THE ARMY UNIFIED NETWORK PLAN

2021

THE ARMY UNIFIED NETWORK PLAN ENABLING MULTI-DOMAIN OPERATIONS

This page intentionally left blank.

Executive Summary

The global security environment is increasingly complex and characterized by challenges to the free and open international order and the re-emergence of long-term, strategic competition between nations. Rapid advancements in technologies, coupled with the rise of near-peer competitors, will fundamentally change the operating environment on future battlefields. To address the changing character of war, the Army has embarked on its most expansive modernization program in 40 years. At the core of the Army's transformation is enabling Multi-Domain Operations (MDO) – the ability to operate, compete, and, if necessary, fight and win in all domains – air, land, sea, space, and cyberspace.

As the Army transforms into an MDO-capable Force by 2028, it must also transform its approach to network modernization. The MDO-capable Army of tomorrow must have a Unified Network that enables our Army, as part of the Joint/Coalition Force, to integrate and operate simultaneously and seamlessly in all domains, all environments, across all geographies and all warfighting functions, and enables the Army to calibrate a force posture and converge capabilities at the point of need.

The Unified Network must provide the critical capabilities that our Soldiers and Civilians need to succeed in volatile, congested, and contested environments. For the Army to be successful on tomorrow's battlefields, it must have a Unified Network that provides the Joint/Coalition Force with the ability to extend the range and increase the speed of operations required for decision dominance.

The Army Unified Network Plan addresses Army information technology and the network in a comprehensive approach; therefore, the term "Army Unified Network" in the context of this plan is inclusive of all hardware, software, and infrastructure from the very forward edge of the battlefield back to our posts, camps, and stations. The Army Unified Network Plan aligns to and underpins the Army's Modernization priorities, and supports the Army's intent to build an MDO-capable force by 2028.

The Army Unified Network Plan establishes five Lines of Effort (LOEs) critical to shaping the future Army:

LOE 1: Establish the Unified Network – Enabling Multi-Domain Operations
LOE 2: Posture the Force for Multi-Domain Operations
LOE 3: Security and Survivability – Commander's Freedom of Action in Cyberspace
LOE 4: Reform Processes and Policies – Improve Performance and Affordability
LOE 5: Network Sustainment – Sustain Enterprise and Tactical Networks

As our Nation's adversaries increasingly contest our historical dominance in all operational domains, the Unified Network **is the critical enabler** to the success of the future force. This framework sets the Army on a path to ensure technological dominance against our adversaries and establishes the foundation for an aggressive implementation plan to ensure our Army enables the tenets required to become an MDO-capable Force by 2028.

Christopher Lowman
Senior Official Performing the Duties of the
Under Secretary of the United States Army

Joseph M. Martin
General, United States Army
Vice Chief of Staff

TABLE OF CONTENTS

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 :
LTC Tonya S. Robinson, DANI-NSP, DCS, G-6
Plans and EIEMA Portfolio Management
Division latonya.s.robinson.mil@mail.mil

INTRODUCTION

The Army Unified Network Plan is propelling the network from a perceived invisible asset to a weapons system supporting a Multi-Domain Operations (MDO) Way Point Force by 2028. The Army's Unified Network will deliver a survivable, secure, end-to-end capability that will enable the Army to operate as a part of the Joint/Coalition Force during competition, crisis or conflict and in all operational domains (sea, land, space, cyber, air).

The Chief of Staff of the Army's White Paper on the Army's Transformation to Multi-Domain Operations and goal to have an MDO-capable Force by 2028 spotlights the critical need for the Army's Unified Network. Decision dominance and overmatch ability are at the core of MDO, and the Army can only achieve this through resilient, secure, global network capability and capacity. Based on this, the Army Unified Network Plan aligns multiple, complex network modernization efforts into a single, coherent approach required to support MDO.

Working across multiple lines of effort, the Army Unified Network Plan delivers a Unified Network for the Way Point Force of 2028 and then continuously modernizes as information technologies continue to evolve rapidly.

The Army Unified Network Plan aligns with the Army Strategy's focus on building readiness, modernizing, reforming the Army, and strengthening alliances and partnerships. Existing tactical network modernization strategies and implementation plans nest and align with the Army Unified Network Plan. Additionally, the Army Unified Network Plan parallels and enables the Army Campaign Plan 2019+ over multiple phases and time horizons:

PHASE I: NEAR TERM (PRESENT-2024)—SET THE UNIFIED NETWORK

This phase has begun with synchronizing the modernization of the Integrated Tactical Network (ITN) and the Integrated Enterprise Networks (IEN). Primary efforts during this phase include:

- Decisive to this phase is the establishment of a standards-based security architecture built on zero-trust principles with an initial primary focus on SIPRNet modernization followed by critical capabilities on NIPR including pay, logistics, contracting, etc.
- The Army begins the implementation of a holistic approach to evolve the Unified Network over time that synchronizes multiple efforts and leverages emerging technologies such as software-defined and 5G and beyond wireless networks that also align to zero-trust principles.
- The Army is following Office of the Under Secretary of Defense for wireless cellular networks as a critical technology for both tactical and enterprise network use. This will complement network consolidation and reduce non-wireless network dependency.
- This phase began with the accelerated movement of capabilities into cloud infrastructure coupled with swift divestment of legacy capabilities and processes. Key is the establishment of common data standards to enable emerging capabilities such as Artificial Intelligence (AI) and Machine Learning (ML).
- Ongoing development of the Mission Partner Environment (MPE) will continue as enterprise efforts establish a persistent capability and eliminates wasteful episodic efforts.

- The Army will continue aligning force structure to implement a Department of Defense Information Network Operations (DODIN Ops) construct to operate, maintain, and defend the Unified Network in a contested and congested environment.
- The Army must complete Network Convergence across the enterprise to align a single Army service provider and improve network readiness, standardization, and interoperability; increase the Army's cybersecurity posture; and enable rapid DCO response. This convergence sets the conditions for the Unified Network.

This phase ends with the establishment of a standardized, integrated security architecture that sets the foundation for the Unified Network and enables the rapid deployment and immediate conduct of operations anywhere in the world.

PHASE II: MID TERM (2025 - 2027)—OPERATIONALIZE THE UNIFIED NETWORK

This phase begins in FY25 with the continued convergence of ITN and IEN capabilities. Primary efforts during this phase include:

- The completion of the DODIN Ops construct with supporting force structure that enables defense and operations of the Unified Network in a contested and congested environment.
- This phase completes the establishment of hybrid cloud capabilities including tactical formations that accelerate AI/ML capability development.
- The Army will have established a persistent Mission Partner Network (MPN) inclusive of all hardware, software, infrastructure, and people from the enterprise to the tactical edge including the employment at all Combat Training Centers (CTCs) and Mission Training Complexes.

This phase ends when the Unified Network is fully postured to support the MDO Way Point force of 2028.

PHASE III: FAR TERM (2028 AND BEYOND)—CONTINUOUSLY MODERNIZE THE UNIFIED NETWORK

This phase begins on or about the start of FY28 when the Army Unified Network is fully postured—operationally, technically, and organizationally—to support the MDO Way Point force of 2028.

- Decisive in this phase is the full implementation of a holistic approach to modernize the Unified Network over time, leveraging emerging technologies while divesting of legacy, less secure, capabilities.
- As the Army continues to integrate with the Joint /Coalition Force and mission partners, a number of leap-forward technological capabilities shape this phase. The initial focus areas for these technologies include:
  - Dynamic and diverse transport, robust computing, and edge sensors
  - Data to decisive action
  - Robotics and autonomous operations
  - Corresponding cybersecurity and resiliency capabilities

Given the rapid and consistent pace of change of Information Technology and the Cyber domain, there is no end to this phase—modernization evolves to maturation of the Unified Network. It is a continuous process and there is no set end state for the Unified Network.

The Army Unified Network Plan is accompanied by the Army Unified Network Implementation, a U.S. Army Execution Order (EXORD) that decomposes the Framework into key tasks over near- and mid-term time horizons associated with pursuing the Lines of Effort (LOEs) and supporting objectives within the Framework. As the leads for Network integration and governance, the Chief Information Officer (CIO) and Deputy Chief of Staff (DCS), G-6 will use the Army Unified Network Implementation Plan to synchronize and assess efforts across the Total Force and all mission areas to set the Unified Network to support the MDO-capable Army of 2028.

THE NEED FOR A UNIFIED NETWORK — ENABLING THE MDO-CAPABLE ARMY OF 2028

The pace of technological advances, if not addressed, will dramatically erode the overmatch advantage we have enjoyed for decades. Technological advances enable the integration of space, cyber, information, and electronic warfare (EW) capabilities that can halt American power projection before it begins. Artificial Intelligence, autonomy, robotics, quantum computing, cellular wireless (5G and beyond), and Low Earth Orbit (LEO) Satellite will continue to change the character of operational campaigns, resulting in a battlefield that is faster, more lethal, and distributed. We can no longer assume that the homeland is a sanctuary, or consider the ‘global commons’ uncontested.

It is under this context that the Army has begun its transformation to an MDO-capable Force by 2028 and an MDO-Ready Force by 2035—it is an operational imperative for the Army and, more importantly, the Joint/Coalition Force.

In his White Paper, the CSA lays out several tenets that drive the need for a Unified Network that is resilient, trusted, maneuverable, and defendable—**one that from a complete Doctrine, Organization, Training, Materiel (capability), Leadership, Policy, and Facility (DOTML-PF), delivers a Unified Network that enables rapid, global deployment.** The Unified Network enables Army Formations to operate in a highly contested and congested operational environment with speed and at global range to enable decision dominance and maintain overmatch.

First and foremost, the Army will enable the Joint/Coalition Force to maneuver and prevail, from competition through conflict, with a calibrated force posture of multi-domain capabilities that provide overmatch through speed + range + convergence at the point of need for decision dominance.

The conflicts of tomorrow will be non-linear and contested at all echelons and on a global scale, with the homeland no longer a sanctuary free from adversary kinetic or non-kinetic attacks. This approach requires the Army to address the network holistically, fully integrating both tactical and enterprise (strategic) network segments in one Unified Network.

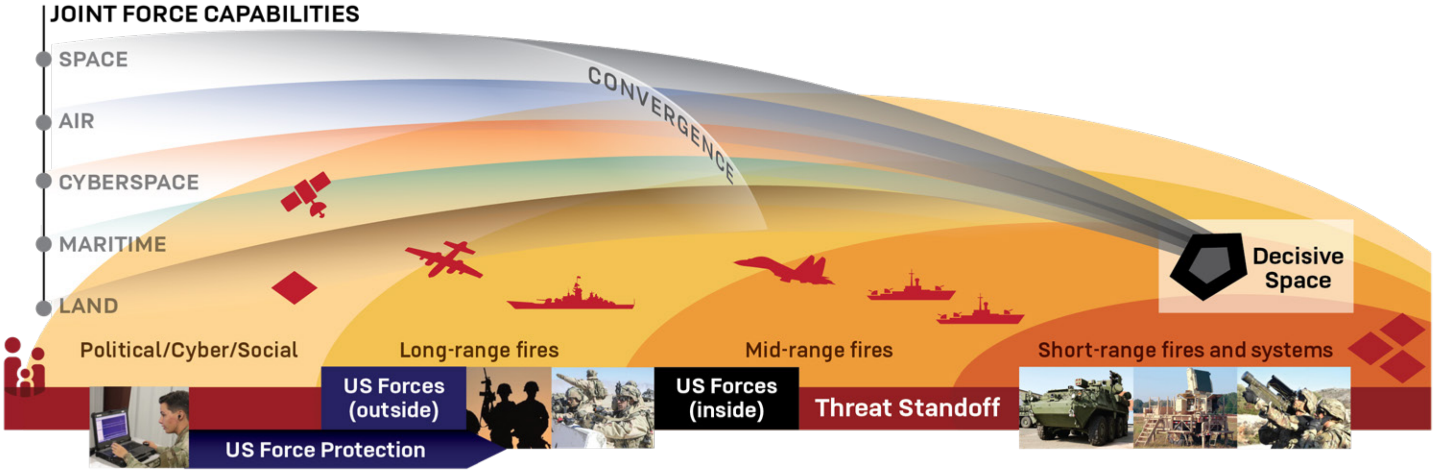
> “The battlefield is becoming faster; it is becoming more lethal; and it is becoming more distributed. OVERMATCH will belong to the side that can make better decisions faster. We are transforming to provide the Joint Force with the SPEED, RANGE, and COVERGENCE of cutting-edge technologies to gain the DECISION DOMINANCE and OVERMATCH we will need to win the next fight.”
>
> GEN James C. McConville,
> Chief of Staff of the Army

Second, the Army will provide the Joint/Coalition Force the ability to deliver strategic, operational, and tactical effects—across all Domains—at the time and place of the Commander's choosing, whether in competition or conflict. The Army will leverage emerging capabilities to expand the battlespace by maneuvering in areas "inside" an adversary's Anti Access/Area Denial (A2/AD) bubble and "outside" the traditional theater construct. Army Multi-Domain Operations, in support of the Joint/Coalition Commander, will occur on a global scale.

Other key aspects of the Army's Transformation to an MDO-capable Force by 2028 include :

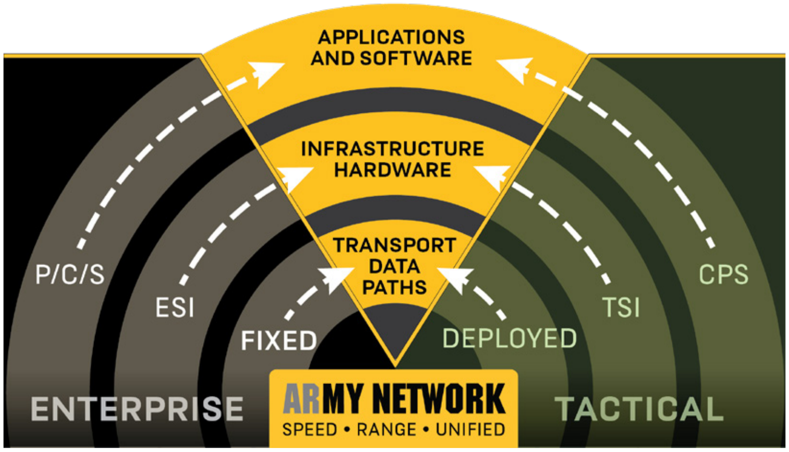
- In all domains, Army capabilities will sustain, enable, extend, and expand the reach of both defensive and offensive actions.
- The Army's 'inside forces' will operate inside the adversary's A2/AD zones to provide credible, survivable capabilities that either deter or defeat adversary area denial efforts.
- 'Outside forces' consist of regional and global expeditionary, surge, and homeland defense formations required to control terrain, consolidate gains, and secure strategic support areas.
- The Army will conduct operations at strategic, operational, and tactical depth that are essential against a peer enemy that enjoys superiority in numbers and complex A2/AD defensive systems.

The integration of strategic, operational, coalition, and tactical effects and capabilities is foundational to the conduct of Multi-Domain Operations. Meeting this requirement requires a network that converges cutting-edge technologies and effects to enable the Joint/Coalition Force Commander. The Unified Network enables all operations, regardless of domain. As such, the Unified Network must precede the Army's Aim Point Force of 2035 by being postured to support the Army's Way Point Force of 2028. It must then continually modernize as technology changes and adversary capabilities evolve. There is no end state for the Unified Network.



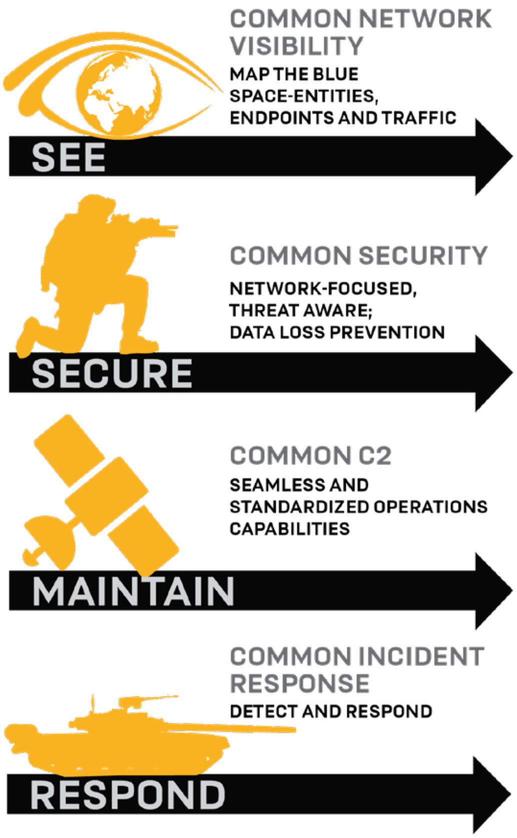
Multi-Domain Operations at Strategic through Tactical Echelons

DEFINING THE ARMY UNIFIED NETWORK—
THE ENABLER FOR MULTI-DOMAIN OPERATIONS



The **Army Unified Network** is a survivable, secure, end-to-end network that enables leaders to compete and, if necessary, to fight and win in large-scale combat operations, with Joint/Coalition, Allies, and Partners, against any adversary. Like any weapons system, the Unified Network must be resilient, defensible, and maneuverable to enable the Commander to achieve decision dominance and deliver kinetic and non-kinetic effects at the precise time and point of need of their choosing.

The Army Unified Network employs a **Common Operating Environment, Services Infrastructure, and Transport Layer, as well as Unified Network Operations and cyber defensive capabilities.** It enables intel at all levels of network classifications required to conduct multi-domain operations. For example, the Unified Network will provide unclassified networks for logistical operations as well as U.S. and Coalition classified capabilities for Mission Command and Fires systems. The Unified Network enables Intelligence operations between national, strategic, and tactical echelons while supporting the deep sensing capabilities required for Long-Range Precision Fires.


COMMON NETWORK VISIBILITY
MAP THE BLUE SPACE-ENTITIES, ENDPOINTS AND TRAFFIC
SEE
COMMON SECURITY
NETWORK-FOCUSED, THREAT AWARE; DATA LOSS PREVENTION
SECURE
COMMON C2
SEAMLESS AND STANDARDIZED OPERATIONS CAPABILITIES
MAINTAIN
COMMON INCIDENT RESPONSE
DETECT AND RESPOND
RESPOND

Unified Network Operations

Common Operating Environment (COE). The COE provides computing technologies and standards that enable secure and interoperable applications to process data at the speed of war. COE allows commanders to direct distributed forces from anywhere in the world, utilizing rapid data-driven, decision-making tools. It delivers common information services necessary to achieve a common operating environment that connects tactical computing environments with national or strategic resources to conduct MDO at speed and range.

Common Services Infrastructure (CSI). The CSI provides globally accessible, common hardware and software designed to secure, store, and compute data. It enables data analytics, AI, and machine learning to support data-driven decision making across the force and allows for the convergence of organizational networks. CSI maximizes commercial cloud services and hybrid cloud capabilities, and other “as a service” models allowing for access to the most modern information technologies.

Common Transport Layer (CTL). The CTL provides reliable, scalable, secure, and resilient pathways to deliver data, information, and collaborative services globally to commanders in any environment, using any device. Converged to a “colorless” transport model, CTL uses software-defined networking (SDN); open system architectures; commercial transport; and encryption technologies. Harnessing these technologies at all echelons will allow the Command Post to function at the same velocity as the home-station operations center. 5G and beyond technologies at all echelons will create an integrated “Internet-of-Things” distribution network for end devices which will link base operations to the tactical edge. Commercial wireless technologies will be leveraged wherever feasible to create mobile, agile, and secure network connections.

Unified Network Operations (UNO). UNO provides the capabilities required to secure, configure, operate, extend, maintain, and sustain the cyberspace to create and preserve the confidentiality, availability, and integrity of the Unified Network. UNO provides DODIN operations personnel with the capabilities to See, Secure, Maintain, and Respond to the Unified Network. UNO seamlessly integrates these capabilities across the Enterprise, Tactical, & Mission Partner Networks.

UNO ensures network availability and freedom of maneuver within the cyber domain for operational commanders to conduct MDO. It delivers a common suite of hardware and software, employing the principles of zero-trust, through a series of integrated activities encompassing the Operating Environment, Services Infrastructure, and the Transport Layer and is built to support the convergence of the ITN and IEN allowing for full-scale DODIN and Defensive Cyberspace Operations (DCO).

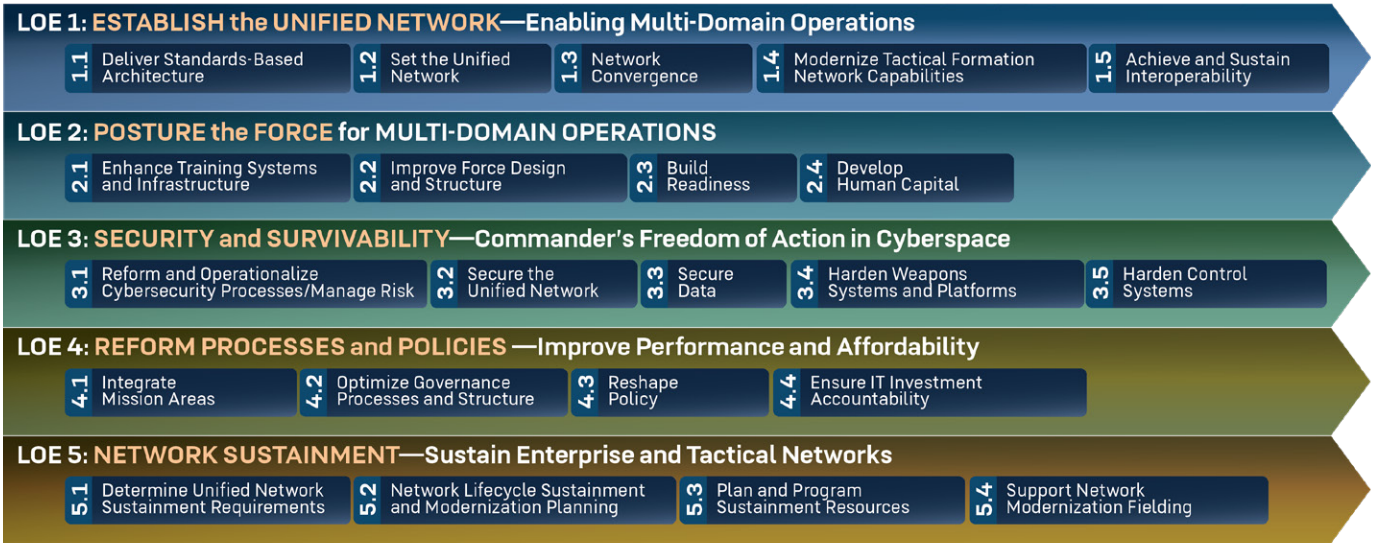
The alignment, standardization, and integration of the core foundations of the enterprise and tactical networks—Transport, Computing, and Services and Infrastructure—underpinned by Unified Network Operations and cybersecurity capabilities is an operational imperative. It sets the foundation for the Unified Network that enables global, cross-domain maneuver as well as the application of strategic, operational, and tactical effects at the speed and range required for the Army and the Joint/Coalition Force in the rapidly emerging battlefield of tomorrow.

STRATEGIC APPROACH

In order to achieve the Army’s bold transformation to provide the Joint/Coalition Force with the range, speed, and convergence of cutting-edge technologies, it will need to achieve future decision dominance and overmatch required to win the next fight; the Army must have an integrated, synchronized network modernization approach across all echelons—tactical, operational, and strategic.

Over the past several years, the Army has made tremendous strides modernizing its tactical formations with the deployment of Integrated Tactical Network (ITN) Capability Sets, but enterprise modernization efforts have significantly lagged and focused primarily on unclassified local area networks (LANs) on our installations. This unbalanced approach creates risk in conducting operations in all domains on a global scale.

The Army Unified Network Plan Framework is a critical element of achieving the Army’s Transformation to an MDO-capable Force. The following LOEs, with their supporting objectives, will shape, synchronize, integrate, and govern the Army's Unified Network modernization efforts and will help synchronize the personnel, organizations, and capabilities required to enable MDO, at echelon.



LOE 1: ESTABLISH the UNIFIED NETWORK—Enabling Multi-Domain Operations

1.1 Deliver Standards-Based Architecture

1.2 Set the Unified Network

1.3 Network Convergence

1.4 Modernize Tactical Formation Network Capabilities

1.5 Achieve and Sustain Interoperability

LOE 2: POSTURE the FORCE for MULTI-DOMAIN OPERATIONS

2.1 Enhance Training Systems and Infrastructure

2.2 Improve Force Design and Structure

2.3 Build Readiness

2.4 Develop Human Capital

LOE 3: SECURITY and SURVIVABILITY—Commander's Freedom of Action in Cyberspace

3.1 Reform and Operationalize Cybersecurity Processes/Manage Risk

3.2 Secure the Unified Network

3.3 Secure Data

3.4 Harden Weapons Systems and Platforms

3.5 Harden Control Systems

LOE 4: REFORM PROCESSES and POLICIES —Improve Performance and Affordability

4.1 Integrate Mission Areas

4.2 Optimize Governance Processes and Structure

4.3 Reshape Policy

4.4 Ensure IT Investment Accountability

LOE 5: NETWORK SUSTAINMENT—Sustain Enterprise and Tactical Networks

5.1 Determine Unified Network Sustainment Requirements

5.2 Network Lifecycle Sustainment and Modernization Planning

5.3 Plan and Program Sustainment Resources

5.4 Support Network Modernization Fielding

Army Unified Network Plan Framework

LINE OF EFFORT #1: ESTABLISH THE UNIFIED NETWORK—ENABLING MULTI-DOMAIN OPERATIONS

This LOE enables the integration and alignment of the ITN and IEN as well as the convergence of the multiple, disparate organizational networks into the Army Unified Network to support MDO by 2028. Central to this line of effort is synchronizing the Network modernization efforts across the Army. The development of network standards and interfaces, required to deliver the Unified Network and the integration of mature CI/CD pipelines to have a standard, secure pipeline that can deliver applications and capabilities to deployment targets across the network. Additionally, this LOE will establish the Unified Network as the Army's contribution to the DODIN as well as establish the Army's Mission Partner Environment to interoperate with Allies and other Coalition partners. The nature of MDO and reliance on Mission Partner capabilities and capacity in future operations requires that the Army train today within the MPE in support of future coalition operations. This LOE consists of the following five objectives:

OBJ 1.1: Deliver a Standards-Based Network Architecture. Define, design, and document an Army Information Technology (IT) Standards Technical Profiles to inform a network design linking operational, institutional, and enterprise zero-trust principles, mission capabilities, systems integration, and data and information flows. The Army will establish a hybrid cloud architecture that is resilient, secure, and able to store data and information seamlessly among the strategic, operational, and tactical levels. This enables the Army to expedite acquisitions that are more agile, standardize integrated implementation, and gain efficiencies of resources while ensuring interoperability, eliminating redundancy and streamline services.

OBJ 1.2: Set the Unified Network. This objective optimizes the current network to address such issues as fragmented networks, cyber vulnerabilities, complexity, fragility, and interoperability challenges with joint and coalition mission partners. This requires the implementation of a standards-based architecture that effectively integrates enterprise and deployed network capabilities across domains and environments, and features a unified transport layer that permits "plug and

> "This is an iterative build to the end state. We never truly reach the end state; the end state is constant innovation."
>
> GEN John M. Murray,
> Commander, Army Futures Command

play" for specific network capabilities. This focus on establishing an overall network security architecture allows tactical formations to "plug and play" within and through the Unified Network while reducing the complexity at the edge. This objective requires flexible cross-domain solutions to maximize the sharing of critical MDO information across multiple classified network enclaves while safeguarding sensitive data sources. It delivers resilient enterprise networks, platforms, applications, and services that are optimized to increase speed and range while converging cutting-edge technologies required for the conduct of cross-domain maneuver(s) in a congested and contested environment. For the Unified Network to operate at the speed that MDO requires, the Army must modernize the network's capabilities of automation, machine learning, and big data platforms to the maximum extent possible.

OBJ 1.3: Network Convergence. This objective converges networks, both vertically with tactical formations and horizontally with separate organizational networks (ORGNETS) 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 Ops capabilities across the Army and gaining fiscal efficiencies.

OBJ 1.4: Modernize Tactical Formation Network Capabilities. Modernization must occur from the tactical level back to the strategic and enterprise level and create a resilient, secure, maneuverable Unified Network. The Army will field Capability Sets on a 2-year cycle and iteratively modernize tactical formations over time. The Capability Sets for the Integrated Tactical Network (ITN), which began with Capability Set 21, will adjust over time as technologies change and will be able to "plug and play" within the Unified Network anywhere in the globe to enable the delivery of strategic and operational intelligence and effects to the tactical level. **ITN main efforts include enabling main tactical network initiatives already underway to include assured network transport, Common Operating Environment (COE), MDO-capable Command Posts, and Joint/Coalition interoperability at the edge.** The ITN must be resilient, secure, and maneuverable with the ability to support forces distributed across vast distances, converge effects from multiple domains, and maintain a common situational understanding in Multi-Domain Operations (MDO).

> "The scale, tempo, lethality, and complexity of large-scale, multi-domain combat operations requires significant changes in how we equip, organize, and structure the force to enable the Army to prevail against peer threats in contested domains."
>
> GEN Paul E. Funk II, Commander of
> Training and Doctrine Command

OBJ 1.5: Achieve and Sustain Interoperability. It is clear that the Army will continue to be a leader in building national partnerships and partner capacity; therefore, we must increase interoperability and have the capability to act routinely together coherently, effectively, and efficiently to achieve tactical, operational, and strategic objectives. To achieve and sustain interoperability and lead in building multinational partnerships, the Army must be effective in the human, procedural and technical aspects of interoperability. To date, MPE capabilities have been episodic and lack a means for a persistent capability required for rapid deployment and immediate operations.

LINE OF EFFORT #2: POSTURE THE FORCE FOR MULTI-DOMAIN OPERATIONS

This LOE focuses on our people, both military and civilian, and providing the training and organizational constructs to successfully compete, operate, and fight in an MDO environment. Foundational to this LOE is the transition to the Expeditionary Signal Battalion – Enhanced (ESB-E) organizational design and the subsequent implementation of a Global DODIN Operations framework to operate, maintain, secure, and maneuver the Unified Network. The Army must synchronize and integrate its organizational, people, training, and talent management initiatives to keep pace with rapid technological evolution.

OBJ 2.1: Enhance Training Systems and Infrastructure. The Army Strategy emphasizes that training will focus on high-intensity conflict, with emphasis on operating in dense urban terrain, electronically degraded environments, and under constant surveillance. The Army must provide forces with the appropriate facilities, systems, and infrastructure to train Soldiers on the Unified Network. Every Soldier must be able to operate his/her assigned network capabilities, and we must continuously adapt our Cyber and Signal training to account for the rapid evolution of network technologies, both in the schoolhouse and at home station.

OBJ 2.2: Improve Force Design and Structure.
The Army is currently updating its Signal and Cyber force structure to support the Army's transformation to an MDO-capable force by 2028. One key element of this redesign revolves around the transition to ESB-E organizational design that will significantly increase operational and sustainment capability and capacity with fewer personnel. This critical objective enables the Army to design and implement a DODIN Operations construct that enables global operations, fully integrates defensive cyberspace operations at echelon, supports the implementation of hybrid cloud capabilities to enable Artificial Intelligence 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: Build Readiness. The Army cyber workforce and capabilities must be ready to enable land power dominance against near-peer competitors in large-scale ground combat operations. This objective will ensure the Army Service Component Commands possess the capabilities and resources to maximize combat readiness in their respective theaters in accordance with their Combatant Commander's requirements and operational plans.

> "Army Networks and data are the foundational weapons system and ammunition for an Information Age force. Success for a multi-domain Army relies on ruthless defense of our networks, data and weapons platforms. We execute data-driven defensive cyber operations to detect, eliminate and defeat threats at mission relevant speed."
>
> LTG Stephen G. Fogarty,
> Commander, Army Cyber Command

OBJ 2.4: Develop Human Capital. People drive success. Our people and our relationships with allied partners are vital to achieving our goal to dominate in MDO. This objective aligns with The Army Strategy's call to take care of our people. We will enable Army talent management strategies that optimize the Army's ability to recruit, develop, and retain high-quality and highly skilled Army cyber workforce Soldiers and Civilians to support operations at the strategic, operational, and tactical levels.

LINE OF EFFORT #3: SECURITY AND SURVIVABILITY—COMMANDER'S FREEDOM OF ACTION IN CYBERSPACE

In cyberspace, the Army is in competition today against adversaries operating below the level of armed conflict. Whether in competition, crisis, or conflict, the Unified Network can only provide the means to apply strategic, operational, and tactical effects if it is secured and defended. In today's environment, adversaries continuously seek opportunities to attack our networks, including our industrial base and installations through control systems that are often decades old and antiquated.

The Army must reform its current cybersecurity processes, primarily the Army's Risk Management Framework, by reducing repetitive, time-intensive, and burdensome processes, and focus on operational processes like penetration testing and continuous monitoring. With the pace of technology change and its increasing sophistication, the Army cannot follow an arbitrary, 3-year review cycle. The risk is simply too high, and our adversaries are certainly not waiting around to deploy capabilities. The Army must be able to protect its ever-increasing attack surface area of both traditional IT and non-traditional Operational Technology (OT) assets while still adopting commercial technologies. To achieve this, the Army will implement zero-trust principles for IT and OT assets by completing a current state assessment of zero-trust capabilities for all of its systems.

This LOE focuses on making threat-informed, risk-managed operational decisions to ensure freedom of action within the cyber domain. This includes data integrity, user authentication, and availability of data based on the accesses granted to an authorized user.

OBJ 3.1: Reform and Operationalize Cybersecurity Processes/Manage Risk. To enable cyberspace operations at the speed required for MDO, the Army must address network accessibility, resiliency, and defense requirements. This includes recognizing key cyberspace terrain and understanding how data is positioned to be accessible at the time of need. The Army must adopt an approach to integrate fully offensive and defensive cyber operations to secure the network, our data, and our infrastructure rather than maintain the reactive and compartmentalized cybersecurity practices of the past. The end goal is to automate cybersecurity capabilities while maintaining full understanding of the operational risk.

The intent is to operationalize our current cybersecurity processes; beginning with the Risk Management Framework (RMF). Key to this objective is expanding the use of inherited controls and reciprocity among organizations. The Army must shift from compliance to active security, defense, and monitoring of critical Network and Weapons systems. The Army calls this new approach **RMF 2.0**.

OBJ 3.2: Secure the Unified Network. The main effort for this objective is to secure the Unified Network to support Multi-Domain Operations during competition, crisis, and conflict on a global scale. There are four key aspects to secure the Unified Network: First, the delivery of Unified Network Operations capabilities will be common to all echelons—tactical through strategic.

> "The Army network underpins all of our modernization efforts. It must be resilient, it must be reliable, and it must be able to operate in the dirt in a contested environment."
>
> GEN James C. McConville,
> Chief of Staff of the Army

Second, the implementation of a unified security architecture based on zero-trust principles. Third, the implementation of a DODIN Ops Framework, on a global scale, that leverages personnel reinvestments from the ESB-E transitions. Lastly, the Army will deploy defensive cyber capabilities across the Unified Network to enable Cyber Protection Teams (CPTs) to rapidly maneuver and hunt for adversaries within the network. Key parts of this objective include COMSEC modernization, commercial solutions for classified and raise the bar compliant cross-domain solutions.

OBJ 3.3: Secure Data. 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. This requires the capability to monitor data statuses, identify and mitigate changing threats and vulnerabilities, and ensure the relevance of the data over time. This objective focuses on simultaneously enhancing data security and usage through various means including the modernization of encryption technology and incorporating methods to secure algorithms.

OBJ 3.4: Harden Weapon Systems and Platforms. Every weapons system is connected to the Unified Network in one form or fashion. The Army will continue its Cyberspace Operational Resiliency Assessment-Platform (CORA-P) program to evaluate the cyber vulnerabilities of our major weapon systems, but that is just a start. The objective 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 a weapons system.

OBJ 3.5: Harden Control Systems. The Department of Homeland Security (DHS) identified more than 1,000 vulnerabilities in control system components from more than 260 vendors. That was just a sampling. To address this threat to the Army's ability to rapidly deploy, the Army implemented the Cyberspace Operational Resiliency Assessment - Installation (CORA-I) efforts to evaluate and mitigate vulnerabilities of Army critical infrastructure, Organic Industrial Base, and hardware and software supply chain. The Army must use the same cyber infrastructure to identify, manage, monitor, and defend all endpoints within the network from traditional IT to OT and IoT devices. The objective establishes governance and policy, validates requirements, and synchronizes resources to ensure freedom of maneuver.

LINE OF EFFORT #4: REFORM PROCESSES & POLICIES—IMPROVE PERFORMANCE AND AFFORDABILITY

This LOE will establish a governance and management framework that supports balanced, efficient, and effective investments across the Unified Network portfolio. The Army's implementation of IT category management, centralizing management of common services such as Army 365 and establishing flexible contracting approaches, allows the Army to rapidly adapt the Unified Network in the most fiscally efficient manner possible. These efforts require the validation of requirements through the Army's current processes and enable the Army to target reforms that reduce duplicative requirements while aggressively divesting of legacy systems.

OBJ 4.1: Integrate Mission Areas. Enterprise Information Environment Mission Area (EIEMA) is the foundation for integrating DODIN Ops across all Mission Areas supporting the Army's Unified Network efforts and initiatives. This objective includes a unified approach to the development and implementation of tools, data standards, and processes to support the Army Digital Oversight Council (ADOC), IT Oversight Council (ITOC) and other key governance bodies, as well as the production and alignment of Unified Network strategies, policies, and resourcing.

OBJ 4.2: Optimize Governance Processes and Structure. The Army will enforce the prioritization of investments and resource allocation, through existing Army processes. The Army Enterprise Network Council (AENC) will serve as the principal forum for Army Unified Network Plan Framework governance and will review topics requiring Army Senior Leader decisions for potential referral to the ADOC and ITOC. This governance structure will synchronize decisions, preclude actions being worked in siloed forums, and lead to risk-informed direction for execution.

OBJ 4.3: Reshape Policy. The Army will identify existing policies that prevent desired capabilities and outcomes recommend changes to policies to meet Army strategic goals. Policy process revisions must leverage robust knowledge management capabilities and contribute to better performance and lower risk.

OBJ 4.4: Ensure Unified Network Investment Accountability. Optimize the performance of the overall portfolio of programs based on performance and changing Army priorities and demands. Key to the desired outcome of this objective is an Army ability to provide a consistent approach, integrated and aligned with the Army's Programming, Planning, Budget, and Execution System (PPBES) to ensure that Unified Network resource decisions are made in accordance with the Army's strategic objectives and operational needs. Important components include:

- Establishing visibility and priorities of IT expenditures through category management.
- Where appropriate, implementing Army enterprise-level controls to increase purchasing power and eliminate stove-piped approaches and capabilities.
- Aggressively divesting of legacy or duplicative capabilities.
- Evaluating, prioritizing, and balancing programs and services within resource and funding constraints based on their alignment to building the MDO-capable Army of 2028.

LINE OF EFFORT #5: NETWORK SUSTAINMENT—SUSTAIN ENTERPRISE AND TACTICAL NETWORKS

Unified Network and Information Technologies are in a constant state of change—they are dynamic and constantly evolving. In this ever-changing environment, the Army must reassess its traditional sustainment model of Network capabilities. To support the MDO-capable Army of 2028 and, objectively, the MDO-Ready Army of 2035, the Unified Network must continuously evolve as technology and, just as importantly, the threat evolves. Sustainment requirements must be documented, planned, and programmed in order to ensure that the Unified Network remains resilient, defensible, and maneuverable in support of Army and Joint/Coalition Forces, during competition, crisis, and conflict.

Additionally, as we build the Unified Network with new capabilities such as Artificial Intelligence (AI) and Machine Learning (ML), we must aggressively divest legacy capabilities as we modernize. This LOE is a major paradigm shift in how the Army approaches sustainment for technologies in continuous evolution—the Army must achieve a balance between modernization and life-cycle sustainment to keep pace with our adversaries.

OBJ 5.1: Determine Unified Network Sustainment Requirements. Effective, continuous modernization of the Army's Unified Network is paramount to the conduct of MDO. Army Unified Network components in sustainment must augment and support, not impede, the Army's modernization requirements. This objective will identify and validate sustainment requirements and then synchronize them with other Unified Network modernization efforts.

OBJ 5.2: Network Life Cycle Sustainment and Modernization Planning. Life cycle sustainment is a key component of any operational capability, but it is even more critical for rapidly evolving capabilities such as the Unified Network. The Army must achieve a balance between sustainment and modernization.

This objective links sustainment and modernization efforts through the oversight of targeted governance and configuration control boards. It includes Technical Data Packages (TDP) and Intellectual Property (IP) rights in contract requirements in order to allow the Organic Industrial Base (OIB) to fabricate, repair, and make equipment modifications throughout the life cycle.

OBJ 5.3: Plan and Program Sustainment Resources. Programmed resources in the annual Army budget plan will ensure readiness and availability of the Army's networks and connected systems. This objective focuses on the planning, programming, budgeting, and execution planning for Unified Network sustainment operations, once balanced with the Army's iterative, continuous modernization efforts.

OBJ 5.4: Support Network Modernization Fielding. New modernized networks and connected systems are currently being planned for delivery in the tactical battlespace as modernized capability sets (CAPSETS) in FY21, FY23, FY25, and FY27. Capability documents are in development to assist in modernizing the Tactical Network. Concurrently, there are ongoing efforts for the modernization of Enterprise networks and connected systems that require fielding support.

CONCLUSION

The Army Unified Network Plan provides the strategic framework to guide the development of the Unified Network that the Army requires to realize its transformation to an MDO-capable force by 2028. The Unified Network modernization must be more than just developing and fielding capabilities—it must be a holistic approach that addresses our people, training, organizations, policies, and processes.

As our Nation's adversaries increasingly contest our historical dominance in all operational domains, the Unified Network is the critical enabler to the success of the future force. This framework sets the Army on a path that will ensure technological dominance against our adversaries and establishes the foundation for an aggressive implementation plan to ensure our Army is postured to be an MDO-capable force by 2028.

U.S.ARMY®