

**PORTFOLIO**

**PEO  CBT**

**PROGRAM EXECUTIVE OFFICE COMMAND CONTROL COMMUNICATIONS-TACTICAL**



# TABLE OF CONTENTS

	<p><b>A   JTNC</b> Joint Tactical Networking Center (JTNC)</p>	<p>6-7</p>
	<p><b>B   PM I2S</b> Capability Set Development</p> <ul style="list-style-type: none"> <li>• Capability Set 21: Expeditionary &amp; Intuitive</li> <li>• Capability Set 23: Capacity &amp; Resiliency</li> <li>• Capability Set 25: Automated &amp; Protected</li> <li>• Capability Set 27: Multi-Domain Dominance</li> </ul> <p>Command Post Integrated Infrastructure (CPI2) Common Hardware Systems (CHS) Tactical Network Initialization and Configuration (TNIC) Unified Network Operations (UNO)</p>	<p>8-9 8-9 10-11 10-11 12-13 14-15 16-17 18-19</p>
	<p><b>C   PM MC</b> Command Post Computing Environment (CPCE) Fire Support Command and Control (FSC2) Joint Battle Command-Platform (JBC-P) Mounted Mission Command (MMC) Mission Command Cyber (MC Cyber)</p>	<p>20-21 22-23 24-25 26-27 28-29</p>
	<p><b>D   PM TN</b> Tactical Network Transport At-The-Halt Tactical Network Transport On-The-Move Regional Hub Node (RHN) &amp; Global Agile Integrated Transport (GAIT) Enroute Mission Command (EMC) High Capacity Radio Systems Secure Wireless Commercial Coalition Equipment (CCE) and Common Services-Hub (CS-Hub) Modular Communications Node-Advanced Enclave (MCN-AE) SATCOM Family of Terminals Secure, Mobile, Anti-Jam, Reliable, Tactical-Terminal (SMART-T) Deployable Ku Band Earth Terminals (DKET) Sustainment Transport System (STS)</p>	<p>30-31 32-33 34-35 36-37 38-39 40-41 42-43 44-45 46-47 48-49 50-51 52-53</p>
	<p><b>E   PM TR</b> Combat Net Radio (CNR) Communications Security (COMSEC) Integrated Tactical Network (ITN) Handheld, Manpack, and Small Form Fit (HMS) Helicopter and Multi Mission Radios (HAMMR) Waveforms</p>	<p>54-55 56-57 58-59 60-61 62-63 64-65</p>
<p><b>ACRONYMS</b></p>		<p>68-69</p>



Army transformation efforts are delivering a unified network that addresses the most critical operational needs and supports the Army of 2030. Two-year modernized network capability sets began fielding in 2021 with Capability Set 21 to seven infantry brigade combat teams and one Stryker regiment squadron. The capability set effort is continuing with Capability Set 23 by completing fielding across the entire Stryker regiment, additional fielding to infantry formations, and for the first time to division headquarters and enabling formations, starting with the 82nd Airborne Division in 2023.





Headquartered at Aberdeen Proving Ground, Maryland, the Program Executive Office for Command, Control and Communications-Tactical (PEO C3T) is responsible for the material development and fielding of each capability set and supporting network systems. In 2023 alone, more than 400 Army, Army Reserve and Army National Guard formations will be fielded with modernized network and mission command application technology. Each capability set builds on the previous one, is infused with commercial solutions informed by Soldier-led experimentation, and transitions Army science and technology initiatives into program offices. Through capability set development, the Army is enhancing the network to give commanders multiple communication choices (both military and commercial networks), remove complexity, harden against cyber and EW threats, and provide easier methods to share information with coalition partners. Most importantly, advancements in data security and management will provide the Army with zero trust attribute-based data for improved data visualization at echelon.

PEO C3T fields capability sets on a two-year basis in addition to providing supporting modernized network communications gear, mission command and cyber understanding applications, network management tools, integrated and mobile command posts, network initialization capability and communications security technology to all service components. The capability set approach uses continual market research, enabling insertion of the latest commercial capabilities into future sets, with four supporting priorities focused on institutional reforms, policy and governance, research and development, and more experimental and exploratory science and technology.

In order to incorporate real-time operational feedback and generate fewer prescriptive requirements, the PEO and Network Cross-Functional Team are utilizing the proven industry practice of development security operations (DevSecOps) and robust operational experimentation, which places developers side-by-side with Soldiers in operational units to evaluate potential technology solutions. The assessments 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.

To deliver the Army of 2030, the Army's four capability sets in Fiscal Years 2021, 2023, 2025, and 2027 will provide expeditionary, intuitive, resilient, automated, and protected capabilities that will lead to multi-domain dominance. Capability set development integrates lessons learned from Soldier touchpoints, Project Convergence, and other experimentation, and supports network modernization initiatives, including achieving unified network operations; fielding an integrated tactical network; enhancing satellite communications; delivering mission command applications and sensor-to-shooter capabilities; and advancing waveform, data management, and artificial intelligence integration. Technology insertions will continue beyond Capability Set 27 following this same iterative approach.



# JTNC

A

The Joint Tactical Networking Center (JTNC) is a support organization to the Services, the DoD Chief Information Officer (CIO), the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), the Joint Staff J6, and USD Research and Engineering (USD(R&E)).



**DESCRIPTION**

The JTNC enables secure, interoperable, and resilient tactical communications capabilities aligned to modular open architectures in support of Service, Multi-Service, and Coalition forces. JTNC core functions include maintaining a cyber-hardened DoD Information Repository (IR); providing technical analyses and capability characterizations on tactical communications products; providing open systems architecture standards; and serving as technical advisor to the Communications, Command, and Control Leadership Board (C3LB).

The JTNC is supporting ongoing Joint All-Domain Command and Control efforts by assisting in the analysis/development of appropriate architectures, Joint Force requirements, standards, mission threads, attributes and functional characteristics required to address capability gaps and needs. The JTNC serves as technical advisor to DoD CIO, and is responsible for providing oversight of Lead Service activities and assisting in the identification and resolution of cross-service networking disconnects.

**CAPABILITIES**

- DoD Information Repository (IR): The JTNC maintains a cyber-hardened DoD IR to provide controlled access for proprietary and non-proprietary waveforms and associated network managers, operating environment software, models, architectural standards, application program interfaces, and future tactical communications products. This serves to protect and distribute code and documentation based on legal agreements between government and software developers.
- Joint Communications Marketplace (JCM) is an online portal and DoD collaboration space for vendors to showcase their tactical communications products. JCM provides acquisition authorities the capability to conduct market research on

emerging technologies, informed by Government analyses that may incorporate JTNC capability characterization results.

- JTNC Capability Characterization process has been developed for commercial off-the-shelf /non-developmental item tactical communications products. JTNC's Capability Characterization verifies and validates a product's performance against developer-stated specifications to provide a report on the innovative technologies and capabilities.
- Modular Radio Architecture (MRA) will expand the Government's ability to develop affordable, secure and standardized tactical communications products. The MRA is intended to address emerging networking scenarios, while utilizing the necessary interfaces to maximize interoperability. MRA establishes open systems architecture to facilitate the integration of technology.
- Technical Analysis: The JTNC performs waveform analyses, Waveform Assessment for System Milestone Review, conformance evaluations, and capability characterizations on tactical communications products assessing which products meet their advertised capabilities and align with DoD wireless communications, interoperability, and cybersecurity standards and policies.
- Exportability Analysis and Licensing Review: The JTNC analyzes potential exportability of tactical communications products. Recommendations are provided that lead to exportability. JTNC reviews software defined radios and waveform export license requests, providing recommendations to DoD CIO. The JTNC supports Service and various DoD agencies overseeing the protection of critical technologies of wireless communications exported under commercial, direct commercial sales and/or foreign military sales and licenses/agreements.



**A-C | JTNC enables interoperable, secure and resilient waveform and wireless communications by recommending standards, conducting technical analyses, and maintaining a DoD Information Repository.**



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**



The Army fielded Capability Set 21 to seven brigade combat teams and one Stryker regiment squadron in FY21 and FY22, plus six Expeditionary Signal Battalions-Enhanced. CS21 improves expeditionary capability and makes the network simple and more intuitive. Communications systems are smaller, lighter, and faster. Soldiers find that applications and network devices are easier to learn and use, and commanders of infantry formations are provided more connectivity options to ensure they can communicate in any environment.

Capability Set 23 (CS23) fielding is underway to complete fielding to the entire Stryker regiment and one BCT, with additional BCTs plus experimentation with divisions as unit of action planned for the remainder FY23 and FY24. CS23 is building upon advances in expeditionary capabilities and intuitiveness to increase capacity, resiliency and convergence of the network.



Converged mission command applications, integrated intelligence data, and an enhanced common operational picture ensure usable information supports warfighter decision-making, underpinned by timely and accurate data.

CS23 helps to provide a more robust transport layer to support the requirements of the Army's other modernization priorities.

**CAPABILITY SET 21:  
 EXPEDITIONARY &  
 INTUITIVE**

- Integrated Tactical Network (ITN) fielded to select BCTs, a Stryker Regiment, and ESB-Es.
- Initial fielding of the common operating environment through the 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 post mobility and survivability improvements
- Improved tactical network transport to prepare for integration of IVAS

**CAPABILITY SET  
 23: CAPACITY &  
 RESILIENCY**

- Initial commercial SATCOM at-the-halt, providing high capability communications
- Continued ITN fielding to Infantry and Stryker Brigade Command Teams (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, which is a modular open systems architecture 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



**A |** A Soldier with the 3rd Infantry Brigade Combat Team, 25th Infantry Division checks his Android Tactical Assault Kit-enabled end-user device at the Kahuka Training Area, Hawaii, during the unit's Bronco Rumble exercise. Paired with a two-channel leader radio, the ATAK map-based software application enables coordination among troops with features such as a position data, chat, mission planning and shared overlays.

**B |** Soldiers with the 3rd Squadron, 2nd Cavalry Regiment participate in a live fires exercise May 31 – June 3, 2022 at Grafenwohr Training Area, Germany. The Army conducted the Network CS23 Ops Demo Phase 1 to generate additional user feedback and key instrumented data, used to make iterative improvements to CS23 Integrated Tactical Network.



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**

UNIFIED NETWORK

COMMON OPERATING ENVIRONMENT

JOINT & COALITION INTEROPERABILITY

CP MOBILITY/SURVIVABILITY



Capability Set 25 (CS25), represents the Army's shift from Brigade to Division as Unit of Action. Designating the Division as Unit of Action moves system complexity out of lower echelons, taking the burden off of the tactical edge.

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 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. Data networking capability between ground forces and aviation will provide advanced air-to-ground communications.

With Capability Set 27 (CS27), the Army's insertion of commercial technologies in two-year phases will be fully institutionalized. 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, information-sharing, and accelerated decision making.



**CAPABILITY SET 25 :  
AUTOMATED &  
PROTECTED**

- Continued ITN fielding
- Armor formation network modernization
- 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

**CAPABILITY SET 27:  
MULTI-DOMAIN  
DOMINANCE**

- 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



**A** | Capability Set 27 will integrate a range of artificial intelligence tools that will aid the commander with decision making across the battlefield.

**B** | Soldiers assigned to the 2nd Armored Brigade Combat Team, 3rd Infantry Division conduct mission command and network communications on-the-move during the Army's three-week Armored Formation On-The-Move Network Pilot, at Fort Stewart, Georgia.



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**

UNIFIED NETWORK

COMMON OPERATING ENVIRONMENT

JOINT & COALITION INTEROPERABILITY

CP MOBILITY/SURVIVABILITY



A

The Command Post Integrated Infrastructure (CPI2) program is tackling mobility, scalability and survivability of Army command posts. The program incorporates the five components of mission command—personnel, networks, information systems, process and procedures, facilities and equipment—integrating emerging technologies and leveraging Soldier feedback from experimental units.



**DESCRIPTION**

As one of the Army's top priorities for network modernization, the CPI2 program addresses the challenges posed by contemporary and future land conflict, such as physical signatures, mobility, and standardization. Command post designs for this effort are integrating approved commercial off-the-shelf (COTS) and government-off-the-shelf (GOTS) systems, as well as government programs of record (POR) that support command post operational needs.

The program is under development in two increments, termed Inc 0 and Inc 1. Inc 0 is the initial effort, which is currently executing multiple phases of prototyping, integration, and experimentation through multiple Soldier touchpoints. The feedback and lessons learned during Inc 0 is informing Inc 1, which expands upon the Inc 0 product lines with an additional mix of military vehicle platforms, including a variety of armored vehicles, Joint Light Tactical Vehicles and Medium Tactical Vehicles. The effort also consists of the Command Post Support Vehicle, which serves as a communications node for brigade and above, assorted shelter systems and supporting intelligent power capabilities.

The CPI2 program recently achieved its Milestone B decision authority under Inc 1, allowing the program to move forward into the engineering and manufacturing phase. Following the Inc 1 contract award and platform production, the Army will field the first unit equipped with Inc 1 platforms in FY25. The CPI2 program will ultimately field the modernized command post Inc 0 and Inc 1 capabilities to 86 units, with one additional system available for training activities.

**CAPABILITIES**

CPI2 leverages improvements in technology to reduce the current CP footprint and improve mobility and

agility. It consists of the integration of approved and fielded mission command information systems, GOTS and COTS technology that support the operational needs of the corps, division and brigade combat team (BCT) main and tactical CPs, and the BCT battalion CPs. The centerpieces of CPI2 are the Mission Command Platform (MCP) and Command Post Support Vehicle (CPSV). CPI2 also provides all the ancillary equipment for fully outfitting the mobile CP, including the CPI2 Integrated Support System (ISS), tents, environmental control units (ECUs), power generation, displays, tables and chairs.

- **Mission Command Platform (MCP):** The MCP provides digitally connected workstations to support staffs at CPs, as well as command groups at corps, division, and BCT. The MCP uses current PoR, GOTS and COTS systems to plan, prepare, execute and assess operations.
- **Command Post Support Vehicle (CPSV):** The CPSV hosts mission command servers, radios, local area network (LAN) systems and a Unified Voice Management System (UVMS) for conferencing, access to tactical voice radio, Voice over Internet Protocol (VOIP) telephone, and radio cross banding.
- **Integrated Support System (ISS):** CPI2 will develop or acquire the Command Post Display System (CPDS) and UVMS. The CPDS, with its accompanying software, will support enhanced collaboration and communication by allowing the commander and staff the option to view multiple common operating pictures (COPs) simultaneously. The UVMS provides data communication exchange between Army standard network and radio protocols within and between the mobile CPs.



**A | U.S. Soldiers with 4ID conduct an operational test validating the integrated capabilities of CPI2.**

**B | The 4th Infantry Division demonstrates a Command Post Platform-Improved at Fort Carson, Colorado. It represents a potential CPI2 CPSV solution.**

**C | Soldiers with the 1st Armored Division, 2nd Armored Brigade Combat Team's 1st Squadron, 1st Cavalry Regiment Main plan their mission from inside the Lightweight Mobile Command Post TAC during the Network Integration Evaluation/Army Warfighter Assessments.**



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**



# CHS

Common Hardware Systems (CHS) acquires and supports sustainment of highly flexible, cost-effective, common, and simplified non-developmental, commercial information technology (IT) solutions that improve interoperability and connectivity on the battlefield, while garnering efficient competition to enable the latest commercial technology solutions to meet tactical and operational requirements.



**DESCRIPTION**

Army Regulation 25-1 Army Information Technology identifies CHS as the mandatory source for the procurement of commercial IT hardware for tactical/operational requirements. As such, CHS coordinates across tactical programs, providing consolidated procurement and sustainment support of commercial IT hardware including non-developmental and modified commercial off-the-shelf (COTS) items. The program portfolio continually updates new contract items ensuring modern, emerging technologies are available to enable overmatch capabilities for warfighters.

The CHS office maintains a procurement contract to execute their mission in support of tactical and operational requirements. From receipt of requirements to award of a corresponding delivery order for a supported program, CHS averages a 90-day processing time with an expedited capability available to meet urgent needs.

CHS also provides the government with an increased ability to perform supply chain risk management, critical function analysis of components, critical program information assessments and implementation of other protection measures contained in program protection plans. This contract feature protects the network and strengthens the Army's cybersecurity posture.

CHS includes a pre-negotiated pricing schedule for the life of the contract with quantity discounts; additional warranty options with up to eight years of coverage providing a 72-hour turnaround time; incentives to provide the lowest price hardware; and the ability to procure technical documents based on competitive pricing.

**CAPABILITIES**

- **Rapid Acquisition:** Centralized approach to contracting streamlines ordering process, reduces time between order and delivery, and allows for economies of scale in pricing.
- **Design & Engineering:** Provides direct customer support throughout the development of new capabilities, assists in the design of hardware configurations, facilitates hardware evaluations, and informs the selection of common hardware solutions.
- **Lifecycle Management:** Provides warranty options, failure analysis reporting, worldwide 72-hour repair, and warranty/repair tracking.
- **Configuration Management:** Maintains the configuration of equipment for the life of the contract or until the product is going End-of-Life/End-of-Sale
- **Ruggedization:** Provides modified commercial IT hardware for tactical/operational use in accordance with MIL-STD-810 to ensure product survivability in austere conditions.
- **End-of-Life Management:** Coordinates with customers who previously procured items that have gone End-of-Life/End-of-Sale to determine future needs and identify suitable replacements.
- **Bonded Storage:** Provides for up to one year of bonded storage for any customer



- A | A Soldier uses a CHS ruggedized device in the field.**
- B | The Tactical Control Console is the primary interface for the AN/VIC-5 system.**
- C | A Soldier assesses his mission using CHS equipment during Enroute Mission Command exercise.**
- D | A Soldiers configures operational transit cases.**



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**



Tactical Network Initialization and Configuration (TNIC) rapidly delivers relevant network initialization products and solutions to the warfighter in support of evolving Army directives. Data Products are a collection of mission data required to initialize the tactical network and command and control (C2) applications. This data includes the information required to enable end-to-end network-centric connectivity and interoperability across the tactical internet (TI), such as internet protocol (IP) addressing, unit reference numbers (URNs), router, switch and firewall configurations, and more. Data Products are used to instantiate the digital systems. Once loaded, they populate look-up tables and local databases, and are expected to be maintained within the runtime operational environment by the systems utilizing the data or by the network manager responsible for that system.



**DESCRIPTION**

The information within Data Products is used to populate address books; create default message lists; determine communication protocols between systems; and determine how a system processes and handles information from another system. Every PM that touches the tactical network needs Data Products to establish the network layer and enable binary messaging protocols, such as Variable Message Format (VMF) and United States Message Text Format (USMTF) in support of the common operating picture (COP), situational awareness (SA) and command and control (C2) messages for Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, Reconnaissance (C5ISR) applications. All systems internal and external to PEO C3T who meet these criteria need Data Products.

**CAPABILITIES**

- **Command Control/Application (C2/Apps) Initialization:** Provides critical components that enable system-of-system interoperability for software applications that would otherwise be incompatible; assigns, manages and deconflicts Unit Reference Numbers (URN); generates address books and other application-specific data bases as required.
- **Initialization Tool Suite (ITS):** A capability fielded to units that allows them to add, modify, and delete data in their fielded data products to ensure the digital architecture is configured optimally to support the mission as it evolves through the phases of operation.
- **Network Initialization:** Provides critical components that enable system-of-system interoperability for the Army's tactical network; assigns, manages and deconflicts tactical Army IP address space for NIPR, SIPR, MPE and Colorless (private, public and multicast); assigns and manages autonomous system numbers (ASN), Global Block Numbering Plans and telephony; generation of network device configurations (i.e., router, switch and firewall) and unit specific IP plans.



**A** | Initialization products provide the technical glue to ensure the components of the overall network are able to function together in a manner consistent with current and future warfighter requirements.

**B** | The 50th Expeditionary Signal Battalion-Enhanced and 63rd Expeditionary Signal Battalion conducted a combined Large Scale Combat Operations (LSCO) communications exercise on Fort Bragg, North Carolina.



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**

UNIFIED NETWORK

COMMON OPERATING ENVIRONMENT

JOINT & COALITION INTEROPERABILITY

CP MOBILITY/SURVIVABILITY



# UNIFIED NETWORK OPERATIONS

The Unified Network Operations (UNO) program is a key enabler for resilient secure global data exchange and the Army's on-going network modernization efforts, such as a zero trust security architecture. These tools make it easier for Signal Soldiers (S6/G6) from the tactical edge up through Corps to plan, configure, manage, monitor, control and secure/defend their tactical network assets.



**DESCRIPTION**

UNO is foundational to Army network modernization efforts that enhance network security, resiliency and data exchange, and to the service's Unified Network vision — which integrates and converges enterprise and tactical networks as found in the Army Data Plan and Unified Network Plan. UNO's initial integrated suite of software applications will integrate existing network operation tools into a simplified user-friendly capability, enabling Signal Soldiers to plan, manage, monitor, configure, and secure the Army's Unified Network more effectively. Simplifying the network management and monitoring applications and tools will improve the user experience, increase situational awareness, and create stronger cyber network defense. The UNO program is moving towards a singular intuitive user interface, where Soldiers will be able to conduct endpoint management at a single device that can reach out to all of their unit's different network nodes. As the UNO program of record (PoR) matures in fiscal year 2024, future capability will further support key Army modernization efforts that will streamline strategic and installation network operations, and enhance security and data exchange through Identity Credentialing and Access Management (ICAM). UNO's ICAM software will play a major role in the Army's zero trust security architecture and attribute-based data access and exchange, which will require users to be authenticated, authorized, and continuously validated for security configuration and posture to access applications and data. Under the UNO Middle Tier Acquisition (MTA) rapid prototyping authority, PdM TCNO developed prototype tools to streamline and simplify NetOps tools used in the Capability Set design while supporting Army network modernization goals. There are several

MTA prototypes under development, with the following tools being piloted to Army units already. These prototype tools are steppingstones to a fully integrated UNO capability and will continue to merge over time leading up to the UNO PoR:

**Ruggedized Applications Platform -Tactical Radios (RAP-TR):** Combines several software applications to a single tactical network management tool to plan, configure, load, and monitor legacy waveforms and advanced networking waveforms in current and future tactical radios. This suite of Lower Tier Tactical (LTT) NetOps software tools was fielded to the first unit in FY22.

- **Atom** (Primary RAP-TR software) – an easy-to-use single radio planning and loading tool that supports all of the Army's tactical radios and four advanced/legacy waveforms simultaneously.

**UNO Planner:** Consolidates Lower Tier Tactical (Atom) and Upper Tier Tactical (UTT) planning tools into one unified application, with one easy-to-use universal graphical user interface (GUI). The UNO Planner is currently under development with piloting expected to begin late FY23.

**Network Operations Management Systems (NOMS):** This NetOps software helps Soldiers to monitor and manage the UTT network in a more streamlined, efficient and effective manner. PdM TCNO began fielding the TNT-OTM NOMS software package in FY22.

**Integrated NetOps Battalion and Below (INB2):** Monitors and manages the LTT radio network. Similar conceptually to NOMS, INB2 consolidates 11 current vendor-specific LTT management tools while providing additional capability. INB2 was granted phototype authority, with the first official pilot beginning in Nov 2022.



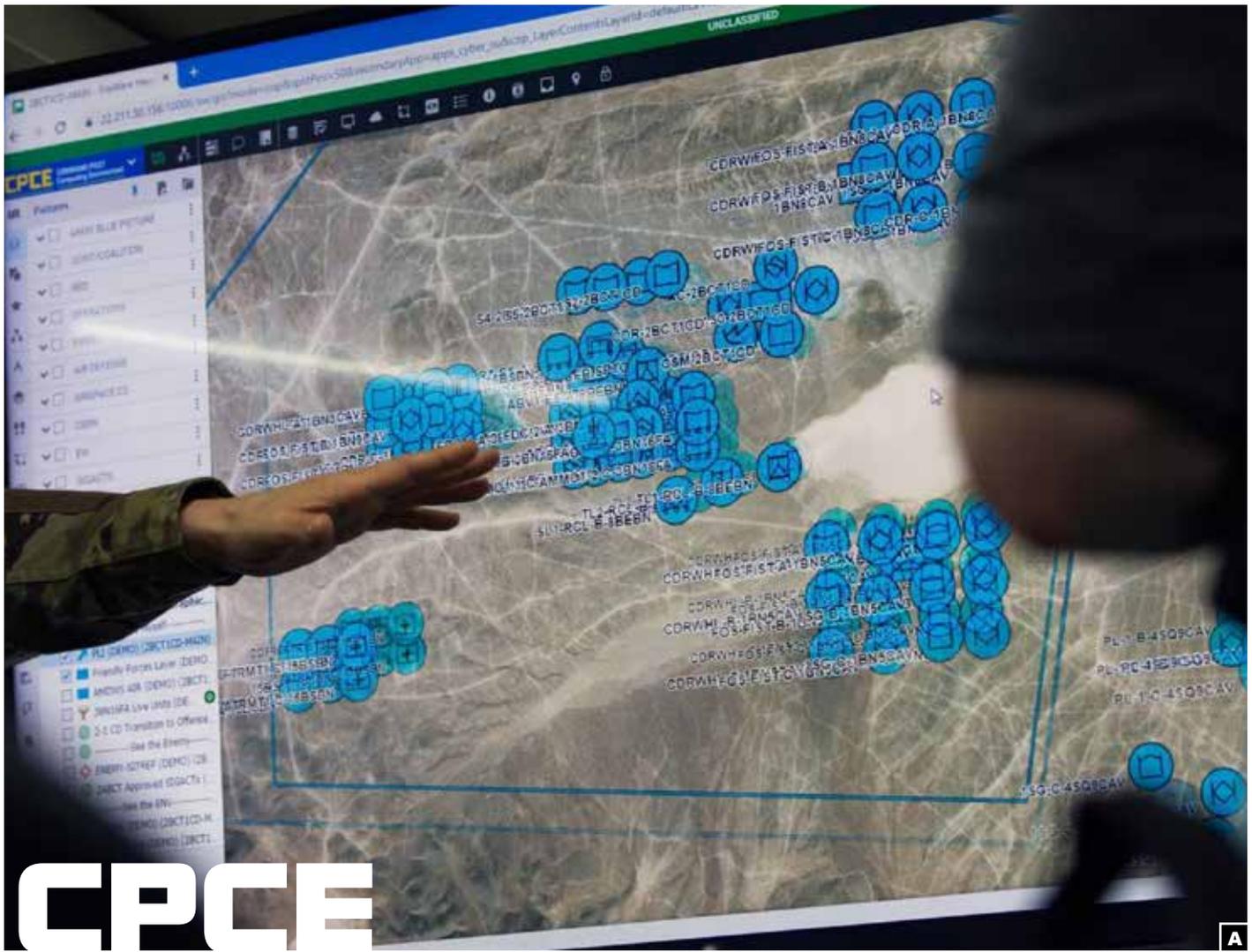
**A** | Indiana National Guard Soldiers with the 38th Infantry Division, Maj. Adam Barlow, operations chief from Shelbyville, and Capt. Justin Shutt, battle captain from Fort Wayne, monitor a simulated battle during the division's command post exercise at Camp Atterbury near Edinburgh, Indiana.

**B** | Soldiers train on mobile ad hoc network (MANET) radios during the Army's Operations Demo Phase II, conducted during the 2d Cavalry Regiment's Dragoon Ready 2023 operational exercise in Hohenfels, Germany, in February 2023, which provided an opportunity for Soldiers to train on multiple software defined radios.

**C** | A Soldier operates the UNO software, which provides a common operating picture that allows Soldiers in the command post to track every single radio on the network, during the Army's Operations Demo Phase II, conducted during the 2d Cavalry Regiment's Dragoon Ready 2023 operational exercise in Hohenfels, Germany.



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**



# CPCE

CPCE/Tactical Server Infrastructure (TSI) eliminates stove-piped legacy systems and provides an integrated, interoperable, cyber-secure, and cost-effective computing infrastructure framework for multiple warfighting functions.



**DESCRIPTION**

CPCE key features include an integrated COP, core staff utilities, coalition interoperability, backwards compatibility with current warfighting systems, and a framework onto which new and existing Warfighting System Functionality can converge. CPCE software operates on the Tactical Server Infrastructure (TSI), the Command Post computer hardware platform.

This effort eliminates duplicative or redundant implementations, speeds up and simplifies future development efforts, and enhances interoperability and data sharing across multiple echelons. The program's acquisition goals include acquisition agility, open system architectures (OSAs), reduced lifecycle costs, and a cyber-hardened foundation for applications and services.

**CAPABILITIES**

- CPCE software provides the Commander the ability to understand, visualize, and direct the operational environment allowing them to plan and execute the mission scenario. CPCE enables the command to execute the mission scenario by providing a tailorable operational picture leveraging common data; the ability to collaborate within and external to the unit leveraging voice, video, and chat; the ability to plan through wargaming leveraging artificial intelligence technology; and provides access to All Domain Networks, nonrecurring engineering of Cross Domain Solutions for Mission Partner Environment, data, information, and compute resources by leveraging Cloud Services.
- CPCE implements an integrated, interoperable, cyber-secure, software infrastructure that serves as the host for a unified set of multiple warfighting functional applications within the command post at echelons Battalion to Army

Service Component Command, eliminating “stove-piped” systems, duplicative or redundant implementations, simplifying future application development efforts, and provides key improvements in interoperability and data sharing across multiple echelons.

- CPCE offers a common geospatial solution (map) and common data services, including an extensible database and data persistence. The system is designed to reduce the training burden on Soldiers. The Integrated Software Development Kit (ISDK) allows external PoRs the ability to integrate new capabilities without rebuilding common components.
- CPCE is optimized through Developmental Operations (DevOps) to improve responsiveness, 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 manager and developers are working to address underlying data analytics, data dissemination and federation associated with the use of CPCE. These major efforts are key focuses of Capability Set 23 development.
- The latest **Tactical Server Infrastructure, (TSI)**, hardware is being fielded to units receiving CPCE. More than 860 TSiv2 systems have been fielded (about 30% of the Army) so far and are providing various improvements over the legacy Battle Command Common Services server stacks including an 800-pound weight reduction, a 50-percent reduction in setup and teardown time, and a reduction in the number of transit cases from nine to three, significantly increasing agility. The next generation of TSI, TSiv3 is currently anticipated to start fielding in FY25.



**A** | PEO C3T personnel highlight recent Command Post Computing Environment enhancements during a demonstration at Joint Base Myer-Henderson Hall.

**B** | Soldiers complete Command Post Computing Environment training during the Mission Command Training Program at Fort Leavenworth, Kansas.

**C** | During JWA21, a U.S. led multi-national division conducted tactical operations in a live, virtual and constructed environment, where the Army conducted operational assessments on several network capabilities managed by PEO C3T, including two critical to coalition interoperability – the CCE network enclave and CPCE software. The Army flexed these systems in the Mission Partner Environment and injected an operational threat with contested cyber and electromagnetic activities.



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**

UNIFIED NETWORK	COMMON OPERATING ENVIRONMENT	JOINT & COALITION INTEROPERABILITY	CP MOBILITY/SURVIVABILITY
-----------------	------------------------------	------------------------------------	---------------------------



Fire Support Command and Control (FSC2) empowers commanders to plan and execute the delivery of lethal fires and effects by providing capabilities to employ joint digital fires, enhance situational awareness and increase collaboration.



**DESCRIPTION**

FSC2 provides Army, joint and coalition commanders with the capability to plan, execute and deliver both lethal and non-lethal fires and effects. FSC2 systems comprise the entire sensor-to-shooter digital kill chain, from the dismounted forward observer through theater and Combatant Command planning cells. These systems integrate Army, Joint and coalition targeting capabilities and fuse that information with the ballistic calculations required to deliver precision munitions.

**CAPABILITIES**

- **Advanced Field Artillery Tactical Data System (AFATDS)** provides fully automated support for planning, coordinating, controlling and executing fires and effects, including mortars, field artillery cannons, rockets and missiles, close air support, attack aviation and Naval surface fire-support systems. AFATDS is the primary command and control system for Long-Range Precision Fires (LRPF) Cross-Functional Team (CFT) initiatives, such as Extended Range Cannon Artillery (ERCA), Extended Range Guided Multiple Launch Rocket System (ER-GMLRS), Precision Strike Missile Program (PrSM) and Projectile Tracking System (PTS).
- **Precision Fires-Dismounted (PF-D)** is used by forward observers and fire support teams to transmit and receive fire support messages over standard military line-of-sight, high-frequency and satellite communications radios. PF-D enhances this functionality over legacy systems with a revamped user interface and precision fires targeting capabilities. PF-D is hosted as a software application on common Army hardware in the Handheld Computing Environment.

- The **Joint Targeting Integrated Command and Coordination Suite (JTIC2S)** software solution will provide critical fires/targeting capability for joint and organic Army fire support management, and a joint fires/ targeting common operational picture (COP) for joint and coalition partners, as well as at echelon for target development. JTIC2S will replace the Joint Automated Deep Operations Coordination System (JADOCs) capability and will enable commanders to functionally integrate targeting efforts in a federated method.
- Military service branches at echelon will utilize the functions within JTIC2S for a synchronized targeting tactical picture with Army and Joint Fires COP to support Joint All Domain Command and Control (JADC2) and Multi Domain Operations (MDO) against a near-peer adversary.
- Fires capabilities in sustainment include the Lightweight Forward Entry Device (LFED), which hosts the Forward Observer System (FOS) software, enabling mounted forward observers and fire support officers to plan, control and execute fire support operations at maneuver platoon, company, and battalion and brigade levels across the mounted formation; the Profiler weather system, which improves artillery accuracy by providing meteorological (MET) data, one of five requirements for accurate predicted fires; CENTAUR, the lightweight technical fire direction system that provides an automated cannon ballistic firing solution to the Fire Direction Centers (FDCs); and the JADOCs, a joint mission management software application that provides a suite of tools and interfaces for integration across battlespace functional areas focusing on the Joint Target Cycle.



**A** | A Stinger missile is launched using a Man-Portable Air Defense System during a live-fire training exercise. The soldiers are with the 35th Air Defense Artillery Brigade.

**B** | Sgt. Eric Stadtmueller receives over-the-shoulder training on the capabilities of the Joint Automated Deep Operations Coordination System. The system is part of the Advanced Field Artillery Tactical Data System training.

**C** | Product Manager Fire Support Command and Control conducts usability testing with the 1-37 Field Artillery, 1-2 Stryker Brigade Combat Team, 7th Infantry Division at Joint Base Lewis-McChord, Washington to obtain Soldier feedback for the Precision Fires-Mounted (PF-M) system.



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**



# JBC-P

JBC-P, is the Army's current mounted friendly force tracking system, equipping Soldiers with a faster satellite network, secure data encryption and advanced logistics.



### DESCRIPTION

Fielded to the first unit equipped in May 2015, JBC-P includes an intuitive interface with features like touch-to-zoom maps and drag-and-drop icons. JBC-P will be interoperable with the Nett Warrior handheld device, managed by PEO Soldier, delivering situational awareness capabilities to dismounted Soldiers. JBC-P incorporates the common hardware solution known as the Mounted Family of Computer Systems (MFoCS), which encompasses standardized tactical computers that are scalable and tailorable to the mission and vehicle. Ranging in options from a detachable tablet to a fully loaded, vehicle-mounted workstation, MFoCS can also run other software applications, reducing size, weight and power (SWaP) demands. JBC-P builds on the situational awareness capability known as Force XXI Battle Command Brigade and Below/Blue Force Tracking (FBCB2/BFT), which is integrated on more than 120,000 platforms and is fielded or authorized to every brigade combat team in the Army.

### CAPABILITIES

- Increased accuracy and density of situational awareness to further mitigate risk of fratricide
- Orders, graphical overlays, friendly, hostile, neutral, unknown, and non-combatant situational awareness
- Free draw, free text, chat and combat messages
- Sensor integration to enable capability to pinpoint location
- Hybrid network
- Improved user interface
- Electronic Causality Report (ECR)
- Improved route planning



**A** | Mounted Family of Computer Systems (MFoCS) will serve as the hardware provider for the MCE, Android-based software.

**B** | 2nd Infantry Brigade Combat Team, 25th Infantry Division at Schofield Barracks, Hawaii, received and installed more than 250 JBC-P systems.

**C** | Sgt. Sean Spragley installs a Joint Battle Command Platform into a High Mobility Multipurpose Wheeled Vehicle at the port of Alexandroupolis, Greece.



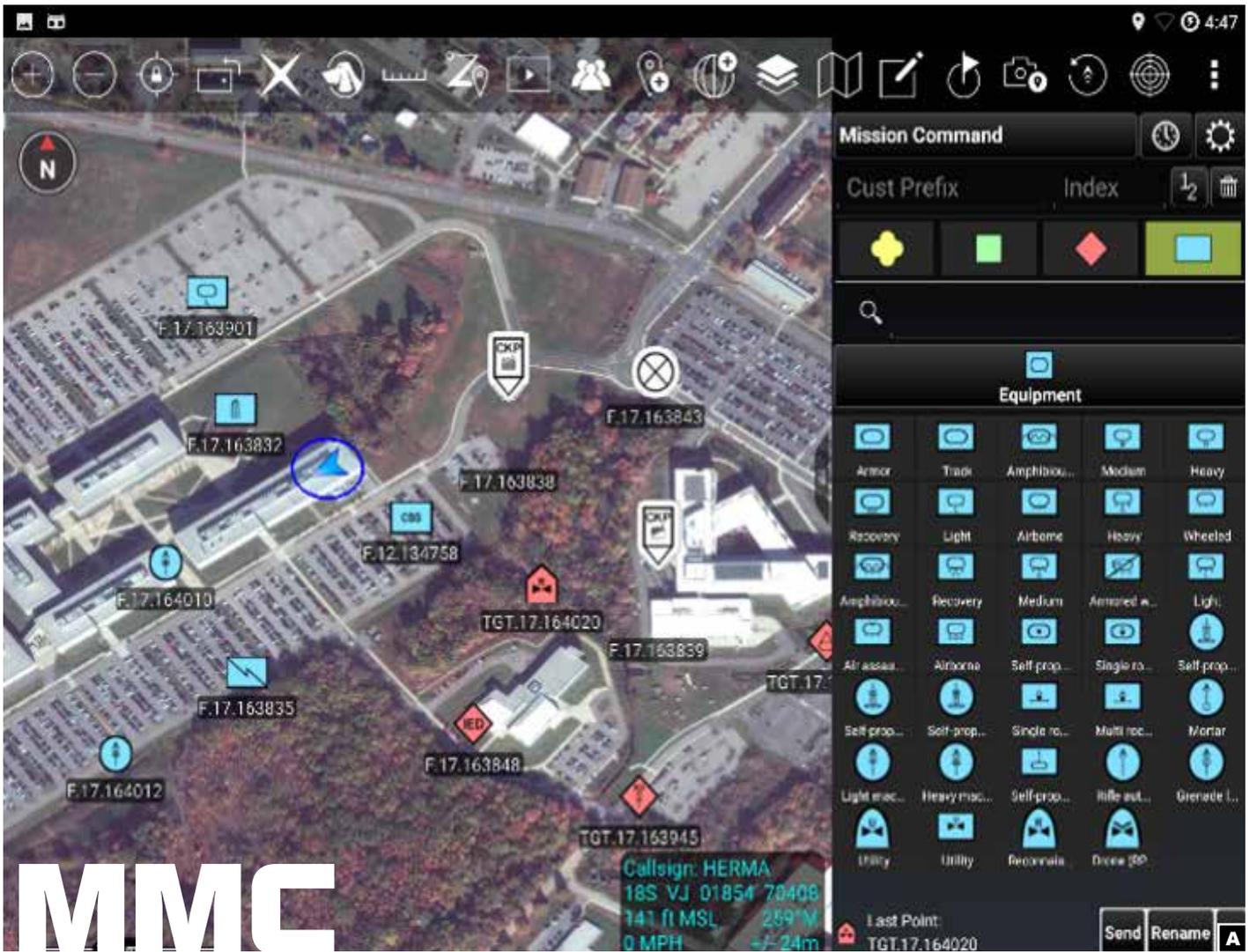
## ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

UNIFIED NETWORK

COMMON OPERATING ENVIRONMENT

JOINT & COALITION INTEROPERABILITY

CP MOBILITY/SURVIVABILITY



# MMC

The next generation of JBC-P, known as Mounted Mission Command (MMC) will leverage the existing JBC-P Program of Record and evolve utilizing a phased modernization approach with four Lines of Effort under the MMC Family of Systems: Software, Network, Transport Hardware and Compute and Store.



**DESCRIPTION**

MMC will be based on open standards that promotes competition and enables the ability to inject new technology every two years. Rather than a one-size-fits-all solution, variants of hardware will deliver MMC capability. As part of the Mounted Computing Environment (MCE) – one of six computing environments that make up the Army-wide Common Operating Environment (COE) – MMC provides all the movement and maneuver apps but also supports needs of the wider community and Warfighting Functions (WfFs) (Integrated COP, Intel, Fires, Engineer, Medical, Logistics, and third-party applications providing additional functionality through integration via the MCE software convergence architecture and infrastructure). MMC will leverage proven, Army investments – the JBC-P hardware and network – and will be deployed as a software-only upgrade to replace JBC-P software. The MMC software will exploit the MMC transport and hardware capability-maturation, continuously enhancing capabilities, security and network resiliency that outpaces adversarial countermeasures and threats. It will provide a common user-experience that enables leaders to lead and fight their formations from anywhere on the battlefield. Convergence partners leverage the infrastructure and services of MCE to develop WFF capabilities without having to build a complete system from the ground up – resulting in streamlined integration, hardening, accreditation and critical capabilities delivered to the Warfighter rapidly.

**CAPABILITIES**

- Enables Mission Command On-The-Move (MCOTM) by providing an environment for an integrated suite of platform-based mission command applications and services
- COTS-based application framework built on Android for a simplified / intuitive user experience with embedded help functions for reduced training burden
- Governing standards & common software for common look and feel across the Army Common Operating Environment (COE) enabling critical cross-cutting capabilities
- Provides a Software Development Kit (SDK) framework and infrastructure that enables an application hosting environment of all WfFs and rapid integration of third-party software
- Improved Situational Awareness (SA) through tactical symbology, graphics, and overlays
- Improved Command and Control (C2) through tactical messaging, chat, instant message, and free text
- Improved on and off-road vehicle navigation with steer-to capability and route planning
- Over-the-air (OTA) updates for maps, software, security patches, and network keys
- Multi-Band path diverse networking with APACE and Smart Routing (4G LTE, WiFi, Iridium, etc.)
- Increased on-board and off-board sensor and weapons integration via open standard interfaces
- Assured – Position, Navigation, and Timing (A-PNT)



**A | Screenshot of MMC-Software**  
**B | Soldiers from the 11th Armored Cavalry Regiment (11th ACR) at Fort Irwin, California, leverage Mounted Mission Command-Software (MMC-S) during their Blackhorse Stakes training event.**  
**C | Cpt. Jonathan DiBianca, E Troop Commander, 2nd Squadron, 11th ACR, uses Mounted Mission Command-Software during the unit's Blackhorse Stakes training event at Fort Irwin, California.**



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**



# MC CYBER

Mission Command (MC) Cyber designs, develops and deploys cyber capabilities to the Army to establish cyber operational overmatch. MC Cyber delivers capabilities to Army Service Component Commands (ASCCs) through divisions at the tactical edge that allow warfighters to understand and depict cyberspace while defending friendly key cyber terrain.



**DESCRIPTION**

MC Cyber’s agile acquisition and integration processes achieve both near- and long-term capability development to ensure dominance in the cyber battlefield.

**CAPABILITIES**

• **Cyber Situational Understanding:**

Maneuver commanders and staff have a need for effective analysis and improved understanding of the cyber and electromagnetic activities (CEMA) in their area of operations. Cyber SU provides analytics and visualization of the CEMA posture, focused on integrating cyberspace awareness and impacts during combat operations. This understanding, coupled with the ability to deploy this information in the common operating environment through Command Post Computing Environment (CPCE) software, facilitates informed planning, timely decision making, and mission accomplishment in the cyber-contested operating environment.

• **Tactical Defensive (Cyberspace Operations) Infrastructure (TDI):**

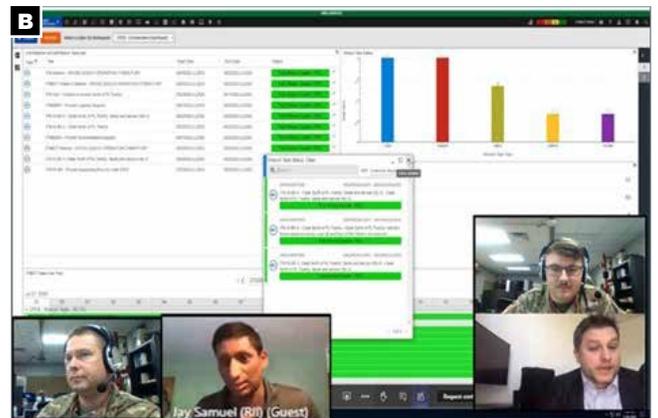
Cyberspace defenders have the need to locally and remotely protect friendly tactical cyber terrain, maneuver in and across tactical enclaves, and counter cyber adversaries to ensure the reliability of critical tasks and services. TDI provides users with active hunt and defense tools to protect against cyber-attacks in the tactical network. The TDI system is physically and logistically converged with the Tactical Server Infrastructure (TSI) to minimize size, weight, and power (SWaP) requirements at Divisions and above.



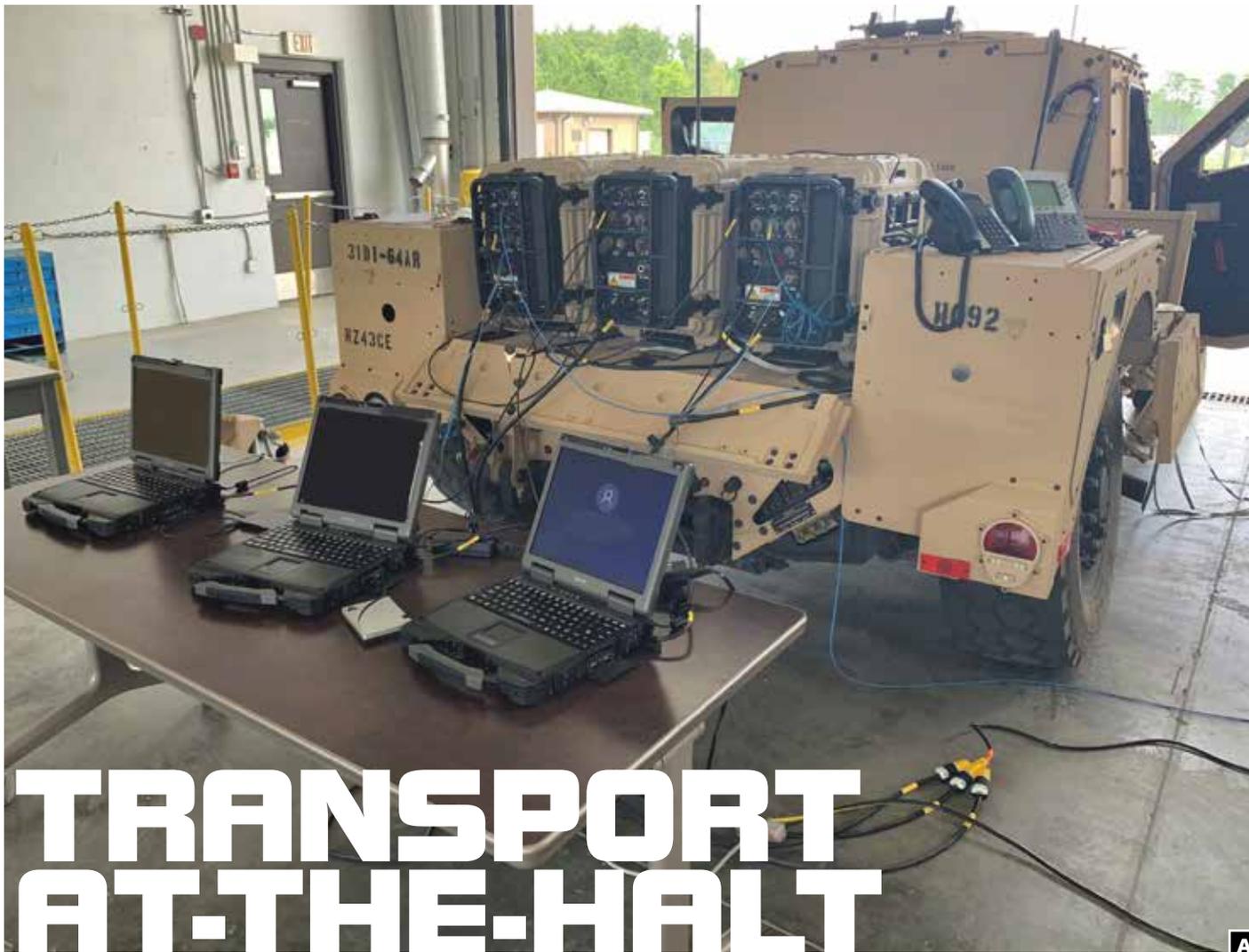
**A** | Spc. James Hyman, 915th CWB, completes an event-driven cyberspace incident scenario from the perspective of an intelligence analyst using the Cyber SU software application.

**B** | System evaluators provided visual and audio feedback on the Cyber SU prototype to developers and other key program stakeholders during the Soldier Touch Point at Ft. Gordon’s Cyber Battle Lab. This event helped to facilitate delivery of Cyber SU to III Armored Corps, which is the first unit equipped with this critical command post cyber capability.

**C** | XX



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**



# TRANSPORT AT-THE-HALT

Tactical Network Transport-At-The-Halt (TNT-ATH) enables global mission command and robust voice, video, and data communications anywhere on the planet. TNT-ATH leverages a combination of high-capacity line-of-sight (radio) and beyond-line-of-sight (satellite) communications nodes for multipath diversity and resiliency in contested environments. These robust network communications systems operate at-the-halt and at-the-quick-halt (ATQH) and deliver the real-time data that commanders need to make rapid informed decisions.



**DESCRIPTION**

To support expanding network requirements and improve the readiness of today's operational force, the Army continues to modernize the TNT-ATH capability, improving mobility, computing power, and interoperability, while optimizing and increasing bandwidth and resiliency in congested and contested environments.

Product Manager Mission Network has been delivering the Network Integration Technology Enhancement (NITE) to refresh the Army's widely fielded Joint Network Node (JNN) and Command Post Node (CPN) equipment, which is reaching end of life. The modular NITE solution provides a more than 200 percent increase in computing power, while reducing size, weight and power (SWaP) and equipment setup time for increased mobility. In conjunction with the NITE, enhanced Satellite Transportable Terminals (STTs) address STT obsolescence, increase capability, modularity, mobility, and operational flexibility, and reduce SWaP for a more expeditionary force.

Additionally, PdM Mission Network is accelerating efforts to redesign, modernize and field three enhanced TNT-ATH configuration items, which will be known as the NITE CPNv2, NITE JNNv2, and a next generation STT to be known as the Large Deployable Terminal (LDT) as part of PM Tactical Network's Satellite Communications (SATCOM) Family of Terminals.

**CAPABILITES**

- The Army's traditional TNT-ATH portfolio contains three main transportable network nodes: the Tactical Hub Node (THN) support division and above headquarters; the Joint Network Node (JNN)

supports brigade and above headquarters; and the Command Post Node (CPN) supports battalion-level headquarters and smaller-sized units.

- As part of the SATCOM Family of Terminals, Project Manager Tactical Network will modernize the current THN design, which consists of the Unit Hub Node (baseband) and the Unit Hub Satellite Truck. The modernization effort will result in a multi-band beyond-line-of-sight capability for division-level units and above, with a sizable reduction in SWaP and significant improvements in modularity and transportability. This next generation THN will be known as the Extra Large Deployable Terminal (XLDT).
- Satellite Transportable Terminals (STTs) operate in conjunction with JNNs and CPNs. These satellite terminals are designed to establish secure voice, video and data communications virtually anytime and anywhere. Future modernized capability will be known as the Large Deployable Terminal (LDT) and will be part of the SATCOM Family of Terminals.
- As part of the Army's Capability Set network modernization efforts and Family of SATCOM Terminals approach, Scalable Network Nodes (SNNs) support Expeditionary Signal Battalion-Enhanced (ESB-E) and other expeditionary formations. The smaller footprint of the SNN and reduced complexity of the kit has enabled modernized ESB-E formations to significantly increase their Command Post support, while reducing transportation requirements by more than 60 percent.



**A** | PM Tactical Network completed equipping the 1st ABCT, 3rd ID with new prototype more expeditionary TNT-ATH equipment enhancements, referred to as NITE.

**B** | A Company, 51st Expeditionary Signal Battalion train on and validate a JNN and STT, at Joint Base Lewis McChord, Washington.

**C** | Spc. Jamil Ahmed, a multichannel transmission systems operator-maintainer with the 248th Aviation Support Battalion, Maryland NG, sets up a secure internet protocol phone at Camp Grayling, Michigan.

**D** | Soldiers from the 50th ESB-E, 35th Corps Signal Brigade, set up SNN equipment during a field training exercise at Fort Bragg, N.C.



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**



Integrated on a variety of tactical vehicles to best suit unit requirements, Tactical Network Transport-On The Move (TNT-OTM) configurations enable mobile mission command and robust voice, video and data communications; from anywhere on the battlefield. TNT-OTM enables Soldiers operating in remote and challenging terrain to maintain network communications while on patrol, with connectivity similar to that of a stationary command post. Using both line-of-sight and beyond-line-of-sight for optimal network connectivity, these configurations deliver a global, mobile, resilient tactical communications network.



**DESCRIPTION**

TNT-OTM's mobility ensures effective and less predictable offensive and defensive operations in a multi-domain operational fight against a near peer adversary. In the fires battalions, these systems improve the speed and reliability of the fires network, while also extending range and increasing the survivability of artillery units. Soldiers can expand operational reach well beyond line-of-sight radio ranges and still maintain voice, chat, and data communications using satellite-based re-transmission.

**Traditional TNT-OTM** configurations include the Tactical Communications Node-Lite (TCN-L), which provides satellite and line-of-sight network connectivity, both on-the-move in a convoy, at the quick halt, and to the stationary command post; the Network Operations and Security Center-Lite (NOSC-L), which provides network management and enhanced tactical network planning, administration, monitoring and response capabilities; and the Next-Gen Points of Presence (PoPs) and Soldier Network Extensions (SNEs), which enable mobile mission command by providing on-the-move network connectivity, both line-of-sight and beyond-line-of-sight.

**MODERNIZATION EFFORTS**

- TNT-OTM is currently integrated on a variety of tactical vehicles, including Mine Resistant Ambush Protected (MRAP) platforms, Strykers, and Humvees. PEO C3T will deliver TNT-OTM configurations integrated onto the **Joint Light Tactical Vehicles (JLTVs)** that will eventually replace the Army's fleet of Humvees.
- As part of the Army's network modernization Capability Set 25 (CS) efforts, PM Tactical Network will conduct **Phase II of the Armored Formation Network OTM Pilot** in FY24. This pilot will inform the integration of final modernized OTM network design solutions into Armored Formations, to enable these lethal units to conduct more effective and less predictable offensive and defensive operations.
- One way the Army is enhancing network resiliency is through automated agnostic transport diversity, significantly increasing the number of network communication pathways available to units. The more pathway options that exist for data to travel through, the more resilient the network becomes. As part of a scalable Family of Terminals approach, PM Tactical Network is working with the S&T community to deliver the **Next Generation Tactical Terminal (NGTT)** — a single terminal that will enable automatic agnostic transport diversity, leveraging multi-orbit, multi-constellation, and multi-band capabilities. Both the OTM and At-The-Halt NGTT solutions are targeted to support CS27.



**A |** During the Army's Armored Formation On-The-Move Network Pilot, 1st Lt. T. J. Allen, the communications and network officer assigned to the 6th Squadron, 8th Cavalry Regiment, 2nd Armored Brigade Combat Team, 3rd Infantry Division, communicates with the brigade headquarters from inside his network-integrated tracked vehicle at a remote location at Fort Stewart, Georgia.

**B |** The Army concluded four weeks of testing of prototype TNT-OTM configuration items integrated on JLTV platforms, at Electronic Proving Ground, at Fort Huachuca, Arizona.

**C |** Soldiers assigned to the 2nd Armored Brigade Combat Team, 3rd Infantry Division conduct mission command and network communications on-the-move, during the Army's three-week Armored Formation On-The-Move Network Pilot, at Fort Stewart, Georgia.



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**



# RHN & GAIT

A

The Army's large fixed-installation Regional Hub Nodes (RHNs) support theater-level operations. The regionally located RHNs enable global network connectivity to securely transport information both within theater and around the world. RHNs support joint training and real-world contingency operations, as well as humanitarian, disaster relief and national emergency response. Additionally, through the Global Agile Integrated Transport (GAIT) design, commands with dispersed units around the globe can maintain mission command and network operations capabilities from their home station or forward-deployed headquarters.



**DESCRIPTION**

The GAIT network design creates a global network mesh that enables secure high-capacity voice, video and data exchange, mission command and network operations between Army formations located around world. This dynamic architecture provides multiple routing path options and solutions, enabling a more robust, resilient and expeditionary network. GAIT interconnects the Army's RHNs and multiple DoD satellite communication gateways worldwide to enable integrated global network transport. Additionally, with the continued evolution of the architecture, units can choose to bypass the RHNs or gateways and transport data directly between hundreds of GAIT Points of Presence. These network routers are installed at fixed military locations, such as corps, division, theater tactical signal brigades and special user home stations. This simplifies network transport even further and enhances multipath diversity for a more resilient network.

GAIT delivers a more unified and robust network, enabling current expeditionary network capabilities and laying the groundwork for future network transport innovation. GAIT is a cornerstone in the Army's two-year incremental network modernization Capability Set (CS) efforts, posturing the service to meet its multi domain operation goals. GAIT enables commanders to execute mission command and make faster decisions by enabling a unified network transport for mission command systems and the integration of those systems and their server stacks between home station and forward deployed locations. This unified integration

enables near real-time common operating picture that commanders can trust. It will also support the Army's future CS25 and CS27 cloud computing initiatives.

Future multi-domain operations will require an expeditionary force that is ready to fight the battle as soon as boots hit the ground. Before deploying to contingency, support or training missions, Army and Marine Corps units can leverage GAIT from their home station to complete the long list of networking configuration and policy tasks needed to connect to overseas coalition networks and conduct integrated mission command. Commanders and their units can also practice on mission command and signal integration in the forward theater before they deploy, and participate in coalition meetings and battle update briefs, increasing unit proficiency ahead of the fight.

**CAPABILITIES**

- Enables global network connectivity to transport information both within theater and around the world
- Enables home-station mission command and network operations
- Complex networking configuration and policy tasks needed to connect to overseas coalition networks and conduct integrated mission command can be completed at home-station so Soldiers can connect once they hit the ground.
- Cornerstone in the Army's two-year incremental network modernization Capability Set efforts
- Supports the Army's cloud modernization efforts



**A | The extensive satellite communications capabilities of RHNs enable regionalized reach-back to the Army's global network.**

**B | Soldiers at the network service center of CONUS East RHN provide 24/7 support to missions worldwide.**

**C | RHN network components are seen here at the Continental United States East RHN.**



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**



Enroute Mission Command (EMC) provides short notice units, such as the XVIII Airborne Corps, with the critical in-flight mission command and plane-to-plane/plane-to-ground network communications they need to be successful in joint forcible entry operations.



**DESCRIPTION**

EMC's suite of network communications capabilities provide commanders with the same mission command capabilities they would use in a command post on the ground, in essence, turning the plane into a flying command post. The real-time situational awareness enables early entry forces to be better prepared and to adjust courses of action as needed, prior to combating near peer adversaries on the ground. Once boots hit the ground, they can immediately begin executing the mission.

By leveraging technologies similar to those used by today's commercial airlines to provide inflight internet access, EMC enables rapidly deployed units to access mission command capabilities, including Advanced Field Artillery Tactical Data System, and secure reliable voice, video and data communications, all from an Air Force C-17 aircraft. Commanders enroute to an objective can tap into mission command applications and utilize services such as Secure Voice over Internet Protocol phone calls, chat and email.

Additionally, EMC capabilities increase the reliability of unit communications between aircraft. Soldiers operating EMC can extend the same enroute communications, enhanced situational awareness and planning capabilities to other planes that are flying to the mission, enabling all forces to remain synchronized.

The comprehensive real-time situational awareness and operational understanding provided by EMC can be critical to the effectiveness of the unit in the initial stages of early entry operations.

**MAIN COMPONENTS**

- The upgraded commercial Ka-band Fuselage Mount Antenna (FMA) provide tactical network connectivity on select Air Force C-17 aircraft. Once

EMC's FISA is integrated onto a C-17 aircraft, Soldiers merely roll-on the other EMC equipment, and roll it off at the end of the mission. The new commercial Ka-band provides dedicated bandwidth, improved service, and better worldwide coverage at a comparable cost.

- The Key-leader Enroute Node (KEN) provides airborne units with broadband reach-back data capability; intra-aircraft data and voice communications with subordinate units, Secure Video Teleconferencing and SVoIP, plane-to-plane and plane-to-ground communications between task force commanders and combatant commanders.
- The Dependent Airborne Node (DAN) enables subordinate commanders that are flying in formation (connected with their leaders operating a KEN) to receive critical situational awareness updates through the intra-aircraft data and voice capability. Through the DAN, commanders can utilize services such as chat and radio voice to maintain the lines of communications with their leaders and peers within the same flying formation.
- The Command And Staff Palletized Airborne Node (CASPAN) coupled with the KEN provides the Airborne task force commander and his staff with a complete platform in which they can conduct mission planning while enroute to the target area. In addition to EMC's individual workstations, this large roll-on/roll-off workstation is designed for in-flight mission command collaboration. The CASPAN has ten seat positions, four LED screens, ruggedized laptop computers, headsets, and provides adequate bandwidth to support a prioritized set of mission planning applications.



**A |** Signaleers from the 270th Signal Company, 50th Expeditionary Signal Battalion-Enhanced provided enroute communication services to joint partners during the 437th Airlift Wing's Mass Generation Exercise 2023, involving 24 C-17s. The 270th Soldiers enabled enroute comms to the Air Mobility Commander and to 2nd Battalion, 10th Marines in support of a fires mission.

**B |** Project Manager Tactical Network completed the final new equipment training on the EMC Ka-Band Upgrade Kits for Soldiers from the 270th Signal Company, 50th Expeditionary Signal Battalion-Enhanced, 35th Signal Brigade, at Fort Bragg, North Carolina.

**C | D** Signaleers from the 270th Signal Company, 50th Expeditionary Signal Battalion-Enhanced provided enroute communication services to joint partners during the 437th Airlift Wing's Mass Generation Exercise 2023, involving 24 C-17s. The 270th Soldiers enabled enroute comms to the Air Mobility Commander and to 2nd Battalion, 10th Marines in support of a fires mission.



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**

UNIFIED NETWORK

COMMON OPERATING ENVIRONMENT

JOINT & COALITION INTEROPERABILITY

CP MOBILITY/SURVIVABILITY



# HIGH-CAPACITY RADIO SYSTEMS

The high-capacity radio technologies in the Product Manager Network Modernization (PdM NetMod) portfolio provide commanders multiple communication options for a more resilient network in contested and congested environments. These solutions enable increased data flow between upper and lower echelons, and improved data fusion into the common operational picture at the brigade level and above. These high-capacity radio systems address the growing demand for distributing high-bandwidth data in harsh tactical environments.



**DESCRIPTION**

The easy-to-transport, high-capacity radios improve the expeditionary nature of U.S. Army units, while significantly increasing network throughput and range, operational flexibility and multipath diversity in contested and congested environments to enhance decision dominance.

The **Terrestrial Transmission Line-Of-Sight (TriLOS)** Radio provides a significant reduction in size, weight and power (SWaP) compared to the High Capacity Line Of Sight (HCLOS) radio that it replaces. The system is much easier and faster to set up, operate, and maintain. The TriLOS radio increases the robustness of the Army's tactical network by providing a significant increase in bandwidth and range, with lower latency than satellite communications.

The Army's next generation **Tropospheric Scatter Transmission (Tropo)** capability will provide expeditionary "beyond-line-of-sight" capability that will extend network range and significantly increase throughput, while greatly reducing size, weight and power (SWaP) requirements, compared to the current Tropo capability that it will replace. This versatile commercial system can operate in satellite denied environments, will increase multipath diversity and enhance units' PACE plans in congested and contested environments. Its lower latency compared to satellite capability, improving the performance of the network, especially for real-time applications. Tropo uses tropospheric scattering capability, which bounces signals off of the Earth's atmosphere to provide high-capacity beyond-line-of-sight capability without using expensive and limited satellite resources. It also uses particles in the atmosphere as reflectors for microwave radio signals.

The **Mid-Tier Backhaul Radios** are

similar to TriLOS but with less range and bandwidth. However, unlike TriLOS, this resilient mesh radio does not use directional antennas; it provides point-to-point, multi-point-to-point and multi-point-to-multi-point connectivity. It is portable, rapidly deployable, and units are able to operate on the move. This brigade and battalion-level mesh radio is self-forming/self-healing without need for human intervention. Mesh radio nodes are provided for command post use, integrated onto vehicles (such as Strykers and Joint Light Tactical Vehicles) and can even be used from Unmanned Aircraft like Gray Eagle and variable height antennas.

The **Tactical Radio Integration Kit (TRIK)** provides radio-bridging capability at the battalion and company level. TRIK integrates multiple varieties of tactical radios to enable different user groups, such as U.S. and coalition forces, to seamlessly communicate with different radios.

**CAPABILITIES**

- Adds multipath diversity, enhanced PACE communications, and operational flexibility to the tactical network
- Operates in satellite denied-environments
- Significant SWaP reduction over previous capability for improved unit agility
- Significant increase in bandwidth and range
- Easy to operate and deploy; requires only two Soldiers for rapid set-up/tear-down
- Fully interoperable with the Army's tactical network and architecture
- Reduces the Army's reliance on satellites; saves costs by reducing the use of commercial satellite airtime leases



**A** | 67th Expeditionary Signal Battalion (ESB) new equipment training and fielding for the expeditionary TRILOS Radio.

**B** | Soldiers from the C Company, 307th Expeditionary Signal Battalion - Enhanced train in cold weather operations in Alaska using their expeditionary network equipment, including the Scalable Network Node (SNN) satellite terminals and Terrestrial Transmission Line of Sight (TRILOS) high-capacity radios seen here.

**C** | Soldiers from the 44th Expeditionary Signal Battalion-Enhanced train with their TRILOS radio in Baumholder, Germany.

**D** | CS23 ITN classroom time is critical, shown here during a Silvus radio new equipment training class with the 3rd Squadron, 2nd Cavalry Regiment, in Germany.



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**

UNIFIED NETWORK

COMMON OPERATING ENVIRONMENT

JOINT & COALITION INTEROPERABILITY

CP MOBILITY/SURVIVABILITY



The Army's Secure Wireless systems use the National Security Agency-approved Commercial Solutions for Classified solution to provide secure classified and unclassified Wi-Fi to the Command Post, with prototype capability also enabling vehicle-to-vehicle wireless communication. Secure Wireless provides agility and operational flexibility, enabling commanders and staff to stay securely connected with full situational awareness and mission command capability for the maximum amount of time possible during command post relocation.



**DESCRIPTION**

By going wireless, command post setup and tear down times are significantly reduced, for increased unit maneuverability, operational flexibility, and survivability. Following command post setup, units can turn on their Secure Wireless and the network will come up first instead of last as with cabling, in minutes instead of hours, and Soldiers can stay connected longer when jumping the command post. Logistical burden is also reduced with less cable and protective flooring needed to be transported from location to location.

**Command Post Wireless Small Form Factor (CPW SFF)** provides secure wireless capability in the command post and other structures, enabling untethered mission command and data exchange through wireless laptops, tablets, and phones. Project Manager Tactical Network fielded a **Secure Wireless Campus Wide Local Area Network (CWLAN)** upgrade improves system resiliency, ease of use, and reduces setup/tear down times even further, for increased unit mobility and command post survivability.

To improve units' expeditionary command post capabilities, PEO C3T's Command Post Integrated Infrastructure (CPI2) modernization efforts will provide mobile, scalable and survivable platforms and further increase command post survivability. Secure Wireless is a key component of this effort and is being integrated on prototype vehicles, enabling Soldiers to pull up to any site and connect to the network in minutes. This enhanced system, known as Secure Wireless Mesh Remote Endpoint (SWMRE), will provide a vehicle-to-vehicle wireless connection that will enable units to disperse their command post vehicles, making the command post more survivable. PEO C3T is working

directly with Soldiers for continual feedback on prototype solutions and progressing toward a fielded solution. The **Mobile Broadband Kit (MBK)** is a ruggedized, cloud-managed 3G/4G LTE/5G networking platform designed to provide connectivity across a broad range of network devices. MBK enables all connected devices to push and/or pull both data and position location information to/from the secure cloud via Wi-Fi and cellular. It can be used in a command post or on-the-move for local Wi-Fi bubble without the cellular backhaul enabled.

**CAPABILITIES**

- Enables an expeditionary command post, significantly reducing command post setup and teardown time; eliminates 17 boxes of expensive cable weighing hundreds of pounds
- Fast and easy set up / tear down for rapid relocation and maneuver
- Enables commanders and staff to leverage their mission command systems much sooner, resulting in a more accurate and timelier common operating picture, improving military decision process effectiveness and unit survivability.
- Secure Wireless provides agility and operational flexibility, enabling commanders and staff to stay securely connected with full situational awareness and mission command capability for the maximum amount of time possible.
- SIPR without Encryption Hardware: National Security Agency (NSA)-approved Commercial Solutions for Classified (CSfC) software based encryption
- Transport Agnostic, Multi-Security Enclave Network
- Works with commercial, NIPR, SIPR and coalition networks.
- Up to 200 Simultaneous laptops connected.



**A-B | Soldiers from the 4th Infantry Division use Command Post Integrated Infrastructure (CPI2) capabilities, including SWMRE, during a command post exercise at Fort Carson, Colorado.**

**C | Project Manager Tactical Network provided new equipment training to Soldiers from the 57th Expeditionary Signal Battalion Enhanced at Fort Hood, Texas.**



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**



# CCE & CS-HUB

To support Multi-Domain Operations, the U.S. Army works side-by-side with coalition forces in a Mission Partner Environment, or MPE. In this coalition network environment, data is fluidly exchanged between interoperable systems so forces can contribute to a common operational picture from which commanders can make informed rapid decisions.



**DESCRIPTION**

**Commercial Coalition Equipment (CCE)** is a core component of an **Mission Partner Environment (MPE)**. It provides expeditionary coalition or commercial network connectivity to enable mission command, network communications -- voice, video, and data -- and situational awareness between Army, joint and coalition forces. Each of the coalition countries has their own unique transport networks that enable them to connect into the combined coalition network. The U.S. Army uses CCE to connect to the coalition network over its tactical communications network. This easy-to-transport system enables the Army to both send and receive select critical situational awareness with its coalition partners and contribute to a trusted real-time common operating picture across the theater of operations. The CCE can be rapidly reconfigured to provide secure tactical access for the coalition or commercial networks, to support both civil and military operations.

- **CCEv2:** connects multiple voice networks to radio nets so that key personnel not ordinarily a part of the radio network can join without requiring a radio.
- **CCEv4:** is designed to enable U.S. Army forces to implement MPE interoperability concepts for information exchange and rapid technical integration with NATO and coalition partners. Leveraging an innovative small form factor technology design, the integrated radio-bridging and voice-cross Land and Mobile Radio (LMR) module enables CCEv4 to establish multinational radio information exchanges between telephones, combat FMZ networks, and voice applications

in support of MPE command and control operations.

- U.S. Army Soldiers and coalition partners use the **Common Services-Hub (CS-Hub)** -- comprised of a CCE variant and the Tactical Server Infrastructure (TSI) -- to host mission partner enterprise services, such as email, Voice over Internet Protocol (VoIP), file sharing, chat and video teleconferencing. The TSI is comprised of ruggedized laptops that function as servers and host a variety of battle command applications.

**CAPABILITIES**

- Enables voice, video, and data communications and mission command between U.S. and coalition force networks
- Core components of an interoperable MPE
- Provides secure tactical access for coalition or commercial networks to support both civil and military operations
- CCE reduces size, weight and power (SWaP) for initial entry operations and increased unit agility.
- Provides access to commercial internet and phone services through the Tactical Network Regional Hub Nodes
- Enables mission partner enterprise services, such as email, VoIP, file sharing, chat and video teleconferencing



**A |** Chilean Army Maj. Gen. Ricardo Stangher, Multinational Forces South Deputy Commanding General, speaks on the phone during PANAMAX 2022 at Joint Base San Antonio - Fort Sam Houston.

**B |** PdM NetMod completed new equipment training with CCEv4 and Secure Wireless capabilities to the 57th Expeditionary Signal Battalion-Enhanced at Fort Hood, Texas.

**C |** Chief Warrant Officer 2 Roberto Gonzalez, a network engineer at U.S. Army Joint Modernization Command, works on creating the Project Convergence Mission Partner Environment during a Risk Reduction Event in February at Joint Modernization Command at Fort Bliss, Texas.



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**



# MCN-AE

A

Sharing intelligence data is critical to successful missions on the battlefield. 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 stand-alone TROJAN Intelligence Network, but instead using the Army's Tactical Network.



**DESCRIPTION**

Each MCN-AE fits into a suitcase-sized transit case, and the system uses a unit's organic tactical network transport equipment to relay intelligence data across the battlefield. MCN-AE enables the Army to replace the tactical elements of the intelligence network's TROJAN Special Purpose Integrated Remote Intelligence Terminal (SPIRIT) system, a large truck and trailer, with two carry on cases, cutting down on footprint. The system reduces size, weight and power (SWaP) requirements for a more expeditionary force while increasing a unit's operational flexibility.

MCN-AE improves operational flexibility and multipath diversity. Unlike the current TROJAN Network that only uses the TROJAN SPIRIT system for network transport, the Tactical Network provides numerous network transport options via a wide range of Army transport nodes. These network transport nodes can operate in all satellite bands (Ka, Ku, X-band, etc).

The MCN-AE also enables commanders conducting operational missions to dynamically assign bandwidth between their tactical mission command and intelligence assets as they see fit, with the ability to reassign additional bandwidth on demand.

Traditionally, in the past, the Army's tactical operations, intelligence, logistics and medical communities each used separate

communications networks to pass information. The Army is converging the intelligence, logistics and portions of the medical networks onto the tactical network, an effort, known as Transport Convergence. The lightweight expeditionary MCN-AE is at the heart of the intelligence convergence effort – Phase 1 of Transport Convergence.

**CAPABILITIES**

- Provides intelligence data exchange with commercial off-the-shelf and/or government off-the-shelf baseband network
- Reduces size, weight and power (SWaP) for increased unit agility
- Enables commanders conducting operational missions to dynamically assign bandwidth between tactical mission command and intelligence assets, with the ability to reassign additional bandwidth on demand
- Uses the robust and redundant tactical network, delivering needed redundancy to the intelligence community



**A** | The small form factor 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 Army's Tactical Network.

**B** | Each MCN-AE fits into a suitcase-sized case, and the system uses a unit's organic tactical network transport equipment to relay intelligence data across the battlefield.

**C** | PM Tactical Network demonstrated MCN-AE to Army leadership at the Army National Guard G6 Mission Command Workshop at Little Rock, Arkansas.



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**

UNIFIED NETWORK

COMMON OPERATING ENVIRONMENT

JOINT & COALITION INTEROPERABILITY

CP MOBILITY/SURVIVABILITY



The Army's flexible, modular, scalable and tailorable Satellite Communication (SATCOM) Family of Terminals provide an optimal variety of expeditionary, mobile satellite terminals to units worldwide to best support different formations, echelons, mission requirements, and locations. These SATCOM systems provide global voice and data network communications, and the exchange of time-sensitive situational awareness, intelligence, and mission command information, while at-the-quick-halt, during all operational phases, echelons and missions -- from initial entry at the tactical edge to more mature long-standing operations. The expeditionary quick set-up easy-to-use systems facilitate the fusion of maneuver, fires, intelligence and sustainment information at the front edge of the battlefield and remote locations.



**DESCRIPTION**

The commercial Family of SATCOM Terminals supports command post mobility and survivability by providing several easy-to-deploy, quick-set up/tear down communications solutions for units to relocate rapidly, while delivering critical real-time battlefield situational awareness to keep forces safe and ensure mission success.

As the Army looks to integrate new capability every two years as part of its iterative network modernization Capability Set design, acquisition and fielding process, the service is leveraging the Family of Terminals acquisition strategy to support its expeditionary SATCOM needs. This strategy allows for procurement of the most capable and formation-appropriate terminals to best suit requirements. The Army plans to further streamline the current variety of ground satellite equipment in its portfolio, leveraging the more versatile “family of systems” approach, while retaining the acquisition flexibility to insert new technologies as they evolve.

**CAPABILITIES**

Extra Small:

- **Global Rapid Response Information Package (GRRIP)** and modernized T2C2-Ultra Lite [Integrated antenna] fits into a single handheld airline carry-on transit case for rapid mobility and force scalability; set up and connect in minutes; utilize L-Band; and support multiple security and mission enclaves

Small:

- **SCOUT-Small** (0.65m/0.95m) is transportable in three hard side transit cases; supports 12 users over multiple enclaves; is airline checkable for commercial transport; rapidly setup by two Soldiers; and is tri-band capable (X, Ku, & Ka)

Medium:

- **T2C2 Lite** [1.2m Inflatable Satellite

Antenna (ISA)] and T2C2 Lite v2 (1.3m ISA) are transit case-based and airline checkable for commercial transport; support six users over multiple enclaves; rapidly setup by two Soldier; and are tri-band capable (X, Ku, & Ka).

- **SCOUT-Medium** (1.3) is transit case-based and airline checkable for commercial transport; supports 48 users over two enclaves, rapidly setups by two Soldiers and is tri-band capable (X, Ku, & Ka).
- **Scalable Network Node (SNN)** -- See TNT ATH
- **Sustainment Transport System (STS) SATCOM** – See STS

Large:

- **T2C2 Heavy** (2.4m ISA) is transit case-based and airline checkable for rapid commercial transport; supports 48 users over multiple enclaves, sets up quickly by two Soldiers; is tri-band capable (X, Ku, & Ka), and is used by brigades, divisions and corps.
- **Phoenix E-Model:** The new Phoenix E-Model, which replaces the larger footprint D-Model, is being fielded to Expeditionary Signal Battalion-Enhanced (ESB-Es) and other critical formations to provide large division and corps headquarters with agile high-bandwidth network communications.
- **Satellite Transportable Terminal (STT)** – and the future enhanced capability to be known as the Large Deployable Terminal (LDT); see TNT ATH

Extra Large:

- **Tactical Hub Node (TCN)** and the next generation enhanced THN to be known as the Extra Large Deployable Terminal (XLDT) – See TNT ATH
- **Deployable KU-band Earth Terminal (DKET)** – see DKET



**A** | The Army’s SATCOM family of terminals provides expeditionary and mobile satellite terminals to units worldwide.

**B** | PdM UNCI and PdM SATCOM successfully fielded expeditionary SCOUT satellite communications equipment to deployed U.S. Army Europe and Africa units during 4QFY22 in support of logistics data exchange.

**C** | Soldiers from the 50th ESB-E used their new quad-band Phoenix-E Model system in a non-training environment for the first time, supporting the Army SD-WAN Pilot at Fort Bragg, North Carolina.



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**



The Secure, Mobile, Anti-Jam, Reliable, Tactical Terminal (SMART-T) is a protected satellite terminal that provides resilient global beyond-line-of-sight (satellite) data exchange for the current and future unified network. The system enables commanders at brigade and higher to operate in an electronic warfare threat environment that includes both radio frequency signal interference (jamming), signal detection and geographic location threats. SMART-T makes it possible for units to reliably and securely extend the range of their network in such a manner that communications cannot be jammed, detected or intercepted, enabling Soldiers to send critical text, data, voice and video communications beyond their area of operations.



**DESCRIPTION**

Additionally, the SMART-T can also survive the effects of a high-altitude electromagnetic pulse produced by nuclear detonations and can operate and survive in a biological and chemical environment.

SMART-T uses the Advanced Extremely High Frequency (AEHF) satellite constellation, providing the Army with the highest level of protected communications. Additionally, SMART-T provides fully interoperable communications with the AEHF and Milstar terminals of other services (US Air Force, US Navy, US Marine Corps, and other DoD agencies and activities).

**CAPABILITIES**

- Interoperable with AEHF satellite constellation
- Enhanced system interfaces
- Provides Low and Medium Data Rate or Extreme Data Rate capability for voice and data transmission via Serial and/or Ethernet interfaces (future).
- Provides anti-jam and anti-scintillation (nuclear environment) communications



**A** | The 2nd BCT, 1st ID used this SMART-T at Hohenfels Training Area, Germany during Allied Spirit VIII.

**B-C** | Members of Charlie Company, 44th Expeditionary Signal Battalion-Enhanced, 2d Theater Signal Brigade, conduct field communications and data tests between the Terrestrial Transmission line of sight radio systems via the SMART-T near Baumholder, Germany.



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**

UNIFIED NETWORK

COMMON OPERATING ENVIRONMENT

JOINT & COALITION INTEROPERABILITY

CP MOBILITY/SURVIVABILITY



# DKET

Deployable Ku-band Earth Terminals (DKETs) are commercial non-program of record satellite systems that are designed for use at larger hub locations – such as brigade and higher headquarters elements -- to augment the Army's unified tactical communications network infrastructure. The versatile DKET can operate on commercial Ku-, Ka and X-band. They are transportable and self-contained, and can establish headquarters-level, network-hub connectivity anywhere a mission dictates.



**DESCRIPTION**

Some of the DKETs take on dual roles as hubs, providing inter- and intra- theater satellite links at brigade and higher, and linking multiple regional command headquarters. DKETs reduce network traffic load on the Army's five global Regional Hub Nodes by providing network hub services for disadvantaged forward units. They also come in a vehicle-based version, known as a Mobile DKET, or MKET).

DKETs also support other countries, services and agencies world-wide. This support is expanding to include DKETs in fixed locations, the Fixed DKET, or FKET.

The Army's new Satellite Communications (SATCOM) Terminal Remote Monitor Management Network (STRMM) enables management and control of a DKET from a secure remote location, helping to reduce Field Service Representative footprint.

**CAPABILITIES**

- Three configurations: DKET Light (3.7 – 3.9M), Mobile DKET (4.5M) and Standard DKET (4.6M – 7M), with the majority being the light design
- Establishes headquarters-level, network-hub connectivity anywhere a mission dictates
- DKETs operate on Ku, Ka and X-band frequencies
- DKET Light has a tri-fold antenna and a smaller shelter to make redeployment and setup faster and easier
- The robust DKET network makes for a seamless transition to backup equipment or terminals, eliminates long outages and minimizes impact to the Soldier
- Transportable and self-contained; electronics housed in separate shelters
- Reduces network traffic load on the Regional Hub Nodes by providing network hub services for disadvantaged forward units



**A | A DKET is shown as part of Project Manager Tactical Network's Ka and X-band frequency certification effort that enables earth satellite terminals to utilize military satellites.**

**B | DKETs support commercial Ku-Band frequencies and their electronics are housed in separate shelters. They are highly transportable, self-contained and can establish headquarters-level, network-hub connectivity anywhere a mission demands.**

**B | DKETs also come in a vehicle-based version, known as a Mobile DKET, or MKET.**



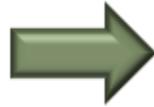
**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**



CSS Automated Information System Interface (CAISI)



CSS VSAT



## New Sustainment Transport System (STS)



STS SATCOM



STS Line of Sight (LOS)



Wi-Fi  
STS Wireless Fidelity (Wi-Fi)

# STS

A

Sustainment Transport System (STS) will provide secure, expeditionary, easy to use, global data transfer for the logistics community -- including logistics, personnel, medical and force protection data -- to enable the rapid delivery of the right supplies and personnel to the right locations on the battlefield. Developed for the general purpose user, these easy to deploy network transport systems will provide the resilient, high-capacity connectivity needed to enable the exchange of critical logistics information worldwide. The U.S. Army continues to modernize the way it exchanges logistics data, both globally and locally on the battlefield. In support, in fiscal year 2023 the service established three new STS data transport programs of record (PoRs): STS Satellite Communications (SATCOM), STS Line-of-Sight, and STS Wireless-Fidelity (Wi-Fi).



**DESCRIPTION**

The legacy logistics network program, known as the Combat Service Support (CSS) network, has been in operation since 2004. PdM UNCI continues to deliver bridge enhancements across the Army's current fleet of logistics systems to make the CSS network more secure and capable. PdM UNCI will continue to manage CSS systems until the STS network systems are fielded across the force.

To support STS SATCOM, commercial ground satellite terminals will provide the tactical network transport needed to enable global data exchange for the Army's logistics information systems and applications, such as Enterprise Resource Planning (ERP), Global Combat Support System-Army (GCSS-Army), Integrated Personnel and Pay System-Army (IPPS-A), Medical Communication for Combat Casualty Care (MC4) and General Fund Enterprise Business Systems (GFEBBS). STS SATCOM systems will expand current CSS SATCOM capabilities to operate on both commercial and military satellites on Ku, Ka, and X bands.

For local data exchange across battlefield logistics support locations, STS Line-of-Sight will increase the range and speed of existing line-of-sight data transmission solutions, while STS Wi-Fi will provide secure wireless connectivity at each of the STS network nodes. All of the easy-to-use STS expeditionary network transport systems are developed for general-purpose users and can be rapidly setup and torn down for enhanced unit maneuverability.

The modernized STS solutions will also provide a more robust capability to support predictive maintenance, telehealth services, and other emerging sustainment services that support the Warfighter.

PdM UNCI is conducting early lab and field-based experimentation and Soldier assessments to inform STS capability and design requirements needed to modernize the legacy logistics network. As part of the process, Soldier feedback is helping to inform near-term Army requirements and future acquisition decisions for an STS solution that is secure, affordable, and in-line with the Army's network modernization priorities.

On the current timeline, following future acquisition decisions, the service plans to begin fielding STS capability to units in FY24.

**CAPABILITIES**

- Secure high-capacity global tactical network transport – SATCOM, Line-Of-Sight and Wi-Fi
- Fully capable to integrate into the Army's unified network
- Leverages the Regional Hub Nodes and Global Agile Integrated Transport
- Commercial auto-acquire satellite terminals
- Easy to use for general purpose user
- Easy to transport for rapid deployment and battlefield mobility
- Supports Army Enterprise Resource Planning solutions



**A** | The Army initiated three new network transport programs of record known as the Sustainment Transport System (STS): STS Satellite Communications (SATCOM), STS Line-of-Sight, and STS Wireless-Fidelity (Wi-Fi). The STS systems will modernize and ultimately replace the SATCOM and line-of-sight systems in the current logistics network program, known as Combat Service Support (CSS), which have been in operation since 2004 and are nearing obsolescence.

**B** | Alert to the critical importance of logistics to any future conflict, the U.S. Army continues to modernize the way it exchanges logistics data, both globally and locally on the battlefield. In the photo, Paratroopers in the 189th Combat Sustainment Support Battalion, 82nd Airborne Division Sustainment Brigade, conduct defense operations as they execute 360 degree security while providing transportation, fuel, maintenance and communication support during Joint Readiness Training Center Operations at Fort Polk, Louisiana.



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**



The Combat Net Radio (CNR) is a single-channel voice and data radio that is part of a holistic effort to phase-out legacy Single Channel Ground and Airborne Radio System (SINCGARS) radios across all service components.

**DESCRIPTION**

The CNR program is one part of the SINGARS modernization strategy that encompasses fielding of HMS Manpack and Leader tactical data radios and modernization of cryptographic devices. The CNR effort supports National Security Agency and Department of Defense cryptographic modernization goals and the Army's unified network strategy by providing assured command and control voice, and limited Fires and Air Defense data in environments where access to the Integrated Tactical Network (ITN) is degraded, enabling multiple communications options for commanders. The radio will be available on both mounted and dismounted missions. The CNR will replace the RT-1523 series legacy radios. It will also continue to support the SINGARS waveform and its associated future upgrades. The CNR maintains the SINGARS ability to provide very high frequency (VHF) communication capability, providing both voice and data handling capability in support of command-and-control operations. CNR-enabled communications will be used for voice transmission of command and control between surface and airborne command and control assets but will also be used to transmit and receive secure data, including position location information within a network via radio-based situational awareness and will func-

tion as a digital data radio. CNR development is part of two Indefinite Delivery/Indefinite Quantity (IDIQ) contracts, with an initial delivery order in March 2022.

**CAPABILITIES**

- CNR will operate in the VHF band and can be used in either single channel or frequency hopping configurations.
- Vendors are considering new-frequency hopping capabilities and cryptographic modernization that includes Tactical Secure Voice Cryptographic Interoperability Specification (TSVCIS) and Advanced Encryption Standard (AES) 256.
- Software programmable to accept future updates. It will provide multipath diversity at the tactical edge.
- Following first article test completion and NSA certification, the Army will field to its first CNR-equipped unit in 4QFY24/1QFY25, with final delivery in the 2030 timeframe.



**A | Soldiers will conduct operations using the new SINGARS waveform.**

**B | CNR radios**

**C | U.S. Army 2nd Lt. Grant Navakuku with the 856th Military Police Company connects an antenna to a Single-Channel Ground and Airborne Radio System (SINGARS) during the situational training exercise (STX) lanes event at Florence Military Reservation, in Florence, Ariz.**



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**



# COMMUNICATIONS SECURITY

COMSEC develops, procures, integrates, tests, fields, and maintains Army general-purpose solutions, which utilize National Security Agency (NSA) cryptographic key material. COMSEC-managed products protect Army communications across the globe in weapon systems, in tactical environments, and throughout the Army's Enterprise Information Infrastructure.



**DESCRIPTION**

COMSEC focus areas include Army Key Management Infrastructure (AKMI) and COMSEC Cryptographic Solutions (CCS). AKMI provides users with an organic key generation capability and a secure, electronic key distribution means to load NSA-generated keys into End Crypto Units (ECUs). AKMI consists of Management Client (MGC), Automated Communications Engineering Software (ACES), Next Generation Load Device (NGLD) family, and Simple Key Loader (SKL).

PdL COMSEC is developing the Next Generation Load Device-Medium (NGLD-M), which will replace the SKL and fulfills COMSEC modernization for key loading across the DoD. The NGLD-M will support stronger cryptographic keys and a more secure method of delivery than the current SKL. These cryptographic key fill devices enable a Soldier to communicate by secure phones, classified computers, and secure VTCs at SECRET, TOP SECRET and other high classification levels. PdL COMSEC also develops CCS, which defends all echelons of the Army Network with modern cipher algorithms.

**CAPABILITIES**

- **Cryptographic Mission Planner:** Provides ACES crypto network planning; generates Signal Operating Instructions; creates COMSEC key tags.
- **COMSEC Load Devices:** NGLD-Small, SKL and in the future NGLD-Medium transfer mission critical cryptographic keys fill into ECU devices and tactical radios.
- **Secure High Assurance Inline Encryption (INE) Link Device:** COMSEC Cryptographic Systems are comprised of INEs, which secure the Army's data and voice communication networks. INE encryption devices include inline network and inline media, link and trunk, secure voice, and commercial solutions for classified communications.



**A** | TKL crypto key device, which answers the Army's call for the NGLD-S, provides critical command and control of emergency, time sensitive and secure communications during Special Forces missions. The TKL's smaller and dimmer screen reduces detection during nighttime operations, making it a critical capability for U.S. Army special operations.

**B** | The NGLD-M will replace aging Simple Loader fill devices and will be used to transfer the strongest NSA-generated cryptographic keys to tactical, strategic, and enterprise network systems.

**C** | Special Forces at U.S. Army Special Operations Command Headquarters, Fort Bragg, North Carolina, initialize their new TKL as part of a new equipment training class in March 2021, where they loaded the cryptographic keys onto tactical radios.



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**



Helicopter and Multi-Mission Radios (HAMMR) procures tactical communication enhancement equipment, ancillaries, and related services in support of the Army's Unified Network Plan.



**DESCRIPTION**

HAMMR provides air-ground interoperability between maneuver ground forces and aviation and is the Army's program for the Integrated Tactical Network (ITN) concept and tactical radio Commercial Off the Shelf (COTS) procurement, fielding, and sustainment. HAMMR radio products include all Army Link-16 radios (Ground ADA, Ground Fires, Aviation, and Gateways).

**CAPABILITIES**

**ITN:** The ITN injects new commercial components and network transport capabilities to lower echelons for capability sets within the Army's tactical network environment. The Army fielded ITN Capability Set 21 to seven infantry brigade combat teams and a partial fielding to one Stryker regiment. ITN Capability Set 23 is underway, fielding to the entire Stryker regiment plus one infantry brigade combat team, with multiple brigade combat teams and divisions as unit of action (DivUA) planned for FY23 and FY24.

**High Frequency Radios:**

- Modernized HF radios support the Army's Class II Engineering Change Proposal (ECP) for ground-based HF requirements to replace the Army's current PRC-150 HF ground-based radio with the new PRC-160 HF Radio.
- The PRC-160 meets new NSA crypto-modernization standards, transmits data faster than the existing HF radio, and is the smallest, lightest and fastest HF Manpack radio systems available.

**Air Ground Networking Radio**

**(AGNR):** Air Ground Networking Radio (AGNR) uses Program of Record ground radios and a federated integration approach that will allow aviation to keep pace with technological changes on the ground to enable Multi-Domain Operations (MDO) Force Packages by FY28.

- ANGR maintains air-ground interoperability between maneuver ground forces and aviation. AGNR will provide commanders enhanced situational awareness and Mission Command to provide a more responsive means of directing aircraft to match changing maneuver forces.

**Multifunctional Information Distribution Systems (MIDS):**

MIDS Low Volume Terminal (LVT) (2/11) is the DoD's primary Link 16 tactical data link network, which provides interoperability, situational awareness, and support for air and missile defense operations at division through corps.

- MIDS Joint Tactical Radio System (Ground Variant) builds upon and will ultimately displace MIDS LVT with a software defined radio solution that introduces modernized Link16 networking.

**Survivor Handheld Evader**

**Locator Device (SHIELD):** CSEL provides aircrews with end-to-end global satellite secure emergency communication capability during combat and peace-time flying operations. The Next Generation Survival Radio (NGSR) CSEL will provide the current CSEL radio capabilities in a smaller, handheld form factor.



**A |** Soldiers with Task Force Falcons exit a CH-47 Chinook Helicopter during Swift Response 21 at Babadag Training Area, Romania. Swift Response 21 was a Defender 21 linked exercise, an annual large-scale US Army-led, multinational, joint exercise designed to build readiness and interoperability between US, NATO, and partner militaries. Air to ground interoperability between maneuver ground forces and aviation provides critical position location information for commanders and their troops.

**B |** A Soldier with the 1st SFAB loads a mounted radio during a validation exercise, at US Army Fort Benning to train military partners during large-scale combat operations.

**C |** Soldiers from the 21st Theater Support Command (TSC) received training on the new PRC-160 HF radio in Baumholder, Germany, which provides increased throughput rates and addresses obsolescence and cryptographic modernization challenges found with the Army's legacy AN/PRC-150 radios.



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**

UNIFIED NETWORK	COMMON OPERATING ENVIRONMENT	JOINT & COALITION INTEROPERABILITY	CP MOBILITY/SURVIVABILITY
-----------------	------------------------------	------------------------------------	---------------------------



# HMS

Handheld, Manpack and Small Form Fit (HMS) acquires Non-Developmental Item radio solutions, providing affordable networking tactical radio systems that meet operational requirements from the Army. Other customers include the Marine Corps, Navy, and Special Operations Command (SOCOM). HMS products provide state-of-the-art networking waveforms, provide human factor upgrades over legacy radio solutions, and are interoperable with specified radios within the current force.



**DESCRIPTION**

Handheld, Manpack and Small Form Fit (HMS) is the total lifecycle manager for tactical radio communication. Paramount to the HMS mission is providing interoperable communications to the tactical edge Warfighter with an on-the-move, at-the-halt and stationary Line of Sight (LOS)/Beyond the Line of Sight (BLOS) capability for both dismounted personnel and platforms. HMS radios provide voice communications as well as support for data services such as text, control graphics, imagery, and video to the tactical edge Warfighter through interoperability with tactical End User Devices (EUDs), and provide Single Channel Data Radios (SCDR), primarily in support of the Integrated Visual Augmentation System (IVAS). HMS products enable net-centric operations, operate in multiple bands and multiple modes, and deliver reliable, secure tactical communications. They are network-scalable to meet operational needs and are developed based on reprogrammable modular Software Communications Architecture (SCA), allowing field and depot service to upgrade such features as security and waveforms.

**Full Rate Production (FRP)**

**Leader Radio:**

- AN/PRC-148C(v)6, Two-Channel, Single Channel Ground Airborne Radio System (SINCGARS), Warrior Robust Enhanced Network (WREN) TSM™
- AN/PRC-163(v)2 and AN/PRC-163(v)3, Two-Channel, SINCGARS, TSM™

**FRP Generation 2**

**Manpack Radio:**

- AN/PRC-158, Two-Channel, Type 1 and Type 2, SRW, MUOS, SINCGARS, SATCOM, WREN TSM™
- AN/PRC-162, Two-Channel, Type 1 and Type 2, SRW, MUOS, SINCGARS, SATCOM, WREN TSM™

**Single Channel Data Radios (SCDR)**

- Streamcaster Mini 4210 (SM4210), One-Channel, Unclassified Data Only, MN-MIMO
- Domo Tactical Communications Software Defined Radio Individual ODU Cable Variant (DTC-SDR-I OCV), One-Channel, Unclassified Data Only, MeshUltra

**CAPABILITIES**

- Simultaneous voice, data and video communications
- Software reprogrammable, enhancing network security and sustainability
- Increased throughput using networking waveforms such as TSM™
- Routing and Retransmission (Crossbanding)
- Increased functionality in a reduced footprint to include Size, Weight, and Power (SWaP) improvements, and additional waveforms (e.g. TSM™, WREN TSM™ and legacy TACSAT for the Manpack)
- TACSAT modernized Mobile User Objective Systems (MUOS) for BLOS
- Interoperability with legacy systems and End User Devices (EUD)



**A** | Soldiers with the 2nd Battalion, 501st Parachute Infantry Regiment (2-501 PIR), assigned to the 1st Brigade, 82nd Airborne Division operate AN/PRC-148C Leader Radios during the HMS Soldier Touch Point at Fort Bragg, N.C.

**B** | The IVAS single channel small form factor radio forms an intra-company level network, designed to support the rapid sharing of IVAS data including PLI. The IVAS system will then pass data from the platoon level into the ITN's TSM™ network for consumption at echelons above the close combat force.

**C** | Cpt. Chiara Botello, battalion S6 for the Brigade Support Battalion (BSB), 3rd Infantry Brigade Combat Team, 25th Infantry Division, operates the Manpack MUOS radio at Dillingham Army Air Field, Hawaii, during the unit's Bronco Rumble exercise.



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**



The Integrated Tactical Network (ITN) is a critical component to the Army's Unified Network Plan. It is delivering a tactical network that is providing expeditionary, mobile, simple to use and hardened capabilities at brigade and below and is currently scaling up to support Division as Unit of Action network solutions for Army 2030 priority units.



**DESCRIPTION**

The ITN provides a simplified, independent, mobile network solution that is available down to the small-unit dismounted leader to facilitate mission command, situational awareness and air-to-ground integration. The ITN incorporates the Army's current tactical network environment (applications, devices, gateways, and network transport) with commercial off-the-shelf components and transport capabilities.

The ITN includes several varieties of high-capacity, line-of-sight software-defined tactical radios, including both single channel radios and two-channel Leader and Manpack Radios running on advanced networking waveforms. It includes voice and data gateways; tactical cross domain solutions; small aperture satellite terminals; expeditionary servers; variable height antennas, commercial phone technology, and small satellite terminals and capabilities that enable transmission between different formats and vehicle-based kits to allow future technology insertions.

ITN radios deliver applications through the Nett Warrior end-user device to consolidate the air, ground and fires pictures onto a single common operating picture.

ITN technologies enable communications through a Secret and a secure but unclassified -encrypted (SBU-E) enclave for a network that is more secure and resilient by offering units multiple network communication pathways when faced with contested or congested communications environments.

The Army fielded ITN Capability Set 21 to the 1st, 2nd, and 3rd Brigade Combat Teams (BCTs), 82nd Airborne Division; 173rd Airborne Brigade; 2nd and 3rd BCTs, 25th Infantry Division; 2nd BCT, 11th Airborne Division; and a partial fielding to the 3rd Squadron, 2nd Cavalry Regiment. Capability Set 23 fielding is underway with the entire 2nd Cavalry Regiment and the 3rd Brigade Combat Team, 101st Division, with additional BCTs plus divisions as unit of action planned for the remainder FY23 and FY24.

**CAPABILITIES**

- Operates in both a Secret and SBU-E enclave to provide commanders with the flexibility to balance security and connectivity based on mission need:
  - Allows data to be categorized in accordance with its classification.
  - Provides the ability to securely transmit data to Army and Coalition forces in an unclassified environment
- Simplifies training, set-up, and employment of the network.
- Enables use of alternate transport including 4G/LTE.
- Interoperates with current network systems to enable mission command systems used in command posts and on platforms.



**A |** Soldiers with the 3rd Brigade Combat Team, 25th Infantry Division participate in their Bronco Rumble exercise in the Kahuka Training, HI, using the Integrated Tactical Network

**B |** The 2nd Cavalry Regiment (2CR) completed its annual Dragoon Ready exercise, which also served as the second ITN operational testing event (Ops Demo Phase II) for Capability Set 23. The 2CR is the first unit equipped to receive the ITN.

**C |** Soldiers with the 2nd Cavalry Regiment (2CR) demonstrate the ITN Variable Height Antenna, or tethered drone, which fitted with a single channel radio extends line of sight communications over environmental obstacles. The demonstration was part of the unit's annual Dragoon Ready exercise at the Joint Multinational Readiness Center in Hohenfels, Germany, and served as the backdrop to the second ITN operational testing event (Ops Demo Phase II) for Capability Set 23.



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**



# WAVEFORMS

A

Waveforms provides the warfighter with a suite of scalable and interoperable tactical waveforms and software products, enabling secure tactical communications, seamless networking, and real-time network management capabilities supporting the Army's tactical radio portfolio.



**DESCRIPTION**

Waveforms provides and sustains mobile and ad hoc networks, as well as network enterprise services to improve tactical warfighting capabilities. Waveforms enable Army tactical radio platforms to transmit voice and data securely across the battlespace. Products and services include multiple Army waveform modernization efforts such as Single Channel Ground and Airborne Radio System (SINGARS), which counters present and emerging Cyber Electromagnetic Activities (CEMA) threats; Warrior Robust Enhanced Network (WREN), which provides improved Electronic Warfare (EW) resilience based on current commercial waveform technologies; and the Advanced Network Waveforms (ANWf) operational analysis, which will provide future radio communication interoperability solutions for the DoD and partner nations incorporating ever increasing EW hardening and resilience features.

**CAPABILITIES**

**SINGARS:**

- SINGARS waveform is currently under a modernization effort as part of the NSA DoD Cryptographic Modernization Effort. It provides warfighting commanders and troops with a highly reliable and secure voice and data handling capability in support of Command-and-Control Operations.
- SINGARS is integrated in ground and aviation platforms including the HMS PRC-158 and PRC-162 MP; PRC 148 and PRC 163 LR, RT-1523 series, PRC-152 series, PRC-117 series, Air Ground Networking Radio, and the newly modernized Combat Net Radio.
- The new SINGARS waveform will include faster frequency hopping capabilities (FH2 and FH3) for use in mounted vehicle radios

and the portable Manpack radio to securely transmit data in contested environments.

**WREN:**

- WREN waveform network scalability increases communication range, reduces spectral footprint, and provides hardened EW protection.
- Supports VHF, UHF and L-Band frequency ranges using 50 kHz, 1.2 MHz, 3.6 MHz, and 10MHz+ Bandwidth.
- Provides simultaneous Position Location Information and voice services.
- Operates in two modes to address the Army's existing and future Integrated Tactical Network (ITN) networking challenges: WREN TSM – provides Spectrum Supportability, point to point range of 3-5km. WREN-NB – provides enhanced Electronic Protection and Spectrum Supportability, for operations in contested and congested environments up to ~15km.
- Adopts TSM BRn (Barrage Relay networking) for extended range and fast frequency hopping.
- WREN supports Type 1 Secret and Below and Sensitive But Unclassified security level interoperability.

**enterprise Over The Air Management (eOTAM):**

- eOTAM is an Application Programming Interface (API) framework and radio service that simplifies network management and enables secure over the air monitoring and remote re-provisioning.
- Features a standardized and secure protocol defined by the government to provide the ability to manage and monitor the Army's tactical radios securely and remotely.



**A | Soldiers with the 2nd Battalion, 501st Parachute Infantry Regiment, assigned to the 1st Brigade Combat Team, 82nd Airborne Division evaluate the AN/PRC-148C Leader radio and the AN/PRC-148D using the Warrior Robust Enhanced Network TSM waveform**

**B | In the future, Soldiers will conduct operations using upgraded waveforms to prepare for mid-to long-term threats, including the new SINGARS waveform, which will include enhancements to both electronic warfare protection and voice quality and WREN-Narrowband (NB), which enhances WREN TSM to extended communications, including air-to-ground, air-to-air and electronic warfare resiliency protection, and supports anti-jamming and low probability of intercept capabilities.**



**ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT**

UNIFIED NETWORK	COMMON OPERATING ENVIRONMENT	JOINT & COALITION INTEROPERABILITY	CP MOBILITY/SURVIVABILITY
-----------------	------------------------------	------------------------------------	---------------------------

# ACRONYMS

- A** Advanced Field Artillery Tactical Data System (AFATDS)  
Air to Ground Networking Information System (AGNIS)  
Air and Missile Defense Workstation (AMDWS)  
Army Key Management System (AKMS)  
Army National Guard (ARNG)  
Android Team Awareness Kit (ATAK)  
At The Halt (ATH)  
Automated Communications Engineering Software (ACES)
- B** Battle Command Common Services (BCCS)  
Communications, Command, and Control Leadership Board (C3LB)  
Battlefield Video Teleconference (BVTC)  
Beyond Line Of Sight (BLOS)  
Brigade Combat Team (BCT)  
Blue Force Tracker (BFT)
- C** Campus Wide Local Area Network (CWLAN)  
Capability Set (CS)  
Coalition Joint Spectrum Management Planning Tool (CJSMPT)  
Combat Camera (COMCAM)  
Combat Net Radio (CNR)  
Combat Survivor Evader Radio (CSEL)  
Combined Enterprise Regional Information Exchange (CENTRIX)  
Command and Control (C2)  
Command and Staff Palletized Airborne Node (CASPAN)  
Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR)  
Command Post Local Area Network (CP LAN)  
Command Post Computing Environment (CPCE)  
Command Post Display System (CPDS)  
Command Post Integrated Infrastructure (CPI2)  
Command Post Support Vehicle (CPSV)  
Commercial Coalition Equipment (CCE)  
Commercial Internet and Phone (COM-IP)  
Commercial-Off-The-Shelf (COTS)  
Commercial Solutions for Classified (CSfC)  
Common Access Card (CAC)  
Common Hardware Systems (CHS)  
Common Operating Environment (COE)  
Common Operational Picture (COP)  
Communications Security (COMSEC)  
Continental United States (CONUS)
- D** Defense Enterprise Computing Centers (DECC)  
Defense Information Systems Network (DISN)  
Defense Readiness Reporting System-Army (DRRS-A)  
Defensive Cyber Operations (DCO)  
Department of Defense (DoD)  
Dependent Airborne Node (DAN)  
Deployable Ku Band Earth Terminals (DKET)  
Developmental Operations (DevOps)  
Disaster Incident Response Emergency Communications Terminal (DIRECT)  
Distributed Common Ground System-Army (DCGS-A)  
Division Hub Node (DHN)
- E** Electronic Causality Report (ECR)  
Electronic Warfare (EW)  
Electronic Warfare Planning and Management Tool (EWPMT)  
Embedded Cryptographic Modernization Initiative (ECMI)  
End of Life (EOL)  
Enroute Mission Command (EMC)  
Enterprise Over The Air Management (eOTAM)  
Environmental control units (ECUs)  
Expeditionary Signal Battalion (ESB)  
Expeditionary Signal Battalion-Enhanced (ESB-E)  
Extended Range Cannon Artillery (ERCA)  
Extended Range Guided Multiple Launch Rocket System (ER-GMLRS)  
Extreme Data Rate (XDR)  
Extremely High Frequency (EHF)
- F** Fire Support Command and Control (FSC2)  
First Unit Equipped (FUE)  
Fiscal Year (FY)  
Fixed Installed Satellite Antenna (FISA)  
Forward Entry Devices (FED)  
Force XXI Battle Command Brigade and Below (FBCB2)  
Forward Observer System (FOS)
- G** General Fund Enterprise Business Systems (GFEBs)  
Global Agile Integrated Transport (GAIT)  
Global Broadcast Service (GBS)  
Global Combat Support System-Army (GCSS-Army)  
Global Information Grid (GIG)  
Global Rapid Response Information Package (GRRIP)  
Global Response Force (GRF)  
Government-Off-The-Shelf (GOTS)  
Gun Display Unit - Replacement (GDU-R)
- H** Hand Held (HH)  
Handheld, Manpack, and Small Form Fit (HMS)  
Helicopter and Multi Mission Radios (HAMMR)  
High-Altitude Electromagnetic Pulse (HEMP)  
High Capacity Line Of Sight (HCLOS)  
High Frequency (HF)  
High Mobility Multipurpose Wheeled Vehicle (HMMWV)
- I** Information Assurance (IA)  
Integrated Personnel and Pay System-Army (IPPS-A)  
Information Repository (IR)  
Integrated Support System (ISS)  
Integrated Tactical Network (ITN)  
Integrated Visual Augmentation System (IVAS)  
Integrated Tactical Networking Environment (ITNE)
- J** Joint Automated Deep Operations Coordination System (JADOCS)  
Joint Battle Command-Platform (JBC-P)  
Joint Enterprise Network Manager (JENM)  
Joint Forcible Entry (JFE)  
Joint Incident Site Communication Capability (JISCC)  
Joint Network Node (JNN)  
Joint Tactical Networking Center (JTNC)  
Joint Tactical Network Environment Network Operations Toolkit (J-TNT)
- K** Key Management Infrastructure (KMI)

- L** Lightweight Forward Entry Device (LFED)  
Line Of Sight (LOS)  
Local Area Networks (LANs)  
Long-Range Precision Fires (LRPF)  
Low Rate Initial Production (LRIP)
- M** Management Client (MGC)  
Manpack (MP)  
Medical Communication for combat Casualty Care (MC4)  
Military Information Support and Operation (MISO)  
Mission Command (MC)  
Mission Partner Environment (MPE)  
Mobile User Objective System (MUOS)  
Modular Communications Node - Advanced Enclave (MCN-AE)  
Modular Radio Architecture (MRA)  
Mounted Computing Environment (MCE)  
Mounted Family of Computer Systems (MFOCS)
- N** National Security Agency (NSA)  
Network Cross-Functional Team (N-CFT)  
Network Extension Packages (NEP)  
Network Integration Technology Enhancement (NITE)  
Network Operations (NetOps)  
NetOps and Security Center (NOSC)  
NOSC-Lite (NOSC-L)  
Next Generation Load Device (NGLD)  
Night Vision Device (NVD)
- O** On-The-Move (OTM)
- P** Point of Presence (PoP)  
Positioning, navigation, and timing (PNT)  
Precision-Fires Dismounted (PF-D)  
Precision Strike Missile Program (PrSM)  
Program Executive Office Command, Control and  
Communication-Tactical (PEO C3T)  
Program Management Office Network Enablers (PMO Net E)  
Project Manager Mission Command (PM MC)  
Project Manager Tactical Radios (PM TR)  
Project Manager Tactical Network (PM TN)  
Projectile Tracking System (PTS)  
Program of Record (PoR)
- R** Regional Hub Nodes (RHN)  
Remote Desktop Protocols (RDPs)  
Rifleman Radio (RR)  
Ruggedized Application Platform-Tactical Radio (RAP-TR)
- S** Satellite Broadcast Manager (SBM)  
Satellite Communications (SATCOM)  
Satellite Transportable Terminal (STT)  
Satellite Transportable Terminal Plus (STT+)  
Secure High Assurance Inline Encryption Link Device (SHIELD)  
Secure Internet Protocol Router (SIPR)  
Secure Internet Protocol Router Network (SIPRNET)  
Secure, Mobile, Anti-Jam, Reliable, Tactical - Terminal (SMART-T)  
Signal Operating Instructions (SOI)  
Single Channel Ground Airborne Radio System (SINCGARS)  
Simple Key Loader (SKL)  
SIPR/NIPR Access Points (SNAP)  
Situational Awareness (SA)  
Software Communications Architecture (SCA)  
Software Development Kit (SDK)  
Soldier Network Extension (SNE)  
Soldier Radio Waveform (SRW)  
Size, Weight and Power (SWaP)  
Special Purpose Integrated Remote Intelligence Terminal (SPIRIT)  
Special Operations Command (SOCOM)  
Standard Tactical Entry Point (STEP)  
Super High Frequency (SHF)  
Sustainment Tactical Network (STN)  
Systems Planning Engineering and Evaluation Device (SPEED)
- T** Tactical Communications Marketplace (TCM)  
Tactical Communication Node (TCN)  
Tactical Command Post (TAC)  
Tactical Communication Node-Lite (TCN-L)  
Tactical Defensive (Cyber Operations) Infrastructure (TDI)  
Tactical Digital Media (TDM)  
Tactical Hub Node (THN)  
Tactical Internet (TI)  
Tactical Mission Command (TMC)  
Tactical Network Initialization & Configuration (TNIC)  
Tactical Operation Center (TOC)  
Tactical Radio Report (TRR)  
Tactical Server Infrastructure (TSI)  
Transportable Tactical Command Communications (T2C2)  
Tactical Theater Signal Brigade (TTSB)  
Tri-band Line of Sight (TRILOS)  
Tobyhanna Army Depot (TYAD)  
Troposcatter Transmission (TROPO)
- U** Ultra High Frequency (UHF)  
Unified Network Operations (UNO)  
Unified Trouble Ticketing System (UTTS)  
Unit Reference File (URN)  
Unit Task Organization (UTO)  
Unit Task Reorganization (UTR)  
United States Message Text Format (USMTF)  
Unmanned Aircraft System (UAS)
- V** Variable Message Format (VMF)  
Vehicle Integration for C4ISR/EW Interoperability (VICTORY)  
Vehicle Wireless Package (VWP)  
Very Small Aperture Terminal (VSAT)  
Voice over Internet Protocol (VoIP)
- W** Wideband Global SATCOM (WGS)  
Wideband Networking Waveform (WNW)  
Warfighter Information Network-Tactical (WIN-T)  
Warfighter Initialization Tool (WIT)



# FOR MORE INFORMATION

PUBLIC SITE: [HTTP://PEOC3T.ARMY.MIL](http://peoc3t.army.mil)

FACEBOOK: [HTTP://WWW.FACEBOOK.COM/PEOC3T](http://www.facebook.com/peoc3t)

TWITTER: [HTTP://TWITTER.COM/PEOC3T](http://twitter.com/peoc3t)

FLICKR: [HTTPS://WWW.FLICKR.COM/PHOTOS/PEOC3TMEDIA](https://www.flickr.com/photos/peoc3tmedia)

LINKEDIN: [HTTPS://WWW.LINKEDIN.COM/COMPANY/PEOC3T](https://www.linkedin.com/company/peoc3t)

**PEOC3T**

PROGRAM EXECUTIVE OFFICE COMMAND CONTROL COMMUNICATIONS-TACTICAL



Approved for public release; distribution is unlimited. March 2023