2024 NDIA MICHIGAN CHAPTER
GROUND VEHICLE SYSTEMS ENGINEERING
AND TECHNOLOGY SYMPOSIUM
MODULAR OPEN SYSTEMS APPROACH (MOSA) TECHNICAL SESSION
AUGUST 13-15, 2024 - NOVI, MICHIGAN

HARNESSING ADVANCED TECHNOLOGIES FOR SWARM OPERATIONS WITHIN CJADC2

Timothy Stewart[1], Emil Kheyfets[1], David Taylor[2]

[1]Aitech, Chatsworth, CA
[2]Thunder Bay Consulting, LLC, Charleston, SC

ABSTRACT

Understanding the impact of swarm dynamics on land defenses means evaluating the complex behaviors exhibited by groups of autonomous or semi-autonomous entities, which require significant synchronization and coordination toward a common objective. Effectively addressing the challenges to ground vehicles while exploiting the opportunities presented by swarm operations requires a holistic understanding of swarm dynamics and the integration of advanced technologies and adaptive command and control systems within the CJADC2 framework. This paper explores the pivotal role of specific technologies— AI, TSN, Sensor Fusion, Autonomous Systems, and Cybersecurity — and MOSA-based open standards in enabling effective swarm operations within CJADC2 to detect, analyze, and respond to swarm threats in real-time across diverse platforms and domains and ensure compatibility with existing command and control infrastructure.

Citation: D. Taylor, T. Stewart, E. Kheyfets "Harnessing Advanced Technologies for Swarm Operations Within CJADC2," In *Proceedings of the Ground Vehicle Systems Engineering and Technology Symposium* (GVSETS), NDIA, Novi, MI, Aug. 13-15, 2024.

1. INTRODUCTION

Swarm operations involve the coordinated deployment of large numbers of autonomous or semi-autonomous agents to achieve military objectives. These operations can manifest in various forms, including swarms of drones, uncrewed vehicles, or cyber agents, and are characterized by their agility, adaptability, and distributed nature.

Conducting offensive swarm operations and protecting the force against adversary swarm attacks present challenges and opportunities for military forces, requiring innovative approaches to Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) coordination.

The use of drones in military operations has been increasing from small scale operations to large, complex initiatives that are changing the future of warfare. These types of attacks pose one of the more significant risks to ground vehicles and in-field operations,

where vehicles and personnel are left exposed and less able to maneuver across certain terrains. This is evident in recent conflicts across both the wars in Ukraine and the Gaza Strip.

For offense measures, drone swarms deployed and controlled by ground offenses can provide advanced tactical maneuvers across a more expansive geography than ground vehicles, leading to more intelligent tactical implementations in combat.

2. CJADC2: ENHANCING JOINT INTEROPERABILITY FOR DECISION SUPERIORITY

CJADC2 is the Combined Joint All-Domain Command and Control capability, which creates a multinational framework for integrated command and control that fosters cooperation, intelligence sharing, and integrated capabilities across multiple nations. It facilitates a combined global defense strategy that integrates data network and sensor connectivity across all entities.

This paradigm shift in military operations aims to unify command and control across all domains—land, air, sea, space, and cyberspace. CJADC2 seeks to enable seamless information sharing, rapid decision-making, and coordinated actions across diverse military forces and platforms, enhancing operational effectiveness and agility in an increasingly complex and contested environment. (Figure 1)

Addressing the complexities of integrating advanced technologies and tactics, techniques, and procedures (TTPs) in swarm operations within the CJADC2 framework can ensure mission success in the face of defeating and controlling swarms.

By harnessing capabilities, from AI-driven swarm management systems to time-sensitive networking (TSN) protocols for real-time coordination, military forces can employ sensor fusion, autonomous systems, and cybersecurity measures to enhance situational awareness, decision-making capabilities, and operational agility. Ground vehicles are playing an increasingly critical role in the management of swarm operations.

3. DECHIPERING SWARM DYNAMICS: CORNERSTONE OF DECISION DOMINANCE IN CJADC2 OPERATIONS

Effectively addressing the challenges while exploiting the opportunities presented by swarm operations requires a holistic understanding of swarm dynamics and the integration of advanced technologies and adaptive command and control systems within the CJADC2 framework.

By analyzing the interactions between large quantities of sensors and shooters, their

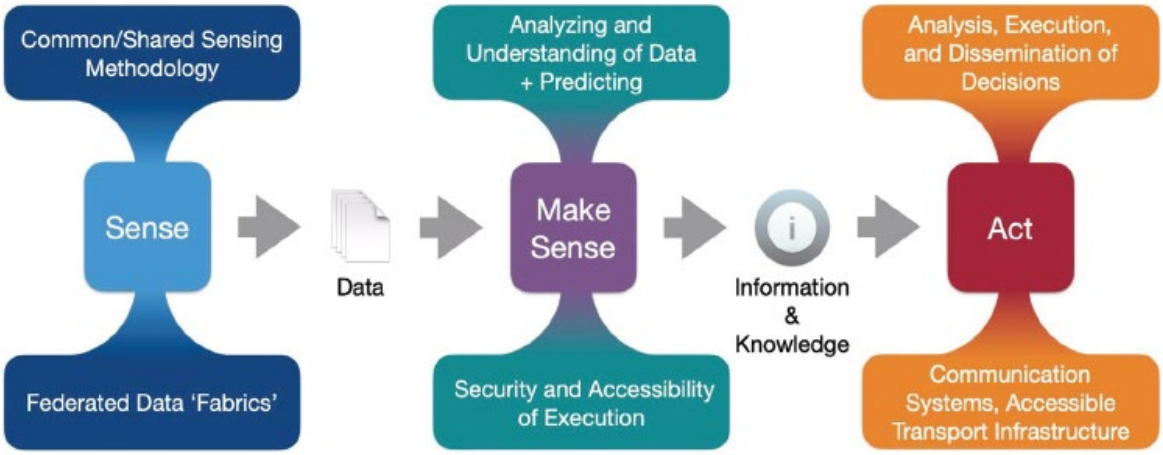

Fig. 1. CJADC2 Action Chain and Process

respective communication protocols, and decision-making processes and technologies, military planners can gain insights into the vulnerabilities, strengths, and potential threats swarms pose to inform plans and decisions. One can then develop strategies to leverage swarm capabilities in shaping multidomain operations or counter adversarial swarms to protect ground forces. (Figure 2)

Fig. 2. With a holistic understanding of swarm dynamics, military planners can gain insights into the vulnerabilities, strengths, and potential threats swarms pose to ground vehicle operations.

Military forces leveraging swarm capabilities can achieve superior situational awareness, rapid response times, and distributed lethality, enabling them to make decisions to counter threats in contested environments and fire and maneuver to a position of advantage to accomplish mission objectives.

4. TECHNOLOGIES ENABLING SWARM OPERATIONS IN CJADC2

Understanding swarm dynamics means evaluating the complex behaviors exhibited by groups of autonomous or semi-autonomous entities, which require significant synchronization and coordination toward a common objective. Transitioning from the conceptual understanding of swarm dynamics, we now outline the pivotal role of specific technologies in enabling effective swarm operations within CJADC2: AI, TSN, Sensor Fusion, Autonomous Systems, and Cybersecurity.

4.1 AI (Artificial Intelligence) for Actionable Intelligence

AI technologies are essential enablers of swarm management within the CJADC2 framework. They empower military forces to effectively leverage swarm capabilities while countering adversarial swarms with agility and precision.

By leveraging AI algorithms and machine learning techniques, military forces can enhance their ability to detect, analyze, and respond to swarm threats in real-time. AI-driven swarm management systems can autonomously coordinate the actions of multiple agents, optimizing their behavior for maximum efficiency and effectiveness.

These systems can analyze vast amounts of sensor data to identify patterns, anomalies, and potential threats, enabling proactive decision-making and response strategies. Additionally, AI algorithms can adapt and learn from experience, continuously improving their performance and resilience against evolving swarm tactics and strategy and better informing decisions.

By integrating AI technologies into C5ISR systems, military commanders can gain real-time insights into swarm dynamics. These AI-powered swarm management systems facilitate rapid decision-making and response coordination, enhancing situational awareness across all domains. (Figure 3)

Fig. 3. AI-driven decision support systems enable commanders to orchestrate effective swarm engagements, while minimizing risks to ground personnel and assets.

AI algorithms can also assist in predictive analytics, forecasting swarm behaviors and trends based on historical data and current observations. AI-driven decision support systems can provide commanders with actionable intelligence and recommendations, enabling them to orchestrate effective swarm engagements while minimizing risks to ground personnel and assets.

4.2 TSN (Time-sensitive Networking) for Real-time Coordination

Time-sensitive networking (TSN) has emerged as a critical component within the CJADC2 framework, particularly for enabling real-time coordination essential for effective swarm operations. TSN protocols prioritize data transmission, ensuring low-latency communication crucial for rapid decision-making and response coordination for Human Machine Integrated Formations.

TSN offers scalability, allowing military forces to adapt their communication networks to the demands of evolving swarm environments. This flexibility enables military commanders to dynamically allocate bandwidth and resources to prioritize critical data transmissions, ensuring that essential information reaches decision-makers in real-time.

Additionally, TSN supports interoperability between disparate systems and platforms, facilitating seamless integration of sensors, autonomous systems, and command and control systems across multiple domains. As military operations become increasingly interconnected and data-intensive, adopting TSN protocols becomes imperative for maintaining operational tempo and achieving mission success in swarm environments within the CJADC2 framework.

In swarm environments, where the sheer volume of data is exchanged between autonomous agents, TSN facilitates a seamless and timely information exchange, enabling synchronized actions across diverse platforms and domains. By leveraging TSN, military forces can overcome the challenges of communication delays and bottlenecks, enabling agile and coordinated responses to dynamic swarm threats.

In conjunction with AI-driven support systems, TSN can be leveraged to optimize the transmission of high-value data content over limited capacity tactical communication links. AI algorithms can dynamically analyze the urgency and importance of data packets, collaborating with TSN mechanisms to prioritize their transmission based on real-time mission requirements and network conditions. This collaborative approach ensures that essential information reaches its destination within the specified timeframe, even in bandwidth-constrained and contested environments.

TSN's deterministic capabilities facilitate the coordination of distributed assets and autonomous agents operating within swarm frameworks. By providing precise timing synchronization and low-latency communication channels, TSN enhances the efficiency and coordination of swarm behaviors, enabling military forces to respond rapidly and effectively to dynamic threats.

The synergy between TSN and AI-driven support systems empowers military commanders with enhanced situational awareness and decision-making capabilities, ultimately optimizing the effectiveness of swarm engagements while minimizing risks to personnel and assets on the battlefield.

4.3 Sensor Fusion and Data Integration for Enhanced Situational Awareness

Sensor fusion and data integration are critical pillars in the arsenal of military capabilities, particularly within the complex and dynamic context of swarm operations under the CJADC2 framework. These

technologies enable the aggregation and correlation of information from disparate sources, ranging from traditional radar and EO/IR sensors to advanced cyber sensors and signal intelligence platforms.

Military forces can synthesize data from multiple sensors through sensor fusion, compensating for individual limitations and enhancing overall situational awareness. By combining inputs from various domains, such as air, land, sea, space, and cyber, sensor fusion provides a comprehensive understanding of the operational environment, enabling precise detection and tracking of swarms in real-time.

Data integration facilitates seamless communication and collaboration between systems and platforms, fostering interoperability and synergy across diverse domains. Standardizing data formats and communication protocols ensures the smooth exchange of information between crewed and uncrewed assets, command centers, and allied forces. Rapidly sharing critical information and enhanced decision-making are crucial tactical objectives for joint operations.

By combining sensor data with other intelligence sources, such as human intelligence and open-source information, data integration gives military commanders a more holistic understanding of the operational landscape. This enables them to anticipate swarm movements, identify vulnerabilities, and formulate effective response strategies.

Sensor fusion and data integration also enable targeted resource allocation by consolidating data from multiple sensors and intelligence sources. Military forces can prioritize strategic actions based on the threat of swarms, deploying resources where they are most needed, maximizing operational impact, and minimizing risks.

4.4 Autonomous Systems and Robotics for Swarm Deployment and Engagement

Human Machine Integrated Formations represent a transformative capability in swarm operations within the CJADC2 framework. They provide a spectrum of uncrewed platforms, ranging from aerial drones to ground-based vehicles and maritime vessels, each tailored to specific operational requirements.

Autonomous systems enhance surveillance capabilities through persistent monitoring of areas prone to swarm activity and early detection of potential threats. They provide rapid deployment and maneuverability, allowing for swift, agile responses to emerging swarm scenarios.

Integrated AI algorithms, autonomous systems, and robotics offer unparalleled adaptability and scalability to analyze vast amounts of sensor data in real-time, enabling autonomous decision-making and adaptive responses to dynamic battlefield conditions. These systems allow a wider operational footprint by augmenting the capabilities of human-operated platforms, extending reach, and enhancing the effectiveness of military operations across all domains. (Figure 4)

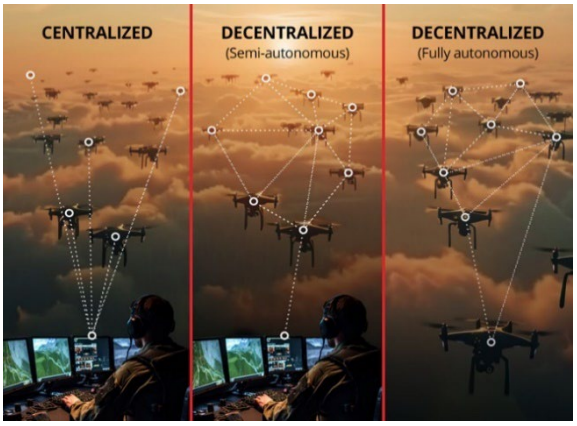

Fig. 4. AI-driven platforms can operate autonomously or collaboratively with crewed assets, forming a networked ecosystem capable of adapting and responding to swarm threats in real-time.

AI-driven autonomy enables uncrewed systems to assess the intent and behavior of swarms, adjusting their tactics and maneuvers accordingly to maintain a tactical advantage. Additionally, robotics enhance force protection by reducing the reliance on human operators in high-risk environments, mitigating potential casualties, and preserving operational continuity in the face of adversarial swarm attacks. These platforms can operate autonomously or collaboratively with crewed assets, forming a networked ecosystem capable of adapting and responding to swarms in real-time.

4.5 Cybersecurity Measures for Protecting Swarm Operations

Cybersecurity measures are imperative to the CJADC2 framework, especially concerning swarm operations, given their reliance on interconnected digital networks and communication systems. The interconnected nature of these systems exposes them to various cyber threats, ranging from infiltration and data breaches to disruption and sabotage.

As such, robust cybersecurity measures are paramount to safeguarding military networks, platforms, and data from malicious actors intent on compromising swarm operations through advanced encryption protocols, access controls, and intrusion detection systems to identify and mitigate threats in real-time.

Additionally, comprehensive, proactive cybersecurity policies and procedures must be established to govern the secure operation of swarm-related technologies, ensuring that they adhere to stringent security standards and best practices. (Figure 5)

This involves continuous threat intelligence gathering, vulnerability assessments, and penetration testing to identify and address weaknesses in network defenses to preemptively identify and mitigate potential cyber-attacks on swarm operations before they can compromise mission integrity.

Fig. 5. Given the reliance on interconnected digital networks, proper swarm management requires cybersecurity policies and procedures to govern secure operation.

Robust incident response plans must also be in place to enable swift and coordinated responses to cyber incidents, minimize their impact on swarm operations, and restore operational functionality expeditiously. Cybersecurity training and awareness programs give military personnel at all levels the knowledge and skills to effectively identify and respond to cyber threats.

Collaboration with industry partners and academia can facilitate the exchange of cybersecurity expertise and best practices, enabling military forces to effectively leverage the latest advancements in cybersecurity technology and techniques to defend against evolving cyber threats.

5. OVERCOMING INTEGRATION CHALLENGES IN SWARM OPERATIONS

Overcoming integration challenges is imperative for seamlessly integrating technologies within the CJADC2 framework for swarm operations, aligning with CJADC2 lines of effort and guidance. One key challenge lies in reconciling the diversity of systems and platforms operated by different military branches and allied forces, each with proprietary technologies and communication protocols.

Collaborative efforts are essential to developing standardized interfaces and protocols, including integration testing and validation procedures, to facilitate

interoperability and data exchange between disparate systems and ensure cohesive integration across all domains in real-world swarm environments.

Coordinating the actions of multiple autonomous agents and ensuring their compatibility with existing command and control infrastructure is complex. As directed by CJADC2 guidance, advanced modeling, and simulation techniques can simulate swarm behaviors and test the interoperability of integrated systems in virtual environments before deployment.

Systems with modular and scalable architectures facilitate the integration of incremental upgrades and enhancements over time while adhering closely to scalability objectives.

6. MODULAR OPEN SYSTEMS ARCHITECTURE (MOSA): ENABLING INTEROPERABILITY FOR SWARM OPERATIONS

The United States Department of Defense (DoD) faces an increasingly complex and dynamic operational environment characterized by rapidly evolving threats and the need for adaptable, interoperable systems. To address this challenge, the DoD has embraced a paradigm shift in defense system design through the implementation of Modular Open Systems Architecture (MOSA).

MOSA represents the culmination of prior initiatives such as the Future Airborne Capability Environment (FACE) and the Open Systems Architecture (OSA). These efforts aimed to overcome the limitations of proprietary, stove-piped systems by promoting open standards and modular design principles. MOSA's development gained momentum in the early 2000s as the DoD recognized the need for greater interoperability and system adaptability to address emerging threats and evolving operational requirements.

6.1 MOSA Core Principles

MOSA is underpinned by a set of core principles that govern its approach to system design and development:

Open Standards: MOSA advocates for the utilization of publicly published standards and interfaces to ensure interoperability across diverse systems irrespective of vendor origin. By adhering to industry-endorsed standards established by consortia like MOSA and SOSA, MOSA-compliant systems achieve seamless integration with third-party components and technologies.

Modular Design: MOSA emphasizes a modular approach to system design. Complex systems are decomposed into smaller, self-contained modules with clearly defined interfaces. This modularity facilitates independent development, testing, and upgrade of individual modules, fostering rapid integration and evolution of overall system capabilities.

Interoperability: Interoperability is a cornerstone of MOSA, enabling disparate components from various vendors and sources to collaborate effectively within a unified system architecture. By adhering to open standards and utilizing standardized interfaces, MOSA-compliant systems achieve seamless data and command exchange, enhancing overall system interoperability and mission effectiveness.

Scalability and Adaptability: MOSA inherently promotes scalability and adaptability by facilitating the incorporation of new technologies and capabilities without requiring extensive system redesign or reintegration efforts. This inherent flexibility ensures that MOSA-compliant systems can adapt and evolve over time to accommodate changing mission requirements and technological advancements. (Figure 6)

6.2 MOSA and CJADC2: Enabling Effective Swarm Operations

The DoD's CJADC2 initiative seeks to establish a connected battlespace where air, land, sea, space, and cyber forces can operate as a single, coordinated entity. This level of integration hinges on seamless communication, data exchange, and interoperability between disparate systems and platforms.

Here's where MOSA becomes a game-changer for swarm operations within CJADC2:

Standardized Interfaces: MOSA ensures that individual swarm elements, regardless of platform or manufacturer, can communicate and share data using common interfaces. This eliminates compatibility issues and allows for the integration of diverse unmanned systems (UxS) into a cohesive swarm architecture.

Modular Design and Open Architectures: By adhering to modular design principles, MOSA facilitates the development of scalable swarm capabilities. New UxS types or functionalities can be readily incorporated into the swarm without requiring a complete system overhaul. This modularity is vital for adapting swarm tactics to meet the demands of various operational scenarios.

Rapid Integration and Experimentation: The modular nature of MOSA-compliant systems coupled with open standards allows for faster integration of new technologies and capabilities. This rapid integration cycle is crucial for experimenting with different swarm configurations and tactics, enabling the development of more effective swarm employment strategies.

Simplified Logistics and Maintenance: The use of common interfaces and standardized components across MOSA-compliant UxS simplifies logistics and maintenance within a swarm. This translates to reduced downtime, improved operational efficiency, and overall cost savings.

In essence, MOSA provides the foundational building blocks for CJADC2 by ensuring interoperability and enabling the seamless integration of diverse systems and

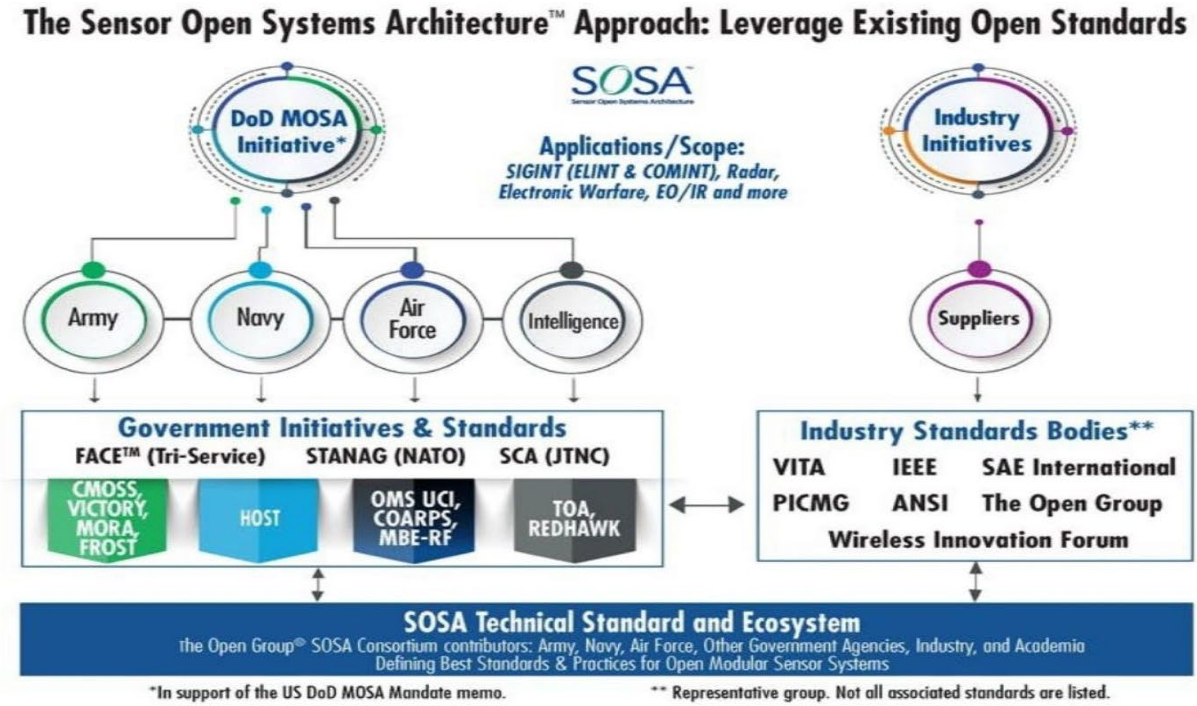

Fig. 6. Overview of the SOSA Technical Standard & Ecosystem.
Photo Credit: The Open Group's SOSA Consortium

platforms. This capability is particularly critical for swarm operations, where effective communication, data exchange, and coordinated action are paramount for mission success.

7. TECHNOLOGIES INTEGRATION WITHIN THE CJADC2 FRAMEWORK

7.1 Interoperability and Stability Efforts

Interoperability and standardization efforts are central to successfully integrating technologies within the CJADC2 framework for swarm operations. Adopting Modular Open Systems Approach (MOSA) principles facilitates interoperability by promoting open standards and interfaces, enabling seamless communication and collaboration between disparate systems and platforms. (Figure 7)

Fig. 7. UAVs equipped with specialized software and sensors fly during the Technical Concept Experiment at Marine Corps Base Camp Pendleton, Calif., Jan. 19, 2024. The event showcased multiple systems designed to enhance the ability to carry out amphibious operations.
Photo credit: Michael Walls, Navy

By adhering to MOSA standards, military forces can avoid vendor lock-in and ensure compatibility between AI-driven swarm management systems, legacy command and control infrastructures, and emerging technologies.

Additionally, adherence to established standards such as NATO STANAGs (Standardization Agreements) and IEEE (Institute of Electrical and Electronics Engineers) protocols further enhances interoperability, enabling multinational collaboration and information exchange in swarm environments.

Efforts to standardize data formats and communication protocols are pivotal in interoperability within the CJADC2 framework. By adopting common data standards such as XML (Extensible Markup Language) or JSON (JavaScript Object Notation), military forces can facilitate the seamless exchange of information between AI-driven swarm management systems, sensor platforms, and command and control centers.

Similarly, standardizing communication protocols ensures compatibility between diverse communication networks and facilitates real-time data sharing and coordination. Moreover, the development of standardized APIs (Application Programming Interfaces) enables interoperability between AI-driven systems and legacy command and control systems, allowing for the integration of advanced technologies while preserving existing investments in infrastructure.

7.2 Scalability and Flexibility of Technology Solutions

Scalability and flexibility are paramount when integrating technologies within the CJADC2 framework for swarm operations. By prioritizing scalability and flexibility in technology integration efforts, military forces can enhance their operational agility and effectiveness in addressing the challenges of swarm operations. This necessitates the deployment of flexible architectures and modular solutions that can accommodate changes in mission objectives, environmental conditions, and adversary tactics.

By leveraging scalable, open standards-based technology solutions, military forces

can allocate resources efficiently and respond effectively to swarm threats of varying scales and complexities.

Technology solutions must be agile and responsive to enable rapid reconfiguration and deployment in response to emergent swarm scenarios. This agility allows military forces to maintain operational tempo and adapt their plans in real-time, ensuring timely and effective decisions to evolving swarm threats. Additionally, flexibility in technology solutions enables interoperability between diverse systems and platforms, facilitating seamless communication and collaboration across all domains. (Figure 8)

Fig. 8. Flexible architectures and modular solutions enable operational agility to accommodate changes in mission objectives, environmental conditions, and adversary tactics.

7.3 Data Processing and Computation

In the past decade, a robust ecosystem of general-purpose graphic processing unit (GPGPU) systems has developed, which served as the catalyst to AI-based computing in military systems. GPGPU uses a parallel structure, with multiple small cores that process multiple tasks simultaneously.

As AI continues to grow and system size continues to shrink, computing systems will be expected to perform in increasingly remote, harsh environments. Military systems, such as distributed computing and signal processing in next-generation autonomous vehicles as well as surveillance, targeting and EW systems, need a rugged infrastructure with advanced GPGPU processing, that minimizes power consumption, as well.

Systems weighing less than 5.5 lbs. and measuring as small as 8.5” x 3.2” x 6.8” that incorporate NVIDIA’s cutting-edge GPGPU architecture, like the Jetson AGX Xavier-based A178 Thunder from Aitech, are providing a SWaP-optimized infrastructure that can easily handle the high-scale data computation needs to enable AI in unmanned operations.

Complete with CUDA cores and Tensor cores, which amplify the matrix processing of large data sets by enabling higher levels of computation with lower power consumption, these new AI systems can handle up to 32 TOPS (trillion operations per second) to provide local processing of high volumes of data closest to system sensors. This exceptional processing power gives these systems the adaptability to handle the multiple data sources incorporated in a typical unmanned system.

Adopting cloud-based architectures and software-defined technologies further enhances scalability and flexibility in swarm operations within CJADC2. Cloud computing enables military forces to dynamically allocate computational resources based on demand, allowing for rapid scaling of AI-driven swarm management systems and other critical applications.

Similarly, software-defined networking (SDN) and virtualization technologies allow users to adapt network configurations and protocols in response to changing operational requirements.

8. BEST PRACTICES IN IMPLEMENTING INTEGRATED TECHNOLOGY SOLUTIONS FOR SWARM OPERATIONS

Recent military experiments, demonstrations, and exercises such as Project Convergence have showcased the utilization of AI-driven swarm management systems, demonstrating coordination and adaptability in responding to simulated swarm threats. This exemplifies the potential of integrated technology solutions to enhance situational awareness, decision-making, and response coordination, echoing the objectives outlined in CJADC2 directives. (Figure 9)

Fig. 9. Field testing with the Inspired Flight 3 Drone during Project Convergence 2022 at Fort Irwin, Calif., Oct. 27, 2022 integrating technologies and concepts from all services and from multinational partners, including in the areas of autonomy, augmented reality, tactical communications, advanced manufacturing, unmanned aerial systems and long-range fires.
Photo Credit: Army Sgt. Woodlyne Escarne

Collaborative efforts between military branches, allied forces, and industry partners in developing and implementing integrated technology solutions for swarm operations embody the spirit of joint experimentation and prototyping emphasized in CJADC2 guidance. These initiatives allow stakeholders to test and validate new technologies in realistic operational scenarios, refining integration strategies and identifying areas for improvement.

Furthermore, partnerships with academia and research institutions facilitate innovation and knowledge exchange, enabling military forces to leverage cutting-edge technologies and methodologies in swarm operations in alignment with CJADC2 objectives for collaboration and interoperability.

Continuous evaluation and feedback mechanisms are integral to refining integrated technology solutions for swarm operations over time, echoing the iterative approach advocated by CJADC2 principles. After-action reviews and lessons-learned exercises provide opportunities to assess the effectiveness of deployed technologies and identify areas for optimization. By soliciting feedback from end-users and stakeholders, military forces can iterate on integrated technology solutions, addressing emerging challenges and evolving operational requirements.

Regular updates and enhancements to technology solutions ensure alignment with the latest advancements in AI, networking, and cybersecurity, enabling military forces to maintain a competitive edge in swarm operations within the CJADC2 framework. Thus, leveraging case studies, best practices, and continuous evaluation processes empowers military forces to maximize the effectiveness of integrated technology solutions in addressing swarm threats and achieving mission success, consistent with CJADC2 objectives for innovation and operational excellence.

9. ADDITIONAL CONSIDERATIONS FOR OPTIMAL EFFECT

Addressing cultural and organizational factors aligns with CJADC2 guidance, which emphasizes fostering a collaborative and innovative culture across military branches and agencies. Resistance to change, siloed organizational structures, and competing priorities may hinder collaboration and information sharing, echoing CJADC2 directives. Thus, leadership commitment is crucial in fostering a culture of collaboration,

innovation, and information sharing across organizational boundaries, which aligns with CJADC2 objectives.

Additionally, as emphasized by CJADC2, training and education programs are vital to equip personnel with the skills and competencies required to integrate and utilize advanced technologies in swarm operations effectively, supporting the overarching goals of the CJADC2 framework. By addressing integration challenges in alignment with CJADC2 lines of effort and guidance, military forces can unlock the full potential of technology integration for swarm operations, enhancing their readiness and effectiveness in modern warfare scenarios.

Swarm operations present unique challenges and opportunities for military ground forces within the CJADC2 framework. Coordinating large numbers of autonomous agents in dynamic and contested environments requires innovative approaches to command and control. Swarms may face issues with communication, synchronization, and maintaining cohesion. However, swarm operations offer significant advantages, including enhanced agility, redundancy, and scalability. (Figure 10)

The ability to respond rapidly and scale C5ISR operations is paramount for maintaining tactical advantage and achieving mission success within the CJADC2 framework. Rapid response capabilities enable ground operations to detect, assess, and adapt to dynamic swarms, minimizing the potential for disruption or exploitation by adversaries.

Additionally, scalability ensures that military forces can effectively command and control swarms of varying sizes and complexities across domains. Whether facing small-scale drone swarms or large-scale cyber swarms, the ability to scale operations allows military commanders to be flexible and adaptive to defeat adversary forces and prevent them from accomplishing their operational and tactical objectives.

Rapid response and scalability enhance operational resilience and agility, enabling military forces to maintain tempo and momentum in contested environments. By leveraging advanced technologies such as AI-driven decision support systems and time-

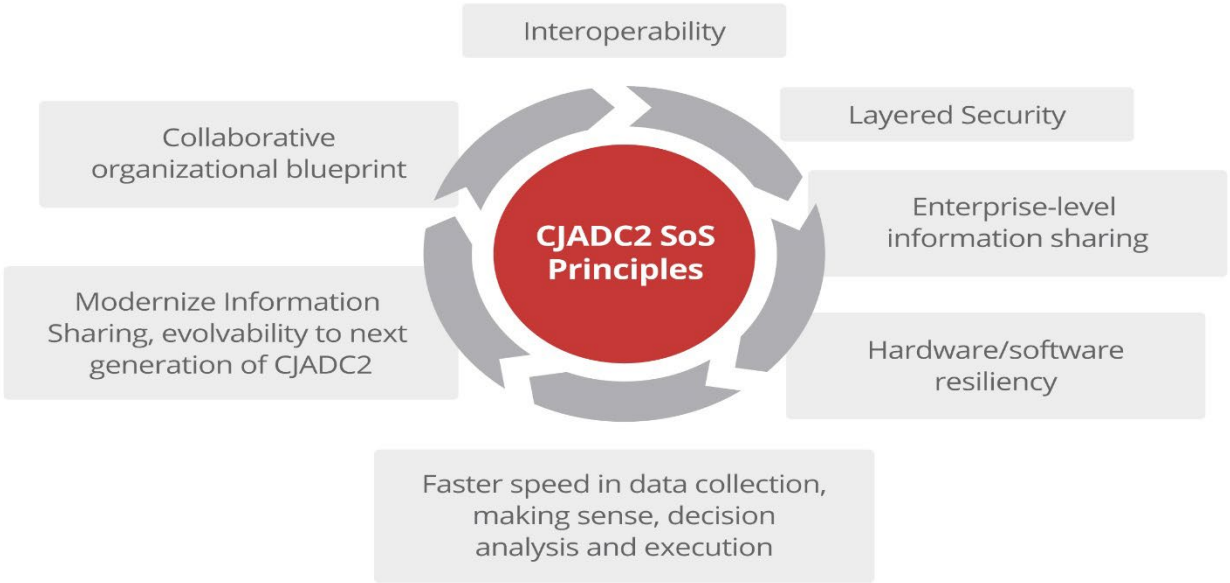

Fig. 10. CJADC2 System of Systems principles in action

sensitive networking protocols, military commanders can orchestrate rapid and coordinated responses to swarm threats, leveraging distributed sensor networks and autonomous systems for real-time situational awareness and engagement.

Additionally, scalable command and control architectures enable seamless integration of diverse assets and capabilities, including crewed and uncrewed platforms, cyber capabilities, and space-based assets, maximizing operational effectiveness across all domains. Rapid response and scalability are foundational elements of effective swarm operations within the CJADC2 framework, empowering military forces to outmaneuver and outpace adversaries in complex and dynamic operational environments.

10. REFERENCES

[1] R. R. Nilchiani, "Report on Joint All-Domain Command and Control (JADC2) Opportunities on the Horizon," Stevens Institute of Technology, Washington, DC, United States, November 2022. Accessed: January 15, 2024 [Online]. Available: https://document.acqirc.org/publication_documents/reports/1670425668.JADC2_REPORT.pdf

[2] J. R. Hoehn, "Joint All-Domain Command and Control (JADC2)," Congressional Research Service, Washington, DC, United States, Rep. no., (optional: vol./issue), January 21, 2022. Accessed: January 27, 2024. [Online]. Available: https://crsreports.congress.gov/product/pdf/IF/IF11493

[3] *Army Advances Learning Capabilities of Drone Swarms*. US Army CCDC Army Research Laboratory Public Affairs August 10, 2020, doi: https://www.army.mil/article/237978/army_advances_learning_capabilities_of_drone_swarms

[4] D. Hambling. "The US Navy Wants Swarms of Thousands of Small Drones." MIT Technology Review. https://www.technologyreview.com/2022/10/24/1062039/us-navy-swarms-of-thousands-of-small-drones/ (February 2, 2024).

[5] K. D. Thompson. "How the Drone War in Ukraine is Transforming Conflict." Council on Foreign Relations. https://www.cfr.org/article/how-drone-war-ukraine-transforming-conflict (February 2, 2024).

[6] R. Cheek. "Autonomous Swarm Drones New Face of Warfare." National Defense. https://www.nationaldefensemagazine.org/articles/2023/12/13/industry-perspective-autonomous-swarm-drones-new-face-of--warfare (retrieved February 2, 2024)

[7] J. Luckenbaugh. "Data Normalization, Distribution Key to CJADC2." National Defense. https://www.nationaldefensemagazine.org/articles/2024/5/9/algorithmic-warfare-data-normalization-distribution-key-to-cjadc2 (retrieved July 11 2, 2024)

[8] J. Clark. "Hicks Announces Delivery of Initial CJADC2 Capability." US Department of Defense. https://www.defense.gov/News/News-Stories/Article/Article/3683482/hicks-announces-delivery-of-initial-cjadc2-capability/ (retrieved July 11, 2024)