Army battalion needs to deploy in response to a situation, that battalion may not be equipped to support disparate mission partners they encounter," said Randall Wood, Solutions Architect for Everfox. "TTC MESA changes that by enabling rapid response capabilities for information dominance."

One way that TTC MESA supports enhanced information dominance is through the use of automated access controls. In any conflict or engagement, data is crucial and can mean the difference between success and failure. However, the value of data diminishes over time. Otherwise known as data decay, the more time passes, the less relevant or actionable the information becomes.

When conflict occurs, the U.S. and its allied mission partners must be able to share, process and act on data quickly, with a high level of confidence. However, current network architectures can be confusing at best, slowing that process significantly.

"The reality is there's a spaghetti mess of layered network transports on existing networks," said Wood. "What we're doing is flattening all of that, consolidating and putting it on one network transport that could be extended and scaled globally."

As the amount of data grows, the need for secure, simplified architectures will only increase. Addressing friction points in data exchanges via cross-domain data architectures will be one way that organizations can effectively process information and turn it into valuable insights–whether using traditional methods or through new, innovative solutions relying on artificial intelligence and machine learning. Regardless of the output, cross-domain solutions will be a crucial part of enhancing mission readiness.

"Once we meet the current demand for acceleration, more data and information will be created and along with that, increased the demand for further acceleration," said Finch. "To prepare for that, at Everfox we've designed our TTC technology and capabilities to be deployed to the furthest edge of the battlespace, so it's not something that only lives in a data center anymore."

In conclusion, achieving decision dominance requires a multifaceted approach that addresses the challenges of data management and sharing, technological integration, and cybersecurity. As we move forward, it's essential to prioritize investment in R&D, establish clear standards for interoperability, and develop comprehensive training programs.

As Mark Drobena, Everfox Principal Product Manager, notes: "As we continue to navigate the complexities for achieving decision and technological dominance, it's clear that the need for greater collaboration across varied elements has never been higher. The pace of technological advancements and the evolving threat landscape demand that we work together to develop integrated solutions that can keep up with the speed of decision-making."

By working together and embracing a collaborative approach, we can accelerate progress toward achieving decision dominance and stay ahead of near-peer adversaries.

Image source: Jacob Wackerhausen via iStock

Unlock the value of your data today

Image source: SeventyFour via iStock

About Everfox

Everfox, formerly Forcepoint Federal, has been a trailblazer in defense-grade cybersecurity for more than two decades. Leading the way in delivering innovative, high-assurance solutions. But we're just getting started.

Learn More

www.everfox.com