

THE ARMY

SD 16

UNIFIED NETWORK PLAN 2.0



AIR



LAND



CYBER

**TRANSFORMING
THE UNIFIED NETWORK
AT ECHELON**



SEA



SPACE

Contents

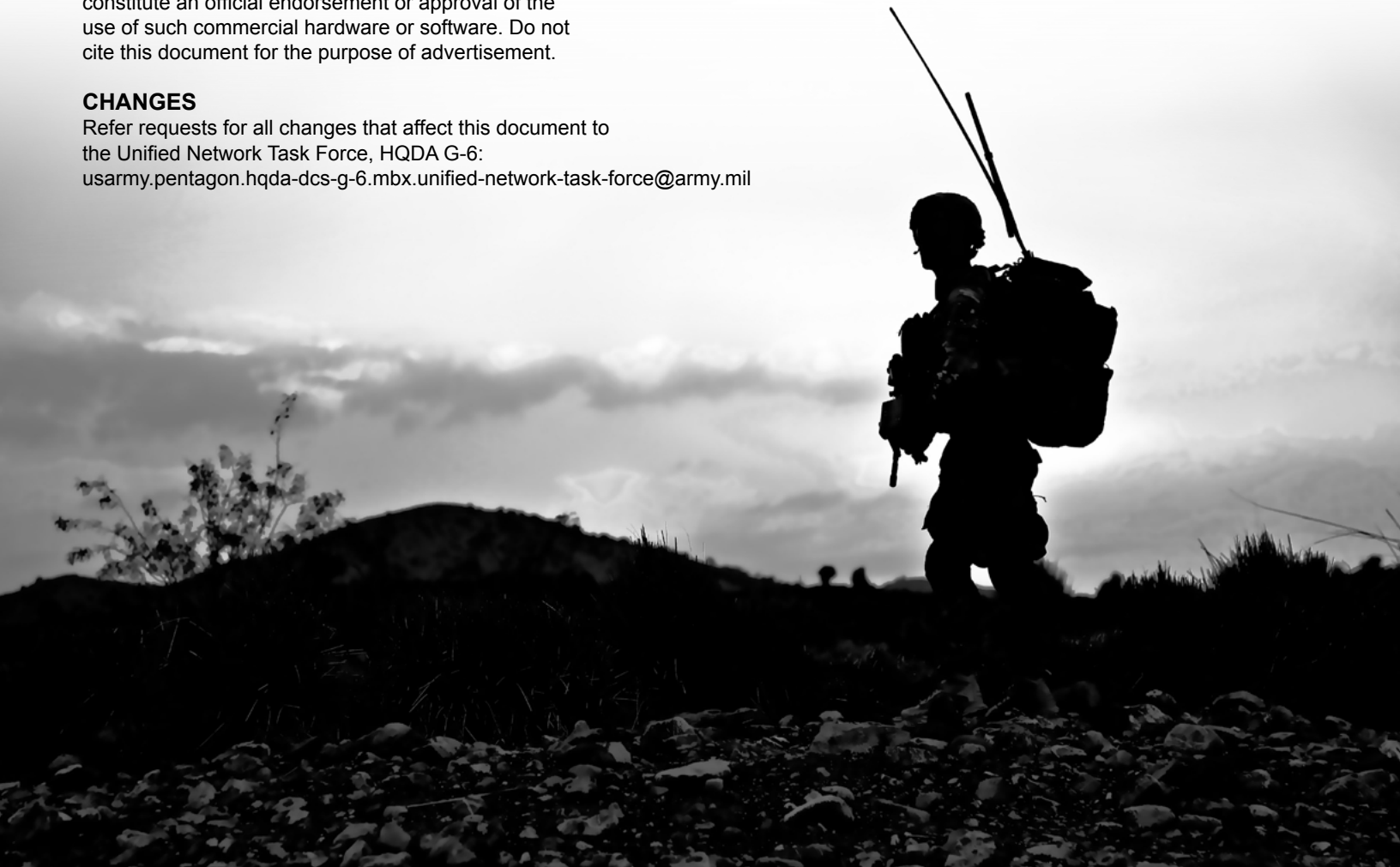
Executive Summary	2
Introduction	3
Defining the Army Unified Network – The Enabler for Multidomain Operations	4
Strategic Approach.....	5
Line of Effort #1: Establish the Unified Network	6
Line of Effort #2: Posture the Force to Support MDO	7
Line of Effort #3: Security and Survivability Based on Zero Trust Principles	9
Line of Effort #4: Transform the Army’s Unified Network Investments, Policy, and Governance	10
Line of Effort #5: Continuously Improve the Unified Network	10
Conclusion	11

DISCLAIMER

The use of trade names in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for the purpose of advertisement.

CHANGES

Refer requests for all changes that affect this document to the Unified Network Task Force, HQDA G-6:
usarmy.pentagon.hqda-dcs-g-6.mbx.unified-network-task-force@army.mil



Executive Summary

The initial Army Unified Network Plan (AUNP), published in 2021, provided a roadmap for the development of a Unified Network to meet the changing character of war and deliver the critical capabilities the Army needs to succeed in volatile, congested, and contested environments. It set a strategy to unify Army networks with common standards, systems, and processes to reduce complexity and increase integration. Since then, a confluence of emerging technologies and events has transformed the world into a multidomain, persistently contested information environment that demands a far more data-centric approach to harness the power of the Army Network to fight and win.

The AUNP 2.0 builds on the foundation of the original AUNP and prepares the force for data-centricity through the integration of Zero Trust principles.

The Army requires secure and timely access to data to inform decision making. The AUNP 2.0 provides an overarching strategic framework, linking information technology standards, policies, and principles across regions, formations, and echelons, whether connected or disconnected. The Unified Network must continue to adapt to incorporate new technologies more quickly and at scale, while simultaneously reducing the cognitive burden at the edge.

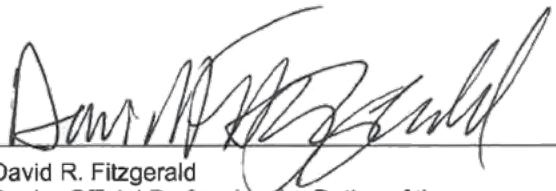


The AUNP 2.0 operationalizes the Unified Network by focusing on how the Army's network moves and secures data to outpace our adversaries through multidomain operations (MDO) up to, and including, large-scale combat operations. AUNP 2.0 represents a fundamental shift from establishing the Unified Network foundation to enabling data-centricity by bringing the global network and common data requirements to theaters, rather than an uneven federation of networks and standards across theaters.

AUNP 2.0 retains five Lines of Effort (LOE) critical to shaping the future Army:

- **LOE 1: Establish the Unified Network**
- **LOE 2: Posture the Force to Support MDO**
- **LOE 3: Security and Survivability based on Zero Trust Principles**
- **LOE 4: Transform the Army's Unified Network Investments, Policy, and Governance**
- **LOE 5: Continuously Improve the Unified Network**

As the Army defends our national interests from malign influence of increasingly sophisticated adversaries, our shared ownership of the AUNP 2.0 will be central to ensuring a more responsive, agile, and survivable network in support of MDO.


David R. Fitzgerald
Senior Official Performing the Duties of the
Under Secretary of the United States Army


James J. Mingus
General, United States Army
Vice Chief of Staff

Introduction

The initial Army Unified Network Plan (AUNP) was published in 2021 to address network gaps associated with the changing character of war from episodic and regional to transregional and global. It set strategic priorities to unify Army Networks with common standards, systems, and processes to reduce complexity and increase integration. Since then, a confluence of emerging technologies and events has transformed the world into a multidomain, persistently contested information environment that demands a far more data-centric approach to harness the power of the Army Network to fight and win.

The original AUNP set the foundational framework for common standards and security across a Unified Network. During Phase I of the AUNP, the Army consolidated 11 of 13 organizational networks to enhance operational capability, improve network security, and establish a data fabric integrated by a data mesh¹. Network and cyber capabilities are now centrally managed and delivered to the force by U.S. Army Cyber Command (ARCYBER) to ensure consistent, reliable, and integrated capabilities across the force. The Assistant Secretary of the Army for Acquisition, Logistics and Technology (ASA(ALT)) streamlined modernization efforts by consolidating network acquisition under a single Program Executive Office (PEO). Resource allocation decisions including those related to software licensing are now aligned under the Digital Program Evaluation Group (DD PEG) to improve oversight and provide decision space for investments and maintenance. Finally, the Signal and Cyber force structures and systems have been realigned to support multidomain operations (MDO).



The AUNP 2.0 builds on this foundation and prepares the force for data-centricity through the integration of Zero Trust (ZT) principles aligned with Department of Defense (DoD) and Joint Staff policies and directives. It is a strategic guide to operationalize the Unified Network through a focus on ZT principles that improve how the Army's network moves and secures data. The plan incorporates observations and lessons learned from ongoing operations around the globe, as well as best practices for security. Static command posts are no longer uncontested in combat operations; neither are our data or network. As with command posts, the network and data must be agile, adaptable, and able to rapidly move to the point of need even in a denied, disrupted, intermittent, and limited bandwidth (DDIL) environment. Whereas past network strategies homed in on perimeter defense and hardware, the AUNP 2.0 is focused on common principles and standards to centrally deliver and manage the network and data.

Key AUNP 2.0 framework principles include:

- **Integrate ZT and data-centricity.**
- **Reduce or eliminate information technology (IT) complexity at the edge.**
- **Centralize IT service delivery and resourcing.**
- **Establish and employ common standards, processes, and systems.**
- **Drive warfighter priorities for Command and Control (C2) in support of MDO and DDIL.**
- **Enable faster, secure data sharing with partners, allies, and across security domains.**
- **Develop CONOPS and validated operational requirements at echelon.**

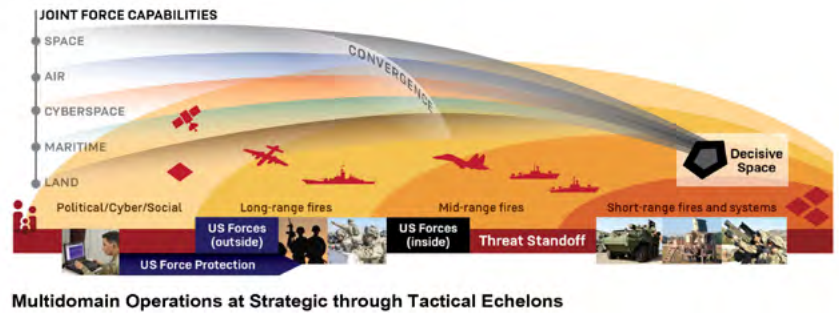
The Chief of Staff of the Army made the network the Army's number one transformation priority because it cuts across nearly all other transformation efforts. With the Unified Network foundation of ZT implementation and convergence of organizational networks, the Army is ready for the data-centric command and control (C2) capabilities to rapidly adapt to a complex threat environment characterized by accelerating technology transformation.

¹See Unified Data Reference Architecture (March 2024).

Defining the Army Unified Network – The Enabler for Multidomain Operations

The Unified Network employs a Common Operating Environment (COE), Common Services Infrastructure (CSI), and Common Transport Layer (CTL), bolstered by Unified Network Operations (UNO) and Centralized Delivery of Services (CDS), including a robust set of cyber defense capabilities.

The AUNP 2.0 framework is based on eight (8) ZT principles: never trust, always verify explicitly; presume breach; hybrid work and location agnostic; incorporate DOTmLPF-P²; simplify and automate; least privilege; scrutinize and analyze behavior; and architectural alignment (DoD ZT Strategy, dated October 21, 2022).



Common Operating Environment. The COE furnishes computing technologies and standards that facilitate secure and interoperable applications capable of processing data at the pace demanded by military operations. By leveraging COE, commanders can effectively oversee distributed forces from any location worldwide, utilizing agile, data-driven decision-making tools. The COE provides essential common information services that establish a unified operating environment, integrating tactical computing environments seamlessly with national or strategic assets. This integration enables the execution of MDO swiftly and across extensive distances.

Common Services Infrastructure. The CSI offers universally accessible hardware and software that securely store, compute, and manage data. It facilitates data analytics, artificial intelligence (AI), and machine learning (ML) to enable data-driven decision-making capabilities across the force. CSI optimizes the utilization of commercial cloud services, hybrid cloud capabilities, and other modern “as-a-service” models, ensuring access to centrally managed data assets at the point of need.

Common Transport Layer. The CTL provides robust, scalable, secure, and resilient pathways for global delivery of data, information, and collaborative services to commanders across any environment and device. Operating on a unified, transport-agnostic model, CTL integrates software-defined networking (SDN), open system architectures, commercial transport, and encryption technologies. Implementing these advancements ensures a common level of security and availability so command posts can operate with the same effectiveness as home-station operations centers. Soon, 5G and future technologies at all levels will enable an integrated “Internet-of-Things” distribution network for end devices, seamlessly linking base operations to the tactical edge. Additionally, commercial wireless and optical technologies enhance the mobility, agility, and security of network connections.

Unified Network Operations. UNO provides the network and systems management capabilities to design, plan, model & simulate, secure, configure, operate, extend, maintain, and sustain the Unified Network. It equips network operations personnel to monitor and safeguard the network comprehensively, supporting visibility, security, maintenance, and rapid response capabilities. UNO seamlessly integrates these functions across Enterprise, Tactical, and Mission Partner Networks. It also ensures network availability and operational flexibility within the cyber domain, crucial for commanders executing MDO. It employs a suite of integrated software-centric tools and applications employing ZT principles, facilitating integrated activities across the Operating Environment, Services Infrastructure, and Transport Layer.

The alignment, standardization, and integration of core network foundations—Transport, Computing, Services, and Infrastructure—supported by Unified Network Operations and cybersecurity capabilities, are operational imperatives. They establish the bedrock for a Unified Network capable of global, cross-domain maneuver and the application of strategic, operational, and tactical effects at the speed and range essential for Army and Joint/Coalition Forces in tomorrow’s evolving battlefield.

Centralized Delivery of Services. The Army consolidated IT service delivery under ARCYBER as the sole provider, accelerating service consistency and enhancing network visibility. Centralizing services under one provider eliminated unnecessary redundancies resulting from ad hoc procurements, resulting in a streamlined, integrated, and fiscally responsible approach to delivering services. A list of baseline services to be delivered under the Centralized Delivery of Services concept is published in the Army Unified Network Service Catalog and is reviewed annually.

²Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy

Strategic Approach

The AUNP 2.0 is organized around five lines of effort (LOE) and synchronizes Unified Network modernization in three phases. Phase I was completed in 2023. AUNP 2.0 furthers those efforts and enables the Army Campaign Plan over two subsequent phases based on core principles. This approach is intended to align personnel, organizations, and capabilities essential for enabling effective MDO.

PHASE II: NEAR TERM (2024 - 2026)—OPERATIONALIZE THE UNIFIED NETWORK

Leveraging the architecture established in Phase I, this phase began in fiscal year 2024 (FY24) and continues today with a focus on modernization activities to maximize the centralized delivery of services and access to the Unified Network. Primary efforts in Phase II include:

- Complete the operations construct for the Army's portion of the Department of Defense Information Network (DODIN-A) with supporting force structure to enable defense and operation of the Unified Network in a contested and congested environment.
- Modernize and implement the Army's hybrid compute capability in support of tactical formations in DDIL environments. This capability should be integrated with the Army Cloud Strategy.
- Establish a persistent Mission Partner Environment (MPE) and associated funding strategy, inclusive of all hardware, software, infrastructure, sustainment, and people from the tactical edge back to the enterprise and employ it at all Combat Training Centers (CTCs) and Mission Training Complexes in accordance with Joint and DoD directives and initiatives.
- Optimize the Army's network capability to enable data-centric warfighting. Establish and operationalize the Digital Program Evaluation Group (DD PEG).
- Organize, optimize, and synchronize data flows to ensure accurate and timely information is available where it is needed most, whether at the tactical, operational, or strategic levels via the Army data orchestration.
- Transition to Internet Protocol version 6 (IPv6), SDN, and a common service management platform.
- Reduce or eliminate undue complexity associated with administrative processes while maintaining effective governance. Examples of areas of focus include but are not limited to the Information Technology Approval System (ITAS) and cross domain solution (CDS) provisioning.
- Identify and report metrics at echelon, linked to Machine Learning-based predictive readiness.
- Deliver a structured framework/architecture to depict and guide modernization activities, centralize service delivery, and enhance access to the Unified Network.
- Identify and ensure systems/services support the decision-making processes that enhance operational effectiveness and mission success.

This phase ends with the establishment of a Unified Network based on Zero Trust principles, enabling the seamless transfer of data across all echelons, postured to support MDO.

PHASE III: MID-TERM (2027 AND BEYOND)—CONTINUOUSLY MODERNIZE AND TRANSFORM THE UNIFIED NETWORK

This phase begins with a Unified Network based on Zero Trust principles postured to support MDO. Primary efforts in Phase III include:

- Full implementation of a holistic approach to modernize the Unified Network over time, leveraging emerging technologies while divesting of legacy capabilities.
- Final integration of Zero Trust Architecture.
- Continued integration with the Joint/Coalition Force and mission partners.

Several emerging technologies shape this phase, including but not limited to:

- Dynamic and diverse transport, robust computing, and edge sensors.
- Data-centric data management technologies and platforms with tagging/labeling at the source.
- Robotics and autonomous operations.
- Corresponding cybersecurity and resiliency capabilities.
- Quantum-resistant encryption and technologies.
- Further integration of mission focused AI/ML models and capabilities.

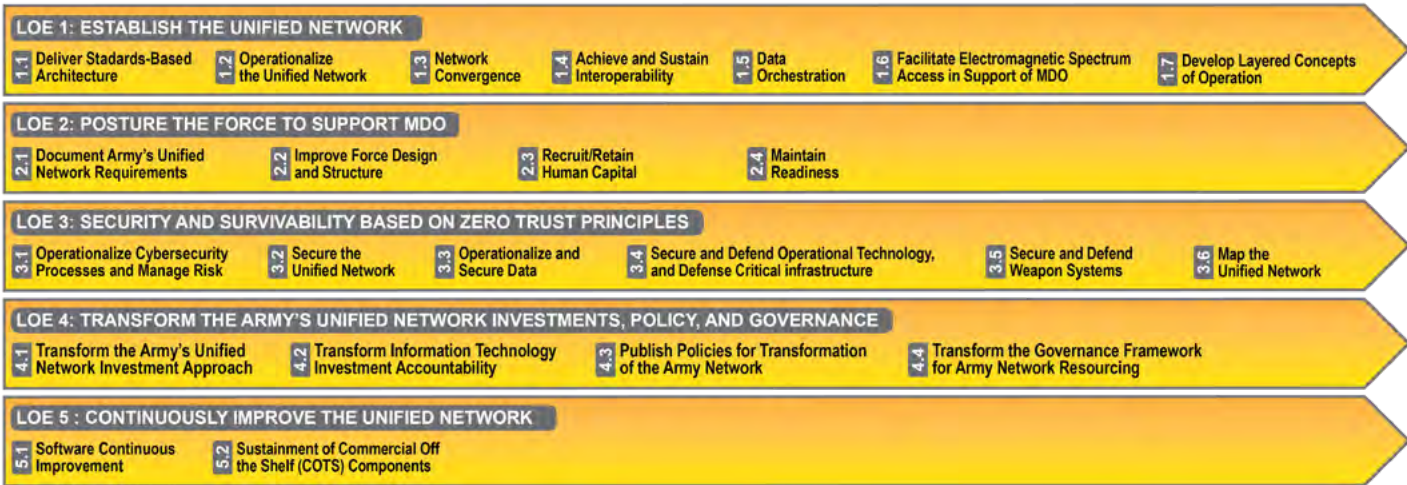
Given the rapid change of information technology in the cyber domain, there is no end to this phase—modernization remains enduring. It is a continuous process and there is no set end state for the Unified Network.

A Headquarters, Department of the Army Execution Order (EXORD) implements the AUNP. The EXORD decomposes the AUNP into key tasks over near- and mid-term time horizons. As the lead for AUNP integration, the Deputy Chief of Staff, G-6 will synchronize and assess efforts across the Total Force and all mission areas to set the Unified Network to support the MDO-capable Army.

Army Unified Network Plan Lines of Effort and Objectives

LINE OF EFFORT #1: ESTABLISH THE UNIFIED NETWORK

LOE 1 enables the integration and alignment of Unified Network capabilities and converges multiple, disparate organizational networks into the Army Unified Network. These efforts facilitate the seamless delivery of data to the right place at the right time, modernizing communications across the Unified Network. Central to this LOE is synchronizing network modernization across the Army. Further, this LOE maintains a secure pipeline that can deliver applications and capabilities to endpoints across the network. Additionally, this LOE will establish the Unified Network as the Army’s contribution to the DODIN-A as well as establish the Army’s Mission Partner Environment to interoperate with Allies and other Coalition partners.



OBJ 1.1: Deliver a Standards-Based Network Architecture. This objective focuses on the definition, design, and documentation of Army IT Standards Technical Profiles to inform a network design linking ZT principles, mission capabilities, systems integration, and data and information flows. The Army will establish an architecture that is resilient, secure, and able to store and transport data and information seamlessly among the strategic, operational, and tactical levels.

OBJ 1.2: Operationalize the Unified Network. This objective seeks to modernize and improve network infrastructure, improve capability, and reduce the cognitive burden of network operations. Critical to this effort is the centralized delivery of services allowing “plug and play” capability across the Unified Network. This objective includes efforts to optimize redundant and obsolete capabilities. Finally, it includes the implementation of new solutions designed to make the Army more effective and dynamic in how it delivers data without sacrificing service quality. The Army is reimagining the way services and data are delivered to endpoints.

The network is the catalyst for Army operations across all warfighting functions. Modernization must occur from the tactical edge to the strategic backbone and create a resilient, secure, maneuverable Unified Network. This objective modernizes network capabilities, enabling initiatives already underway including assured network transport, Common Operating Environment (COE), MDO-capable command posts, and Joint/Coalition interoperability at the edge. Network capabilities must support forces distributed across vast distances, converge effects from multiple domains, and maintain a common situational understanding in MDO.

OBJ 1.3: Network Convergence. This objective converges separate organizational networks, both vertically and horizontally, across all Army components, while also rationalizing and consolidating network management tools and personnel. The Army will deliver a resilient Unified Network optimized to increase speed and range while being maneuverable and defensible. This objective collapses stove-piped, vulnerable networks into the Unified Network while integrating DODIN-A Operations capabilities across the Army and gaining fiscal efficiencies.

OBJ 1.4: Achieve and Sustain Interoperability. To fight and win in the next generation of warfare, the Army must be prepared to operate as part of a Joint or Coalition force. The modern operational environment necessitates robust access to secure and persistent mission partner networks and environments capable of sustaining combat operations. Existing mission partner environments lack a persistent capability essential for rapid deployment and immediate operational readiness. This objective aims to establish, integrate, and secure persistent mission partner networks, supported by an effective data strategy. This approach ensures data-informed decision making within integrated battlespace environments. Achieving and maintaining this interoperability demands proficiency in human, procedural, and technical dimensions.

OBJ 1.5: Data Orchestration. In her memorandum dated February 8, 2022, the Secretary of the Army stated, “[m]y second objective is to ensure the Army becomes more data-centric and can conduct operations in contested environments, which will enable our ability to prevail on the future battlefield.” Accordingly, this objective organizes, optimizes, and synchronizes data flows and data product production to ensure accurate and timely information at the point of need across all echelons via the Army Data Orchestration initiative. Data orchestration plays a crucial role in enhancing situational awareness, operational effectiveness, and mission success by enabling commanders and other decision makers to have timely access to accurate and relevant information. It supports the Army’s goal of leveraging data as a force multiplier in modern warfare scenarios. Essential to this objective is the identification of data requirements, data products, and the technical, policy, and regulatory elements impeding data flow and efforts to overcome identified constraints and restraints. Efforts under this objective must be integrated with the Army’s hybrid cloud strategy and architecture.

OBJ 1.6: Facilitate Electromagnetic Spectrum Access in Support of MDO. Objective 1.6 focuses on enabling electromagnetic spectrum (EMS) access to support MDO. This objective mandates the execution of the National Spectrum Strategy Implementation Plan, emphasizing the development of Dynamic Spectrum Sharing capabilities to advance 5G, 6G, and NextGen wireless technologies. Coordination with national regulators and government agencies is crucial to support electromagnetic warfare test and training events, as well as to allocate frequencies for the research and development of C2 systems and other EMS-dependent technologies. Advocacy efforts through the DoD Chief Information Officer (CIO) and the Department of State aim to secure global EMS access for AUNP wireless systems and other EMS-dependent systems. Additionally, coordination is required to ensure EMS access for tactical data links (e.g., Link 16) and to certify EMS-dependent systems with both the U.S. National Regulator and foreign host nations through Combatant Commands.

OBJ 1.7: Develop Layered Concepts of Operation. The Army must develop layered concepts of operation (CONOPS) to operationalize the objectives and tasks captured in the AUNP 2.0. This objective directs the development of layered CONOPS detailing roles and responsibilities for network and data-enabling activities by echelon to provide clarity and enable synchronization of effort across the force.

LINE OF EFFORT #2: POSTURE THE FORCE TO SUPPORT MDO

LOE 2 focuses on the integration of the AUNP by applying ZT principles and a data-centric approach across doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTmLPF-P). Foundational to this LOE is the development of strategic and tactical capability documents, including the transition to the Fix and Pivot initiative. It considers the roles and impact the AUNP has on our military and civilian personnel and provides the training and organizational constructs to successfully compete and win in MDO. The Army must synchronize and integrate its organizational, people, training, and talent management initiatives to keep pace with rapid technological evolution.



OBJ 2.1: Document the Army's Unified Network Requirements. The Army must prepare the Cyber, Signal, and Unified Network enabling workforce with the appropriate facilities, systems, infrastructure, and training to operate the Unified Network. Unified Network requirements are codified in four base documents – (1) the UNO Information Systems - Initial Capability Document (IS-ICD) with Requirement Definition Packages (RDP) and Software Capability Needs Statements (SW CNS); (2) the Enterprise Computing Environment SW CNS; (3) the currently approved Enterprise Transport Modernization Capability Development Document (CDD), with future enterprise network requirements being subsumed into the Configurable C2 Transport CDD; and (4) the Configurable C2 Services Infrastructure CDD. The UNO IS-ICD and its RDPs and SW CNS provide network and systems management capabilities to design, plan, model and simulate, secure, configure, operate, extend, maintain, and sustain the Unified Network and its data. The Enterprise Computing Environment SW CNS will codify the critical enterprise portion of the Common Operating Environment, which will enable tactical formations to leverage strategic capabilities. The modernization of the Army's transport infrastructure on posts, camps, and stations is in the Enterprise Transport Modernization CDD and in the future will be captured with all transport requirements in the Configurable C2 Transport CDD. The Configurable C2 Services Infrastructure CDD serves as the base document to allow the Army to provide globally accessible, common hardware and software services designed to secure, store, and compute data for Unified Networks evolution.

OBJ 2.2: Improve Force Design and Structure. The Army is currently updating its Cyber and Signal force structure to support the Army's transformation to an MDO-capable force by 2030. One key element of this effort revolves around the Division Signal Battalion (DSB). When implemented, the DSB ensures commanders can task organize Signal formations to enable operations, employ Unified Network platforms and services to enable frequent movement/maneuver of Brigade Combat Teams, and reach back to resilient/persistent cloud environments – with complexity for managing and securing critical data flows at the highest echelon possible. This critical objective enables the Army to design and implement a DODIN-A Operations construct that enables global operations, fully integrates defensive cyberspace operations at echelon, supports the implementation of cloud capabilities to enable mission-focused AI capabilities and speed of decision making, and reduces technical complexity at the edge by consolidating the most complex tasks at the appropriate operational echelon.

OBJ 2.3: Recruit/Retain Human Capital. People drive success. Our people are vital to our ability to dominate in MDO. This objective aligns with the Army Strategy's call to take care of our people. We will enable talent management strategies that optimize the Army's ability to recruit, develop, and retain a high quality and highly skilled Cyber, Signal, and Unified Network enabling workforce of Soldiers and Civilians to support operations at all echelons.

OBJ 2.4: Maintain Readiness. The Army cyber workforce and capabilities must be ready to enable land power dominance against near-peer competitors in MDO. This objective will ensure the Army Service Component Commands possess the skills and capabilities to maximize combat readiness in their respective theaters in accordance with their Combatant Commander's requirements and operational plans. This will include ensuring continuous transformation in operational units through home station training. Every Soldier must be able to operate their assigned network capabilities and the Army must continuously adapt Cyber and Signal training to account for the rapid evolution of network and data-sharing technologies – in both institutional and home station training.



LINE OF EFFORT #3: SECURITY AND SURVIVABILITY BASED ON ZERO TRUST PRINCIPLES

The Army must reform its current cybersecurity approach, primarily the Army's Risk Management Framework, by reducing repetitive, time-intensive, and burdensome processes. The Army must instead focus on transforming tactics, techniques, tools, and procedures to enable continuous monitoring and continuous assessments. The Army must be able to protect its ever-increasing attack surface area of both traditional information technology, non-traditional operational technology (OT), and critical infrastructure assets, while still adopting commercial technologies where appropriate. The National Defense Authorization Act for Fiscal Year 2022 defined OT as "control systems or controllers, communication architectures, and user interfaces that monitor or control infrastructure and equipment operating in various environments, such as weapon systems, utility or energy production and distribution, or medical, logistics, nuclear, biological, chemical, or manufacturing facilities."



OBJ 3.1: Operationalize Cybersecurity Processes and Manage Risk. To enable cyberspace operations at the speed required for MDO, the Army is implementing enhanced techniques and policy to mitigate vulnerabilities in the Unified Network with a priority on cloud/forward facing capabilities. The Army must address network accessibility, resiliency, and defense requirements. The intent is to operationalize our current cybersecurity processes, beginning with ensuring standardization of the Cyber Security Service Provider (CSSP) and improved defense of the DODIN-A.

OBJ 3.2: Secure the Unified Network. Securing the Unified Network includes fielding and integration of critical network capabilities for networks both within and outside the Continental United States, and a security architecture based on ZT principles as described in the DoD Zero Trust Strategy, all of which will increase network visibility and be common to all echelons. The main effort for this objective is to secure the Unified Network to support MDO during competition, crisis, and conflict on a global scale. ARCYBER will deploy defensive cyber capabilities across the Unified Network to enable defenders at echelon to gain and maintain the advantage, and Cyber Protection Teams to rapidly maneuver and hunt for adversaries within the network.

OBJ 3.3: Operationalize and Secure Data. At echelon, the Army will determine data security requirements necessary to maintain decision and information dominance. The Army must enable data management activities, such as ingestion, processing, and storage. It must also prevent unauthorized access, sharing, use, or transfer of data. Through this objective, the Army will establish a data governance structure to address the enterprise. This objective drives the continued focus on simultaneously enhancing data security and usage through various means including the modernization of encryption technology and incorporating methods to secure algorithms. Data security requires implementing controls to ensure only authorized entities have access to required data and that the data retains its integrity throughout its use. Whereas past network strategies homed in on perimeter defense and hardware, the AUNP 2.0 is focused on common principles, standards, and Unified Data Reference Architecture (UDRA) to enable data sharing.

OBJ 3.4: Secure and Defend Operational Technology and Defense Critical infrastructure. In accordance with section 1505 of the National Defense Authorization Act for Fiscal Year 2022, not later than January 1, 2025, the Army will consolidate and strengthen the defense capabilities of local cybersecurity and network forces to ensure comprehensive defense of operational technology assets and industrial control networks, especially Defense Critical Assets and Task Critical Assets. The Army will also implement advanced training programs, utilize cutting-edge defensive technologies, and execute the CIO's policies to ensure a robust defense of Defense Critical Assets and Task Critical Assets in the operational technology domain, supported by specialized, highly skilled forces. Employing predictive maintenance and machine-learning (ML) algorithms to inform risk and strategy is central to this objective.

OBJ 3.5: Secure and Defend Weapon Systems. Every weapon system is connected to the Unified Network. The Army will continue its Cyberspace Operational Resiliency Assessment-Platform (CORA-P) program to evaluate the cyber vulnerabilities of our major weapon systems. The Army will establish a means to assess, resource, and mitigate operational risk from cyber vulnerabilities of major weapon systems from a peer or near-peer adversary throughout the life cycle of those systems.

OBJ 3.6: Map the Unified Network. Mapping the network visualizes physical and virtual networks to monitor performance, identify avenues of attack, locate malicious activity, and enable commanders to make decisions faster than adversaries. The Army must have visibility of the Unified Network's components and data to effectively prevent, protect against, mitigate, respond to, and recover from cyber events. Under this objective, the Army will enable secure interoperable applications to process data at the speed of war, through a Unified Network Common Operating Picture (COP) with ML predictive readiness indicators.

LINE OF EFFORT #4: TRANSFORM THE ARMY'S UNIFIED NETWORK INVESTMENTS, POLICY, AND GOVERNANCE

LOE 4 works to transform how the Army invests in, issues policies for, and governs the resourcing of IT for the Unified Network. This LOE will transform the Army's approach for investing in IT that supports the network, transform the Army's solution for IT portfolio management and how Army organizations are held accountable for investing in IT, establish a repeatable and effective publishing process along with a series of policies to transform the DODIN-A and its tactical extensions, and transform the Army's governance framework for resourcing the Unified Network.

OBJ 4.1: Transform the Army's Unified Network Investment Approach. The Army will transform its approach to IT investments for the Unified Network and cybersecurity including prioritization of foundational ZT activities from legacy to digital. The Army will implement the digital construct, the Digital PEG, and the supporting auditability solutions for resourcing the Unified Network and gaining auditability and accountability thereof. The end state will be a consistent, repeatable, and auditable resourcing approach, integrated and aligned with the Army's Planning, Programming, Budgeting, and Execution (PPBE) process.

OBJ 4.2: Transform Information Technology Investment Accountability. The Army will update policy, programs, and processes for more efficient and effective solutions that ensure accountability for IT investments and their supporting procurements in the year of execution. This objective will update the Army Portfolio Management Solution (APMS) and the ITAS. The end state is to provide near-real-time visibility of the Army's IT investments and spending. As a result, Army leaders will be able to make data-driven decisions for IT investments and programs.

OBJ 4.3: Publish Policies for Transformation of the Army Network. The Army will establish a repeatable and effective process for publishing IT policy and guidance along with a series of policies to transform the DODIN-A and its tactical extensions. The end state will be a series of published guidance memorandums and Army IT regulations that include guidance for capabilities and IT solutions on the Unified Network.

OBJ 4.4: Transform the Governance Framework for Army Network Resourcing. The Army will transform its governance framework for resourcing the Unified Network. This objective will establish a more efficient and effective governance framework that integrates information from the Army Unified Network Council (AUNC) as the primary decision forum for IT resourcing and the Army Business Council (ABC) as the Army's validator for business system requirements to modernize the Unified Network across the DODIN-A and its tactical extensions. The end state will be that the Army has validated and prioritized IT resources supporting the Army Unified Network and its tactical extensions while enabling warfighting priorities.

LINE OF EFFORT #5: CONTINUOUSLY IMPROVE THE UNIFIED NETWORK

It is imperative that network sustainment enables core capabilities at echelon aligned with mission objectives. The aim is to ensure logistics and personnel support are provided efficiently to extend operational duration for mission success. This involves transforming force provider needs into custom support services to meet life-cycle requirements such as availability, reliability, and cost-effectiveness. Sustainment elements include supply chain, maintenance, transport, engineering support, data handling, configuration management, human integration, environmental standards, security measures, supportability, compatibility, and predictive readiness.



OBJ 5.1: Software Continuous Improvement. Army Directive 2024-02 (Enabling Modern Software Development and Acquisition Practices) states that software is no longer developed, tested, procured, operated, and sustained sequentially. Modern software development requires adoption of a continuous integration and continuous delivery/continuous deployment (CI/CD) model where software is iteratively developed and upgraded throughout the development life cycle. However, current processes do not support this model. Current fiscal rules dictate that systems that have transitioned to sustainment are limited to Operations and Maintenance, Army (O&MA) funding, which can only be used for software modifications. This construct prevents software from being iteratively developed throughout its life cycle. This objective seeks to drive implementation of the modern software development and acquisition practices identified in Army Directive 2024-02 and any subsequent guidance.

OBJ 5.2: Sustainment of Commercial Off the Shelf (COTS) Components. COTS acquisitions present a novel sustainment strategy to support rapid fielding. The initial warranty-based strategy includes a timely transition to sustainment decision point to allow adequate sustainment planning, should COTS systems transition to a program of record. The materiel solutions warranty approach promotes ease of component removal and replacement to mitigate unmanageable safety or health hazards. Program Managers, with the support of the product support managers, will develop and implement sustainment programs addressing each of the integrated product support elements to deliver affordable readiness.

Conclusion

The Army Unified Network Plan 2.0 marks a significant advancement in preparing our force for the priority efforts associated with implementing ZT principles and data-centricity. As warfare continues to evolve across multiple domains and our adversaries challenge our historical dominance, the Army's dedication to integrating and modernizing its network infrastructure is crucial. The Unified Network is essential to the future force's success, enabling seamless and effective operations across air, land, sea, space, and cyberspace.

Through five strategic lines of effort, this plan enhances the Army's ability to execute MDO while ensuring the necessary security, agility, and interoperability to stay ahead of adversaries. Through our shared ownership, collaboration, and innovative leadership, the AUNP 2.0 sets a direction for technological superiority and operational readiness for an uncertain future.





U.S. ARMY