NETWORKING
THE SOLDIER
ARMY NETWORK CAPABILITY SET MODERNIZATION

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED. JANUARY 2021
Today, as part of its modernization strategy, the Army is delivering a network that addresses the most critical operational shortfalls and enables Multi-Domain Operations through network capability sets. Capability Sets (CS) and associated technology are fielded on a two-year basis starting in FY21. Each set builds off the previous by adding commercial technology and aligning Army Science & Technology programs for transition into programs. To support this strategy, the Army is executing four network modernization lines of effort to develop and field a network that is more expeditionary and mobile, less complex and better protected.

Today, through CS fielding and development, the Army is actively inserting industry capability to enhance the network to give commanders multiple communication choices (both military and commercial networks), make it more user friendly, harden it against cyber and EW threats and provide easier methods to share information with collation partners.
The Army recognized the need to embark on a new network modernization strategy to better keep pace with commercial IT development and to ensure we remain ahead of our adversaries. The Army’s approach to tactical network modernization is focused at keeping pace with threats in the near term, while simultaneously developing an optimized future network through rapid insertion of new technology. The strategy contains four supporting efforts focused on institutional reforms, policy and governance, research and development, and more experimental and exploratory science and technology. Today, the Army is executing the strategy by building two-year capability sets and conducting market research to insert the latest commercial capabilities into future sets.

EXECUTING THE STRATEGY

In order to incorporate real-time operational feedback and generate less prescriptive requirements, the Army is utilizing the proven industry practice of developmental operations (DevSecOps) and robust operational experimentation, which places developers side-by-side with Soldiers in operational units to evaluate potential technology solutions. Additionally, these developers are working with industry to make real-time program improvements as part of the DevSecOps construct. These assessments will inform Capability Set network design, future capability requirements, resourcing and acquisition decisions, and help the Army and its industry partners to evolve the network at the pace of warfighter demands and commercial innovation.
The Army’s network modernization strategy focuses on four modernization priorities, known as lines of effort (LOEs): (1) creating a unified network transport layer; (2) building a common operating environment (COE) for mission command applications; (3) improving Joint Force and Coalition interoperability and (4) improving command posts’ mobility and survivability.

**LOE 1: UNIFIED NETWORK TRANSPORT**
WHAT: Establish available, reliable and resilient network that ensures seamless connectivity in any operationally contested environment.
WHY: The Army must be able to communicate through an assured network and operate in contested and congested environments.

**LOE 2: COMMON OPERATING ENVIRONMENT (COE)**
WHAT: Provide a simple, intuitive, single common operating picture through a single mission command suite operated and maintained by Soldiers.
WHY: Commanders must be able to make decisions quickly while commanding distributed forces, utilizing rapid decision making skills.

**LOE 3: JOINT INTEROPERABILITY/COALITION ACCESSIBLE**
WHAT: Ensure Army Forces can more effectively interact (technically and operationally) with Joint and Coalition partners.
WHY: The US Army does not fight alone—the Army needs to achieve and sustain a level of interoperability within the Army, Joint and Unified Action Partners to enable Joint All Domain Command and Control (JADC2).

**LOE 4: COMMAND POST (CP) MOBILITY/ SURVIVABILITY**
WHAT: Enable commanders to lead and fight in their formations from anywhere they choose. Ensure command post deployability, reliability, mobility and survivability.
WHY: Command Posts must be mobile and survivable to meet today’s operational needs — Fast, Agile, Lethal.

**Army Network Modernization Lines of Effort**

- LOE 1: Unified Network Transport
- LOE 2: Common Operating Environment (COE)
- LOE 3: Joint Interoperability/Coalition Accessible
- LOE 4: Command Post (CP) Mobility/Survivability
To achieve all-domain dominance, keep pace with industry advancements, and deliver a modernized tactical network, the Army is fielding Capability Sets (CS) in two-year increments. Each CS builds off of the previous and is infused with commercial solutions informed by Soldier-led experimentation. Capability Set development will integrate lessons learned from Soldier Touchpoints, Project Convergence and other experimentation. Capability Sets will support sensor-to-shooter, IVAS, and Multi-Domain Task Force network needs. The CS construct leverages Army and DoD science and technology initiatives, research and development advancements from industry and academia, and modern commercial off-the-shelf solutions. Building to standard with advanced waveforms, mission command applications, cyber security, data management, satellite communications, and artificial intelligence is core to the success of this phased approach.

To deliver the network of 2028, the Army outlined four capability sets in Fiscal Years 2021, 2023, 2025, and 2027 to insert technologies that provide warfighters improved capabilities and dominance in a contested and congested environment against any peer or near-peer adversary. Technology insertions will continue beyond 2027 following this same iterative approach.
CS21 DELIVERS:
• Integrated Tactical Network (ITN) fielded to select BCTs
• Initial fielding of the common operating environment through command post computing environment and across handheld and mounted environments
• Enhanced satellite communication (SATCOM) capability for Expeditionary Signal Battalion–Enhanced units
• Software update for resilient SATCOM over existing terminals
• Initial onsite cloud (edge) agile computing environment that provides distributed mission command
• Foundation for command posted mobility and survivability improvements
• Improved tactical network transport to prepare for integration of the Integrated Visual Augmentation System

In FY20, the Army began prototyping and experimenting with technologies and capabilities that will be considered in the CS23 network design. These prototyping efforts will inform preliminary designs and, where viable, will be inserted into events and exercises for larger-scale experimentation for further assessment.

CS23 DELIVERS:
• Initial commercial SATCOM at–the–halt, providing high capability communications
• Continued ITN fielding to Infantry and Stryker BCTs; field tailored ITN for mounted BCTs that optimizes capabilities to meet operational distance and pace, improved aerial tier, and expanded network operations between tactical and enterprise
• Introduction of C4ISR/Electronic Warfare Modular Open Suite of Standards (CMOSS), a modular open systems architecture (MOSA) that will converge select Army warfighting capabilities
• Introduction of hardened radio capabilities, including mesh network, into all formations and improvements in anti-jamming for waveforms (including Single Channel Ground and Airborne Radio System)
• Convergence of mission command applications to set conditions for Joint–All Domain Operations
• Thickening the transport layer to provide additional artificial intelligence and beyond line of sight for manned/unmanned vehicles, fires, missiles and small aircraft

This CS helps to provide a more robust transport layer to support the requirements of the Army’s other modernization priorities.
CAPABILITY SET 27: MULTI-DOMAIN DOMINANCE

The Army’s insertion of commercial technologies in two-year phases will be fully institutionalized with Capability Set 27 (CS27). Wireless connectivity will be more secure, and the Army’s network will have significant cyber improvements and protection. Automation capabilities inserted in earlier capability sets will now be enabled by artificial intelligence (AI) and machine learning (ML). Command post and unit footprint will be less visible. Full and seamless integration of all applications and systems across different units will result in improved interoperability and information sharing and accelerated decision making.

CS27 DELIVERS:
• Non-traditional waveforms that are spectrum efficient with higher bandwidth, anti-jamming capabilities, and low probability of detection
• Field-integrated AI and ML capabilities and tools to enhance decision making
• Hardened 5G or equivalent
• Dispersed mission command computing in command posts in disadvantaged environments
• Convergence of all warfighting function applications into a Common Operating Environment

CAPABILITY SET 25: AUTOMATED & PROTECTED

Through experimentation and DevSecOps, the Army will continue to leverage and insert commercial solutions into its network with a focus on automation and protection. Through Capability Set 25 (CS25), deployed units will have more robust cloud capability and network management; decision-making tools will become more automated, and network security will be exponentially amplified due to new waveforms. Advanced cellular technology such as 5G, commonplace in the commercial sector, will become accessible to formations, resulting in faster connectivity. Data networking capability between ground forces and aviation will provide advanced air–ground communications.

CS25 DELIVERS:
• Continued ITN fielding
• Armor formation network modernization
• Introduction of radio and SATCOM waveforms to increase electronic warfare resiliency, and, scale, and bandwidth
• Potential integration of 5G (or equivalent) commercial network capacity
• Initial commercial Low Earth Orbit/Medium Earth Orbit on–the–move providing high–capacity communications
• Integration/interoperability of air–ground communications capability
• High-tempo, data–driven decision tools to increase cyber threat visibility
• Hardened command post improvements and reduction of footprint
• Initial integration of network with future mid-size transport assets
The Network Cross-Functional Team (N-CFT) is composed of members of the Army operational community, capability managers, acquisition/contracting professionals, and policy experts. Today, the N-CFT is planning future capability sets and experimentation, conducting industry market research, aligning capability to need, and coordinating network-related science and technology. Near-term focus areas are automation and intelligence, resilient communications and situational understanding of the electromagnetic environment, data management, and prioritizing network-related resources to ensure the Army is poised to quickly procure promising commercial capability. The N-CFT supports the rapid transition of leader-approved capability requirements to the Army Acquisition System, and addresses network disconnects and misalignments by horizontally and vertically integrating requirements while seeking available solutions for experimentation, demonstration, and evaluation by Soldiers and leaders in the field.
The Integrated Tactical Network (ITN) provides a simplified, mobile network availability down to the small unit dismounted leader to facilitate mission command, situational awareness, and air-to-ground integration. It is comprised of a kit of flexible commercial solutions that can be rapidly inserted into the existing tactical network. The ITN operates in both a SECRET and Secure-But-Unclassified (SBU) enclave to provide commanders with the flexibility to balance security and connectivity based on mission need, including the ability to securely transmit data to Army and coalition forces in an unclassified environment.

The ITN’s first iteration includes single-channel commercial radios with advanced networking waveforms, high-capacity line-of-sight radios, voice and data gateways, tactical cross-domain solutions, small aperture satellite terminals, expeditionary servers, variable height antennas (via a quadcopter drone), 4G commercial technology and applications, and associated ancillary devices integrated with Program of Record systems to enable commanders with resilient communications as part of their primary, alternate, contingency, and emergency communications plan.

As a critical component of Capability Set (CS) 21, the ITN is fielding to four Infantry Brigade Combat Teams in FY21, and another five formations in FY22. CS23 will expand fielding to additional infantry BCTs and and Stryker BCTs.

INTEGRATED TACTICAL NETWORK

The NETT Warrior Integrated Dismounted Leader Situational Awareness System is a critical component of the ITN. It hosts the Android Tactical Assault Kit, which securely connects today’s tactical radios and allows soldiers to obtain critical position information location of their troops.
The Army’s Integrated Virtual Augmented System (IVAS) will feature low-cost, single-channel data radios with a Tactical Cloud Package (TCP). IVAS is a single platform featuring head’s up display next-generation night vision goggles, which allows the Soldier to fight, rehearse, and train, while improving Soldier sensing, decision-making, target acquisition, and target engagement. Soldiers use the data radios to transmit data to and from dismounted IVAS users. Data is then routed through echelons by networked radios and services on the TCP, which is integrated onto platforms. The result is onsite cloud compute and storage that enhances IVAS capabilities in network-denied environments for artificial intelligence and machine learning, including facial recognition, language translation, speech-to-text, and object recognition.
2-CHANNEL LEADER RADIOS (LR)

The HMS MP is a software defined, National Security Agency (NSA) Type 1 certified radio, providing two-channel secure voice and data communications via TSM, SINCGARS, SATCOM and SATCOM Integrated Waveform (IW), Mobile User Objective System (MUOS) and Enterprise Over-The-Air Management (OTAM).

TACTICAL RADIO MODERNIZATION

2-CHANNEL MANPACK (MP) RADIOS

The Leader Radio is a software defined, handheld, NSA Type 1 certified radio providing two channel secure voice and data via the TSM and SINCGARS waveform. The LR can also be linked to the Nett Warrior.

TACTICAL RADIO MODERNIZATION

The Army is modernizing the SINCGARS radio and its associated waveform to support NSA and DoD cryptographic modernization goals. The SINCGARS radio will be replaced with the upgraded Combat Net Radio (CNR), which will pursue the requirement for assured voice SINCGARS for command and control and limited data specifically for Fires and Air Defense. The new SINCGARS waveform will include frequency hopping capabilities for use in mounted and dismounted radios to securely transmit data within contested environments.

COMSEC

PdM COMSEC is leading the effort to replace the Simple Key Loader (SKL) with the Next-Generation Load Device-Medium (NGLD-M). The NGLD-M will support stronger encrypted key distribution methods than the current SKL, which are required to counter cyber threats against the DOD systems and to be in compliance with National Security Agency (NSA) and Joint Chiefs directed encryption and network performance standards. The NGLD-M incremental effort will modernize a limited amount of SKLs and then phase out the device as quickly as possible while synchronizing a competitive NGLD-M acquisition strategy to ensure proper integration, certification, and testing. These cryptographic key fill devices enable a Soldier to turn on tactical radios, military communication systems, secure phones, computers, and VTCs so that each can operate at SECRET, TOP SECRET and other high classification levels of network assurance.
Tactical Network Technology Modernization in Service (TNT-MIS) is a major effort in line with establishing Army Network Modernization Strategy Line of Effort 1: Unified Network Transport.

TNT-MIS enables Joint All-Domain Command and Control (JADC2) by providing network connectivity and transport for the ground domain. Current TNT-MIS capability enhances cyber security, simplifies tactical network operational use and initialization, and reduces component size, weight, and power (SWaP). TNT-MIS efforts also include modernizing end-of-life/non-sustainable commercial tactical technology and other IT component equipment, enabling the implementation of a standards-based architecture with new capabilities and technologies.

Through TNT-MIS, the Army can leverage commercial capability to make the network more expeditionary and capable. An example of this is the ongoing fielding of the TNT on-the-move Network Operations and Security Center-Lite (NOSC-L), which greatly reduces SWaP compared to the legacy capability for integration on lighter vehicle platforms. The Army is also leveraging TNT-MIS IT to provide on-the-move capability to Armored Brigade Combat Teams. Additionally, TNT-MIS IT enhancements will also improve the Army’s network Regional Hub Nodes (RHN) and other critical satellite communications (SATCOM) capabilities to support the Expeditionary Signal Battalion—Enhanced modernization priority and other emerging technologies.

As the Army develops future Capability Sets, the TNT-MIS effort will be used to leverage commercial SATCOM into tactical network transport, including, but not limited to, emerging high-throughput commercial satellite constellations in Low Earth Orbit (LEO), Medium Earth Orbit (MEO), and Geosynchronous Orbit (GEO) to provide additional network resiliency to Infantry, Stryker, and Armor formations.
Compared to legacy systems, these easy-to-use systems increase range and bandwidth capacity, some operating in satellite-denied environments, while providing significant reductions in size, weight, and power (SWaP) to enhance maneuverability.

Following a successful developmental operations pilot to inform modernization decisions for the Army’s Expeditionary Signal Battalions (ESBs), the service has begun fielding efforts to equip the first ESB-Enhanced (ESB-E) units with an initial new line-of-sight and beyond-line-of-sight equipment package that includes many of these capabilities. Together they deliver resilient, uninterrupted mission command and the ability to rapidly deploy and maneuver across the battlefield to enable ESB-Es to support the signal requirements of other units.

The Army is also modernizing its legacy logistics network transport capabilities, with the eventual modernized logistics network capability known as Sustainment Tactical Network (STN).
Utilizing the Army’s tactical satellite network, Enroute Mission Command provides critical in-flight mission command to units, such as the 82nd Airborne Division’s Immediate Response Force, while onboard an aircraft enroute to an objective.

Once on the ground, Soldiers can rapidly set up their Family of SATCOM terminals, including Transportable Tactical Command Communications (T2C2) and Scalable Class of Unified Terminals (SCOUT) to enable continuity of mission command during the initial phases of operation. These terminals provide robust, high-bandwidth network communications and mission command for initial entry, as well as more mature forward operations.

The easy-to-transport, high-capacity Terrestrial Transmission Line of Sight (TriLOS) Radio program of record improves the expeditionary nature of U.S. Army units, while significantly increasing network throughput and range, operational flexibility, and multipath diversity in congested and contested environments.

When fielded, the next generation Troposcatter Transmission (Tropo) capability will significantly extend network range and throughput, and greatly reduces SWaP over current capability. Tropo bounces signals off of the Earth’s atmosphere to provide beyond-line-of-sight capability without using expensive and limited satellite resources. Both TriLOS and Tropo operate in satellite-denied environments, increase multipath diversity, and add redundancy and operational flexibility to the tactical network.

The small form factor Modular Communications Node-Advanced Enclave (MCN-AE) augments the existing intelligence network, enabling intelligence users to connect to all of the same resources they have when using the traditional Trojan Intelligence Network, but instead using the tactical network.

The SIGMOD/SATCOM capabilities include:

- **Secure Wireless** uses the NSA-approved Commercial Solutions for Classified solution to provide classified and unclassified wireless capability, with Small Form Factor Secure Wireless providing capability inside the Command Post (CP), and Secure Wireless Mesh Remote Endpoint providing vehicle-to-vehicle connections, to enable units to disperse their Command Post vehicles to make the CP more survivable. Following CP setup, units can turn on their Secure Wireless hotspots and the network can come up first instead of last, in as quickly as minutes instead of hours, and Soldiers can stay connected longer when jumping the CP.

- **Commercial Coalition Equipment (CCE)** can be rapidly reconfigured to provide secure tactical access for the coalition or commercial networks to support both civil and military operations. CCE also provides a radio bridging voice capability that enables radios on different frequencies, or different equipment such as radios or cell phones, to seamlessly connect to one another.
Unified Network Operations (UNO) will reduce network complexity and provide an integrated, standard set of network management applications. UNO enables communication offices (S6/G6) from the tactical edge through corps level to plan, configure, manage, monitor, and secure/defend the network. Likened to a “universal remote control,” the program delivers an integrated, standardized, and simplified Network Operations (NetOps) framework that combines the management of the strategic and tactical network environments into a centrally integrated NetOps architecture. UNO will provide an integrated network management capability to simplify user experience, increase situational awareness, and strengthen cyber network defense. This will ultimately reduce the number of network management and monitoring applications and tools currently used by communication offices.

UNO is an incremental development effort with initial capability supporting the tactical environment, and is managed as a Mid-Tier Acquisition (MTA). UNO capability enhances visualization of NetOps functions, pushes network data to cyber situational awareness tools, and implements a common data model that enables reconfiguration of the network in support of unit task reorganization. The program is being developed with Soldier input as part of the first set of tools to be fielded in support of Capability Set-23 (CS23). UNO empowers leaders with the ability to sense and understand the operational environment by synchronizing Department of Defense Information Networks (DODIN) operations and Defensive Cyber Operations, allowing dynamic negotiation of threats and counter adversaries in a complex and contested environment.

Aligned to Army Network Modernization Strategy Line of Effort 1: Unified Network Transport, UNO software applications will assure uninterrupted access to satellite communications, navigation, and timing (PNT), and intelligence, surveillance, and reconnaissance (ISR) across a multi-domain architecture.

The Army has migrated to a Common Operating Environment (COE) for mission command software and hardware systems. COE is an integrated set of standards, tools, and technologies that enable mission command applications and allow warfighters to adapt and configure the network as conditions change.

This cornerstone of the network modernization strategy provides solutions for current issues with stove-piped mission command systems that function well individually, but do not integrate easily with each other. It also supports collaboration using a common picture with Joint and coalition mission partners.

One tactical solution, the Command Post Computing Environment (CPCE), leverages commercial solutions already in use by Combatant Commands, Special Operations Forces, and other Services and military forces worldwide, which shifts the COE strategy away from a government-owned and government-developed model. CPCE began fielding in FY19, and is delivering a true common operating picture to the command post.

Currently, the Army is also consolidating to a single software baseline for all mission command applications across the Army, Army Reserve, and Army National Guard formations. Standardization of mission command software and implementation of a universal baseline decreases the number of software patches and security updates that must be developed, tracked, and introduced in the field. It also helps with ease of CPCE by creating an environment for interoperability. Additionally, within the next five years all units will be synchronized with the same upgraded mobile mission command software called the Joint Battle Command-Platform (JBC-P), and a version of the Army’s new standardized tactical computer, the Mounted Family of Computing System (MFoCS). The combined capabilities of JBC-P and MFoCS deliver the Army’s next-generation friendly force tracking system.
MODERNIZING MISSION COMMAND

Convergence partners - including the Program Executive Office Intelligence, Electronic Warfare, and Sensors (PEO IEW&S) and Program Executive Office Ground Combat Systems (PEO GCS) - leverage MMC infrastructure and services to develop additional WFF capabilities without having to build a complete system from the ground up. This cooperative effort ensures streamlined integration, hardening, accreditation, and rapid delivery of critical capabilities to the warfighter.

Mounted Mission Command (MMC) software leverages both a next-gen transceiver and MMC transport to provide increased security and network resiliency that outpaces adversarial countermeasures and threats. MMC is a common user-experience enables leaders to lead and fight their formations from anywhere on the battlefield.

MMC provides movement and maneuver applications while supporting a wide range of warfighting functions (WFF): integrated common-operational picture, intel, fires, medical, logistics, and third-party applications. These capabilities provide additional functionality through a converged software architecture and infrastructure.

The Advanced Field Artillery Tactical Data System (AFATDS) provides fully automated support for planning, coordinating, controlling, and executing fires and effects such as mortars, field artillery cannons, rockets and missiles, close-air support, attack aviation, and naval surface fire-support systems. AFATDS interoperates and integrates with more than 80 different battlefield systems, including Navy and Air Force command and control weapon systems and German, French, Turkish, and Italian fire-support systems.

The Army's Long Range Hypersonic Weapon (LRHW) is leveraging an AFATDS variant to provide command and control of the missile while the system's Common Message Translator ensures interoperability between the AFATDS and LRHW message formats for seamless flow of data throughout the digital kill chain.

Cyber Situational Understanding (SU) is a converged application that manages, interacts with, and visualizes Cyberspace Electromagnetic Activities (CEMA). The capability will include back-end analytics that leverage source and enriched data from specific tactical and strategic programs. Its capabilities are intended to provide analysis and forecasting to prioritize information and reduce cognitive workload of warfighters.

Command Post Computing Environment (CPCE) provides an easy-to-use common operational picture through a single mission command suite of software operated and maintained by Soldiers. CPCE provides server hardware that hosts a comprehensive suite of software applications and services for converging warfighter functions and building future applications.

CPCE has been optimized through developmental operations (DevSecOps) to improve improvements, add briefing capability, and implement network management tools. Additionally, to improve system performance and to mitigate unnecessary data flow over constrained tactical network transport bandwidth, program managers and developers are working to address underlying data analytics, data dissemination, and federation associated with the use of CPCE. These major efforts will be key focuses of Capability Set 23 development.
The Command Post Integrated Infrastructure (CPI2) program improves mobility, scalability, and survivability of Army command posts to address the challenges posed by contemporary and future land conflict. Leveraging Soldier feedback from experimental units, the new CPI2 mobile command posts replace vulnerable legacy CPs and feature improvements in physical signatures, mobility, and standardization. CPI2 uses a mix of vehicle platforms and shelter systems to enable fixed CP levels of functionality, while increasing survivability through the mobility and rapid displacement capabilities of mobile CP infrastructure.

The CPI2 final prototype design review has recently set the stage for follow-on fabrication and integration phases of the designs, and within the next year, the Army will start to see the radically mobilized CP designs in action. Initial fielding to select Brigade Combat Teams (BCTs) is slated for FY21.

The Army is executing CPI2 in two increments. Increment 0 involves multiple phases of prototyping, integration, and follow-on formal design for BCT command post designs. The design approach is comparative, taking a government-driven solution, developed through a functional support agreement with the Army’s Combat Capabilities Development Command (CCDC) C5ISR Center, and vetting it with an industry solution to ultimately deliver a best-of-breed product.

Each design incorporates a significant amount of C5ISR equipment, including network communications, mission command hardware and software, power systems, radios, antennas, servers, computers, and electronic control units. Each component has complex interfaces, cabling, security requirements, and power needs that must be taken into consideration.
HTTP://PEOC3T.ARMY.MIL
WWW.FACEBOOK.COM/PEOC3T
WWW.TWITTER.COM/PEOC3T
WWW.FLICKR.COM/PEOC3TMEDIA
WWW.ARMY.MIL/ASAALT
WWW.ARMY.MIL/FUTURES