EVERFOX

Enhancing Cybersecurity for the DoD in the JADC2 and AI Era

Whitepaper

Enhancing Cybersecurity for the DoD in the JADC2 and AI Era

Enhancing Cybersecurity for the Department of Defense in the JADC2 and AI Era

The convergence of our digital and physical worlds—not to mention persistent threats at home and abroad—catalyzed development of the Defense Department's (DoD's) Joint All-Domain Command and Control (JADC2) initiative[1]. This initiative aims to maintain the United States' strategic and operational superiority in modern warfare by increasing collaboration and integrating advanced technologies, including artificial intelligence (AI). As AI becomes increasingly central to JADC2, ensuring the security of AI systems and data becomes paramount. This issue brief explores the intricate relationship between AI, JADC2, and cybersecurity, highlighting the critical measures necessary to protect the DoD's networks from sophisticated cyber threats.

JADC2 Initiatives Today

The JADC2 initiative represents a transformative effort to connect the sensors, shooters, and communications devices across all the military services—Air Force, Army, Marine Corps, Navy, and Space Force—into a single network and enhance overall mission effectiveness. Its primary goal is to regain informational and decision-making advantages through radical information integration and technology utilization.

Each branch of the U.S. military has implemented its own initiatives to comply with JADC2, each focusing on integrating advanced technologies and enhancing interoperability. The primary contributions to the JADC2 effort from each branch are:

→ **Army**
Project Convergence aims to link sensors, shooters, and command systems across all domains, incorporating AI and autonomous systems to improve battlefield communication and decision-making.

→ **Navy**
Project Overmatch focuses on enhancing naval command and control capabilities and upgrading communications infrastructure for secure data exchange.

→ **Air Force**
The Advanced Battle Management System (ABMS) creates a military internet of things, using cloud environments, AI, and new communication methods for seamless data sharing and faster decision-making.

→ **Space Force**
The Unified Data Library (UDL) aggregates data from various sensors to provide comprehensive situational awareness, using AI and machine learning (ML) for data management.

→ **Marine Corps**
Project Dynamis aims to replace outdated equipment and software, supporting distributed operations through Expeditionary Advanced Base Operations (EABO). The Marine Corps works closely with the Navy and other services to ensure interoperability and effective integration of JADC2 capabilities, enhancing command and control in dynamic settings.

The role of AI within the JADC2 program
To achieve program objectives, JADC2 leverages emerging technologies, including AI, ML, and predictive analytics. These technologies enable rapid data processing, automation of repetitive tasks, and provision of accurate predictions and insights, thus supporting faster and more informed decision-making processes. Several cross-branch initiatives demonstrate the integration of AI within JADC2:

→ **Global Information Dominance Experiments (GIDE)**
These experiments integrate AI decision aids and other technologies to enhance joint force capabilities. They aim to refine the interoperability and effectiveness of JADC2 systems across multiple military branches.

→ **Chief Digital and AI Office (CDAO)**
The CDAO oversees the implementation of data analytics and AI strategies across the DoD, ensuring alignment with JADC2 objectives.

These initiatives highlight the critical role of AI in facilitating rapid data processing and analysis, enabling commanders to make quick and effective decisions: AI is indispensable for managing the complexity and speed required in contemporary military operations. It supports data integration, decision-making, communications, and predictive analytics, ensuring that military responses to threats are coordinated and timely.

Ethical Implementation of AI/ML

Responsible use of AI is at the center of the DoD's implementation efforts. Early in 2020, the DoD committed to governing AI adoption with ethical principles that emphasize responsibility, equitability, traceability, reliability, and governability.[2]

Additionally, in response to Executive Order 14110[3], the DoD has committed to the safe, secure, and trustworthy development and use of AI. This commitment includes implementing frameworks such as the DoD Vision for AI[4] and the Data Analytics and Artificial Intelligence Adoption Strategy[5]. These frameworks emphasize scalable AI adoption, infrastructure investment, talent expansion, and responsible AI use to ensure decision superiority for U.S. forces.

The DoD's ethical implementation of AI and cross collaboration are already supporting warfighters in the field. For instance, AI-driven data analytics help synthesize vast amounts of information from various sources, providing commanders with real-time, actionable insights that protect our warfighters in the field.

AI-Driven Threats and Countermeasures

While AI has tremendous promise, it also has tremendous risks. In short, our military is not the only global actor using it. State and non-state actors are using AI to enhance their reconnaissance and social engineering efforts, making attacks more effective and harder to detect. Malicious actors are using AI to refine phishing emails, voice clones, deepfakes, and other deceptions to spread misinformation or steal sensitive information. Every day, cyberattacks become more sophisticated. Recent examples of AI-based cyberattacks against the U.S. military include:

North Korean cyberespionage teams are using generative AI models to investigate foreign think tanks, craft spear-phishing emails, and analyze publicly accessible security flaws.

Iran's Revolutionary Guard is utilizing large-language models to generate code snippets, craft phishing emails, and research how to disable antivirus systems.

Chinese cyber groups are using AI models to support new hacking tool developments, generate believable phishing messages, and source information about high-profile individuals and U.S. defense contractors.

Russian military intelligence divisions are using AI to investigate satellite communication protocols and radar imaging technology that could be related to military operations in Ukraine.

AI is a powerful tool for gaining a competitive edge in the cyber domain. AI can also enhance cybersecurity by identifying and mitigating threats in real time. It can analyze vast amounts of data to detect anomalies and patterns indicative of cyber attacks, predict potential threats, and automate responses to security incidents. AI-powered systems can also adapt to new attack methods, improve threat intelligence, and reduce the time and resources needed for threat detection and response.

Securing Military Operations

To detect and mitigate AI-driven threats, the DoD is committed to implementing a zero trust security model. Zero trust enhances security by continuously verifying the identity and integrity of users and devices, minimizing the risk of data breaches and cyberattacks. Zero trust addresses AI threats while AI enhances zero trust methodologies by automating threat detection, behavior analysis, and anomaly identification[7].

The DoD's commitment to achieving a zero trust security architecture by 2027 involves leveraging AI to streamline implementation processes and ensure continuous security enhancements. This strategy is crucial as agencies move forward with future iterations of zero trust updates and initiatives[8].

Adapting to Rapid Technological Advancements

As cyber threats evolve, the DoD is adapting and responding by prioritizing the following areas:

Responsible AI Development

Adhering to ethical principles and frameworks to ensure AI technologies are developed and used responsibly.

Zero Trust Implementation

Accelerating the adoption of zero trust architectures to safeguard AI systems and data from unauthorized access and cyber threats.

Talent and Infrastructure Investment

Investing in expanding digital talent and developing interoperable, federated infrastructures to support scalable AI adoption.

Collaboration and Information Sharing

Fostering collaboration across military branches and with allied partners to enhance collective defense capabilities against AI-driven threats.

Final Thoughts

The integration of AI within the JADC2 initiative represents a significant advancement in the DoD's efforts to maintain strategic and operational superiority in modern warfare. By implementing responsible AI frameworks, adopting zero trust security models, and investing in infrastructure and talent, the DoD can continue to effectively protect its critical data and networks. As AI continues to evolve, these proactive measures will ensure that the U.S. military remains prepared to counter emerging threats and leverage advanced technologies for mission success.

Citations

1 - Summary of the JADC2 Initiative, Department of Defense, March 2022 https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF

2 - DoD Press Release. "DOD Adopts Ethical Principles for Artificial Intelligence." February 24, 2020. https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/

3 - Congressional Research Service. "The AI Executive Order and Its Potential Implications for DOD." December 12, 2023. https://crsreports.congress.gov/product/pdf/IN/IN12286

4 - Clark, Joseph. "Pentagon Official Lays Out DOD Vision for AI." DOD News. February 21, 2024. https://www.defense.gov/News/News-Stories/Article/Article/3682355/pentagon-official-lays-out-dod-vision-for-ai/

5 - Clark, Joseph. "DOD Releases AI Adoption Strategy." DOD News. November 2, 2023. https://www.defense.gov/News/News-Stories/Article/Article/3578219/dod-releases-ai-adoption-strategy/

6 - Security Staff. "US adversaries employ generative AI in attempted cyberattack." https://www.securitymagazine.com/articles/100418-us-adversaries-employ-generative-ai-in-attempted-cyberattack

7 -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

8 - "Department of Defense Releases Zero Trust Strategy and Roadmap." November 22, 2022. https://www.defense.gov/News/Releases/Release/Article/3225919/department-of-defense-releases-zero-trust-strategy-and-roadmap

Enhancing Cybersecurity for the DoD in the JADC2 and AI Era

Everfox, formerly Forcepoint Federal, has been a trailblazer in defense-grade cybersecurity formore than two decades. Leading the way in delivering innovative, high-assurance solutions.

Learn more @ Everfox.com »

About Government Business Council

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.

EVERFOX

Securing the future

Securing the Future

Logging in: Cybersecurity in the age of AI Next-generation Security Principles

Securing the Future starts with a Focus on Secure by Design Principles

JADC2's central tenet focuses on delivering a decisive advantage to the warfighter at the mission's edge. Emerging technologies will play an increasingly important role in this mission, as technologies like generative AI, ML and predictive analytics combine with contemporary sensors and solutions.

As our world grows increasingly complex, protecting data will require organizations to create a holistic, 360-degree view of their data, assets and workloads.

AI/ML and predictive analytics are shaping consumer experiences across the globe, and they could revolutionize how the DoD and DIB streamline decision-making. For example, at AFCEA West, Chief of Naval Operations, Admiral Lisa Franchetti, mentioned how the U.S. Navy is seeking to use AI as a means of "maintaining, repairing and delivering platforms on time and at a lower cost."

Emerging technology could also be applied to protect data at the edge. Jill Bradshaw, senior industry product marketing manager at Everfox, points toward AI/ML's ability to effectively recognize patterns and flag potentially malicious activity. Unlike human analysts, AI models can effectively analyze large volumes of data quickly and accurately all within a matter of milliseconds, flagging potentially suspicious actions for further review by a human analyst.

"However, once you have the information, you need to get it to the right people at the right time," Bradshaw said.

Augmented reality could be just one of many ways leaders push information to the warfighter or human at the edge. As technologies like augmented reality increasingly find their way onto the battlefield, Cross Domain Transfer and Access solutions could help augment emerging technologies.

Cross domain technologies are designed to protect sensitive classified information while still maintaining a level of integrity, confidentiality and the availability of the data shared with authorized personnel. Cross domain access solutions like Everfox's Trusted Thin Client DC enable simultaneous access to multiple networks/clouds from a single endpoint, advancing innovation at the edge.

"Our Trusted Thin Client DC's capabilities allow agencies to connect to critical data anywhere in the world from anywhere. Soon, we're going to expand these capabilities to include Multi-Enterprise Spanning Architectures (MESA Partner Clusters) that will increase options for secure, controlled collaboration across agencies, commands and partners while maintaining full control of their own resources" said Bradshaw.

While emerging technologies hold great potential, risks exist. How do organizations effectively pursue innovation ***without*** compromising on security?

Balancing Innovation + Security

Balancing innovation and security doesn't have to be a daunting task. Defense leaders in the DoD and DIB can and should look to establish AI security compliance programs and map out boundaries of where and how they will deploy emerging technology. According to a recent report by Harvard's Belfer Center, as threats to data increase, governance will only grow in importance:

"The goals of these compliance programs are to 1) reduce the risk of attacks on AI systems, and 2) mitigate the impact of successful attacks. Compliance programs will accomplish these goals by encouraging stakeholders to adopt a set of best practices in securing their systems and making them more robust against AI attacks," said author and Ph.D. Candidate in Computer Science at Harvard University, Marcus Comiter.

By assessing and determining the specific value-add of an AI system, organizational leadership can account for security and innovation. However, as cyber threats evolve, they will need to update compliance documents regularly.

Living out Compliance

According to the UK's National Cyber Security Centre (NCSC), AI will lower the "barrier to entry" for some potential threat actors, making it easier to "carry out effective access and information gathering operations. Enhanced access will likely contribute to the global ransomware threat over the next two years."

Now is the time for leaders to move from threat detection to threat ***prevention***. Secure by Design, as outlined by the Cyber and Infrastructure Security Agency (CISA), must be included in the design and creation of any new products, hardware and software.

"We were among the first to sign CISA's Secure by Design Pledge," said Bradshaw. "Everything is designed with a security-first approach and we are dedicated to continuously enhancing the resilience of our products and routinely releasing patches for all of our product offerings."

While the transformative potential of AI is real, securing software will be a critical step in ensuring that AI reflects the "principles of the people who build it, the people who use it and the data upon which it is built," as outlined by the Biden Administration in the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.

With the proper precautions in place, programs like JADC2 could harness the power of emerging technologies to effectively deliver the decisive advantage, but only if we pursue Secure by Design principles.

As leaders look toward a future shaped by AI, there are a few considerations to take into account:

- → **Default Passwords** — Does your organization or product rely on default passwords? Are they required to be changed upon log-in?
- → **Classes of Vulnerabilities** — What are you doing to scrub inputs for SQL injection or XSS?
- → **Policy** — Does you business have a vulnerability disclosure policy? When was this last updated?
- → **Logging** — Does your product provide you with detailed logs around configuration changes?

"Ready or not, AI is here to stay," Bradshaw said. "Organizations must prepare for new efficiencies wrought by our adversaries and ensure we are employing the utmost security and we must be ready to adapt in order to stay ahead of the curve and what AI brings both good and bad."