ACCELERATING DECISION DOMINANCE

UNIFYING MILITARY COMMUNICATIONS FOR GLOBAL COMPETITIVENESS

SOSi

Accelerating Decision Dominance

Unifying Military Communications for Global Competitiveness

The modern global security landscape is rapidly evolving.

Today, the U.S. military faces an unprecedented challenge: maintaining decision dominance in an era of peer and near-peer threats. As senior leaders increasingly warn, adversaries are matching or even exceeding U.S. capabilities in key areas such as artificial intelligence and misinformation campaigns.

"Our near-peer adversaries, and then elements like Hamas, have formidable EW capabilities," Brig. Gen. Ed Barker, the Army's program executive officer for intelligence, electronic warfare and sensors, told an audience at a recent C4ISRNET conference.

To retain its competitive edge, SOSi Chief Technology Officer Kyle Fox said the U.S. Army must dramatically accelerate its ability to collect data, derive actionable intelligence, and make quality decisions faster than ever. Prior to joining SOSi, Fox was the Air Force Nuclear Weapons Center (AFNWC) CTO and a Nuclear Command and Control (NC3) Subject Matter Expert.

"Speed is key," Fox said. "Whoever is best accelerating decision speed and quality will win conflicts at nearly any scale."

But doing so is no easy feat. Key challenges include integrating disparate systems, managing vast data streams, and developing cutting-edge applications. An integrated approach across infrastructure, data management, and application development is essential.

By breaking down silos and leveraging emerging technologies, the Army can achieve the connectivity, data fusion, and algorithmic advantages needed to outpace adversaries and maintain its competitive edge.

> "Speed is key. Whoever is best accelerating decision speed and quality will win conflicts at nearly every scale."
>
> - Kyle Fox, SOSi CTO

The Challenge: Fractured Systems in a Data-Intensive Battlespace

Today's military operates in an environment of data abundance, with sensors and systems generating petabytes of information. However, much of this data remains siloed and inaccessible when and where it's needed most. Legacy networks struggle with the "tyranny of distance" across global operations, while rigid security boundaries impede information sharing.

"At the tactical edge, it's hard to secure and relay critical information to enable command and control," Fox said. "It's even more complex when we start to involve U.S. international partners."

This challenge is compounded by the longstanding separation between business systems and warfighting systems.

"We did this to ourselves in government,"

Fox said. “Legacy thinking was to separate the systems that manage people and equipment with war fighting systems. This approach is incompatible with the speed at which software-defined warfare operates. We must treat our IT systems and warfighting systems as one in the same.”

The result of this legacy approach is a fragmented digital ecosystem that struggles to deliver timely, relevant information to decision makers. To regain the advantage, the Army must pursue a unified approach that treats the entire communications and data infrastructure as a weapon system.

An Integrated Solution: Three Pillars for Decision Dominance

1. Infrastructure: Resilient, Adaptive Transport

The foundation for accelerated decision-making is realizing a flexible, high-capacity transport layer that can securely and seamlessly integrate massive datasets with global operations. To accomplish this, it’s essential the Army accelerates efforts to leverage secure transport across both military and commercial networks from modern wireless (5G), space-based networks, and both dark and lit fiber through programs such as Global Commercial Solutions for Classified (CSfC). This diverse ecosystem greatly improves network performance while also improving redundancy resulting in a system that’s much more challenging for an adversary to defeat.

Additionally, the Army should accelerate adoption of key enabling technologies to support secure global transport such as Software-Defined Wide Area Networking (SD-WAN), which enables dynamic routing and prioritization of traffic across diverse transport options. This technology allows the network to adapt in real-time to changing conditions and requirements, ensuring that critical data always finds the most efficient path. By combining military and commercial infrastructure, defended by proven solutions like CSfC and enabled key technologies like SD-WAN, the Army will realize a secure global fabric that’s ready for any future fight.

“To be successful in future conflicts, we need to see a fully meshed infrastructure using everything we can possibly talk on,” says Fox. “It needs to be so simple that any solider can just plug in a box, turn it on, and it just does its magic. This is well within the realm of current technology.”

2. Data Management: Zero Trust, Data Centric Security

With a robust transport layer in place, the next challenge is securely managing and sharing data across echelons and with coalition partners. At the heart of this effort is the implementation of a Data Centric Zero Trust architecture. This approach moves beyond traditional perimeter-based security models to enable granular access controls and continuous authentication.

3 PILLARS FOR DECISION DOMINANCE

1. Infrastructure: Resilient, Adaptive Transport

- Software-Defined Wide Area Networking (SD-WAN)
- Integration of military and commercial networks
- 5G and advanced wireless technologies
- Global Commercial Solutions for Classified (CSfC)

2. Data Management: Zero Trust Data-Centric Security

- Data-centric Zero Trust architecture
- AI-powered data fusion and analytics
- User and Entity Behavior Analytics (UEBA)
- Granular access controls and continuous authentication

3. App Development: Rapid Fielding of Warfighter Capabilities

- DevSecOps practices
- Continuous Authority to Operate (cATO) processes
- Edge computing and tactical cloud capabilities
- Explainable AI and AI-enabled decision support tools

By attaching security policies directly to the data itself, information can flow securely across network boundaries, enabling unprecedented levels of sharing and collaboration while maintaining strict control over who can access sensitive information.

By implementing Data Centric, Zero Trust systems, the Army establishes the critical foundation required to fully unlock the immense value of the vast data being collected, through secure and trusted AI-powered data fusion and analytics capabilities. By combining disparate data sources and applying machine learning algorithms, critical insights and indicators can be surfaced that would be impossible for human analysts to discover manually. This fusion of multi-source intelligence can provide early warning of adversary activities, identify patterns of behavior, and support rapid, data-driven decision making at all levels of command.

As an example, an emerging AI/ML-enabled technology with significant potential in the data management realm is User and Entity Behavior Analytics (UEBA). This approach leverages machine learning to baseline normal behavior patterns for users and systems, then flags anomalies that could indicate insider threats or compromised accounts.

"UEBA is a great use case," SOSi Senior Network Solutions Architect John Netterwald said. "No one can argue against the validity of the security benefit. It's such a powerful capability for detecting anomalous behavior and potential data exfiltration."

> "Our near-peer adversaries, and then elements like Hamas, have formidable EW capabilities."
>
> - Brig. Gen. Ed Barker, U.S. Army Program Executive Officer

EMERGING TECHNOLOGIES IN MILITARY COMMUNICATIONS

SD-WAN (Software-Defined Wide Area Networking)
Dynamic routing technology that optimizes network traffic across multiple paths, enhancing resilience and efficiency in military communications.

Zero Trust Architecture
Security model that assumes no user or system is trustworthy by default, requiring continuous verification for all access requests, even within the network.

UEBA (User and Entity Behavior Analytics)
AI-driven security approach that establishes baselines of normal behavior for users and systems, flagging anomalies that could indicate threats or compromised accounts.

DevSecOps
Integration of security practices throughout the software development lifecycle, enabling rapid, iterative development while maintaining rigorous security standards.

Edge Computing
Pushing processing power closer to data sources at the tactical edge, reducing latency and bandwidth requirements while enhancing operational resilience and supporting AI/ML workloads.

Explainable AI
AI systems designed to provide clear rationales for their decisions, crucial for maintaining human judgment in military decision-making processes and building trust in AI-enabled systems.

Likewise, The Army must continue its investments in edge computing and tactical cloud capabilities to allow for modern applications such as trusted AI/ML-enabled workloads to reliably operate in real world scenarios. By pushing processing power closer to the point of need, latency can be reduced, bandwidth requirements minimized, and system resiliency improved. Adding that to a secure infrastructure with Data Centric, Zero Trust architecture, the Army provides a low risk means to employ AI/ML workloads that are fully explainable and trusted.

3. Application Development: Rapid Fielding of Warfighter Capabilities

The final pillar focuses on streamlining the development and deployment of mission-critical applications. A key approach in this area is the adoption of DevSecOps practices and the implementation of Continuous Authority to Operate (cATO) processes.

By integrating security throughout the development lifecycle and automating many aspects of cybersecurity assessment, the Army can enable rapid, iterative development while maintaining rigorous security standards. This approach allows new capabilities to be fielded in weeks or months, rather than the years often required under traditional acquisition models.

The increasing complexity in global missions is also driving the need for agile infrastructure supporting trusted processing near or at the tactical edge.

SOSi IN ACTION

Accelerating Decision Dominance through Mission Partner Environments

SOSi's groundbreaking work with the USINDOPACOM Mission Partner Environment (MPE) exemplifies our commitment to accelerating decision dominance in modern military operations. By revolutionizing information sharing and collaboration capabilities, we've empowered commanders to make faster, more informed decisions in the face of complex regional challenges.

Our innovative multi enclave client (MEC) approach has transformed disparate data silos into a unified, data-centric information domain. This integration dramatically reduces the time required to form coalition environments from weeks to mere days, providing a significant edge in operational tempo. By leveraging hyper-converged infrastructure and private cloud architecture, we've seamlessly connected approximately 17,000 previously isolated computing environments, creating a robust foundation for rapid information exchange and analysis.

The implementation of advanced virtualization techniques and a Zero-Trust security architecture has not only enhanced the MPE's resilience but also laid the groundwork for integrating cutting-edge AI and machine learning capabilities. These technologies are crucial for processing vast amounts of data and surfacing actionable insights, further accelerating the decision-making cycle.

Our work with USINDOPACOM MPE directly contributes to decision dominance by enabling:

1. Real-time situational awareness through enhanced data fusion and sharing.
2. Rapid formation of secure coalition environments to address emerging threats.
3. Improved interoperability, facilitating seamless collaboration with allies.
4. Advanced security measures that protect critical information while ensuring accessibility.

By streamlining information flows, enhancing security, and enabling advanced analytics, SOSi's innovations in the MPE space are helping to compress the OODA (Observe, Orient, Decide, Act) loop, giving U.S. forces and their allies a decisive advantage in the Indo-Pacific region and beyond.

As AI becomes increasingly central to military operations, the development of explainable AI and AI-enabled decision support tools will be critical. These technologies can provide warriors with algorithmic advantages while maintaining human judgment in the loop, ensuring that AI recommendations can be trusted and understood by commanders making life-or-death decisions.

“As a community we need to be talking about the dominance software has on modern conflict and the need for firm requirements for secure-by-design practices and supply chain transparency through techniques like Software Bills of Materials (SBOM) and explainable AI such as AIBOMs,” Fox said. “These are critical for building trust in our modern AI-enabled systems.”

Recommendations for Policy and Industry Action

Realizing this vision of unified military communications will require changes to acquisition processes, security policies, and industry engagement. A crucial first step is to designate key networking and data platforms as weapon systems. This shift in classification would streamline acquisition processes and emphasize the operational importance of these digital capabilities, allowing them to be funded and developed with the same urgency as traditional kinetic systems.

To accelerate the fielding of new capabilities, the Department of Defense should expand reciprocity agreements for security authorizations across its components. By allowing one service’s security assessment to be recognized by others, redundant testing can be eliminated, and innovative technologies can be deployed more rapidly across the joint force.

Increased investment and adoption velocity in public-private partnerships and commercially derived solutions is essential to leverage industry innovation. The pace of technological advancement in the commercial sector often outstrips that of traditional defense contractors, and the Army must find ways to more

KEY RECOMMENDATIONS FOR POLICY AND INDUSTRY ACTION

Designate Key Networks as Weapon Systems

Reclassify critical networking and data platforms as weapon systems to streamline acquisition and emphasize their operational importance.

Expand Security Authorization Reciprocity

Increase recognition of security assessments across Army and other services to eliminate redundant testing and accelerate technology deployment.

Accelerate Adoption of Commercial Solutions

Increase investment and adoption velocity in public-private partnerships and commercially derived solutions to leverage industry innovation.

Develop Responsible AI Guidelines

Create clear frameworks for AI development and deployment in military contexts, leveraging public-private partnerships to address transparency, ethics, and human control.

Enhance Digital Talent Acquisition

Expand programs like the U.S. Digital Corps, direct commissioning for cyber and AI specialists, and collaborate with academia and industry to create a robust pipeline of technologically skilled personnel.

Unify Business and Warfighting Systems

Treat IT systems and warfighting systems as one, breaking down traditional silos to create a unified digital ecosystem compatible with software-defined warfare.

Prioritize Secure-by-Design Practices

Emphasize security throughout the development process, including Software Bills Of Materials and explainable AI techniques like AIBOMs.

quickly adopt and adapt these cutting-edge capabilities for military use.

As AI becomes more prevalent in military systems, there is a pressing need to develop clearer guidelines and processes for responsible AI development and deployment in military contexts. These frameworks should address issues of bias, transparency, and human control, ensuring that AI-enabled systems align with military ethics and values.

Finally, to build and maintain the sophisticated digital ecosystem envisioned, the DoD must expand programs to attract and retain digital talent. This could include initiatives like the newly established U.S. Digital Corps, direct commissioning programs for cyber and AI specialists, and increased collaboration with academia and industry to create a robust pipeline of technologically skilled personnel.

Conclusion

The future of warfare will be defined by decision speed and quality. By unifying its approach to communications infrastructure, data management, and application development, the U.S. Army can accelerate its Observe, Orient, Decide, Act (OODA) loop and maintain decision dominance against peer adversaries. This will require breaking down traditional silos, embracing emerging technologies, and fostering deeper collaboration between government and industry.

"We're not saying go so fast that it's reckless," Fox said. "We must accelerate safely, or we will lose our safety. It's about building on the shoulders of your peers versus trying to go it alone."

By taking bold action now to modernize its digital backbone, the Army can ensure it remains the most lethal and effective fighting force on the global stage. The path forward requires not just technological innovation, but a fundamental shift in how the military approaches its digital transformation.

With a unified strategy that spans from the tactical edge to the enterprise level, the U.S. Army can create a decisive advantage in the information-driven battles of the future.