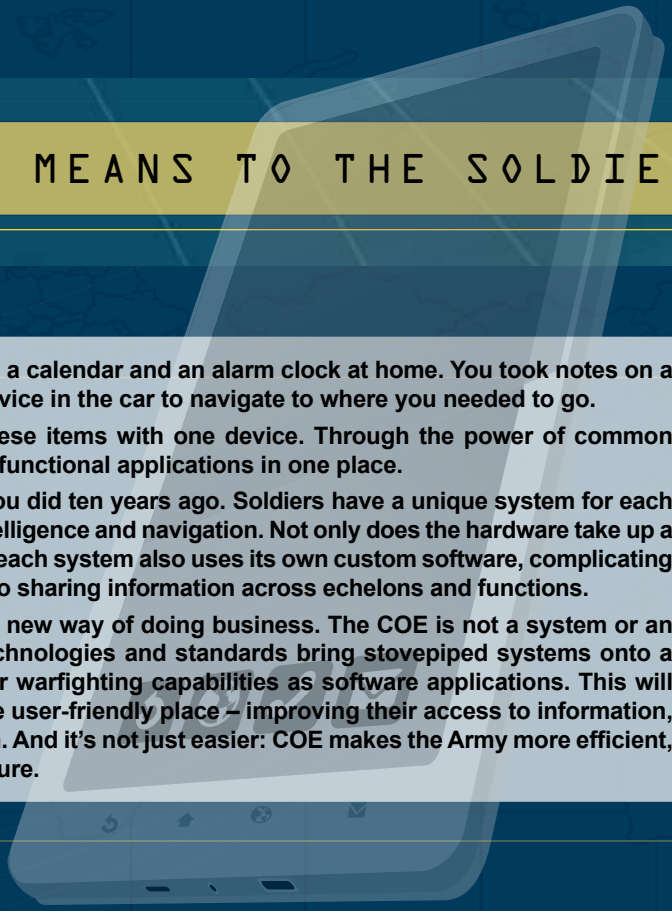
COMMON OPERATING ENVIRONMENT

U.S.ARMY

COE

COE: WHAT IT MEANS TO THE SOLDIER



Ten years ago, chances are you had a calculator, a calendar and an alarm clock at home. You took notes on a piece of paper and used a road map or a GPS device in the car to navigate to where you needed to go.

Today, chances are you have replaced all of these items with one device. Through the power of common software, your smartphone combines dozens of functional applications in one place.

The Army, however, is still doing business like you did ten years ago. Soldiers have a unique system for each warfighting function, such as fires, maneuver, intelligence and navigation. Not only does the hardware take up a lot of space inside vehicles and command posts, each system also uses its own custom software, complicating updates and training. It also creates roadblocks to sharing information across echelons and functions.

The Common Operating Environment (COE) is a new way of doing business. The COE is not a system or an acquisition Program of Record. Rather, COE technologies and standards bring stovepiped systems onto a common foundation to allow the Army to deliver warfighting capabilities as software applications. This will provide Soldiers with a vast range of tools in one user-friendly place – improving their access to information, while reducing their training and logistics burden. And it's not just easier: COE makes the Army more efficient, more operationally effective and more cyber secure.

> WHY COE?

The COE represents a paradigm shift in how Army systems are built and deployed. Following commercial best practices, the COE establishes a common foundation of shared components across key systems, which will make them interoperable "out of the box" rather than today's model of leaving the integration for last. The COE puts integration first, ensuring Soldiers can share information across systems and echelons to get the right data at the right place at the right time. It also increases efficiencies by eliminating duplication in development, operations and sustainment.

Like a commercial smartphone's operating system, the COE's common framework will also allow the Army to quickly adopt new applications as they are created by government, industry or other sources – improving our ability to respond to changing technologies and operational needs. Finally, the COE increases security by building on a standardized, cyber hardened data foundation.

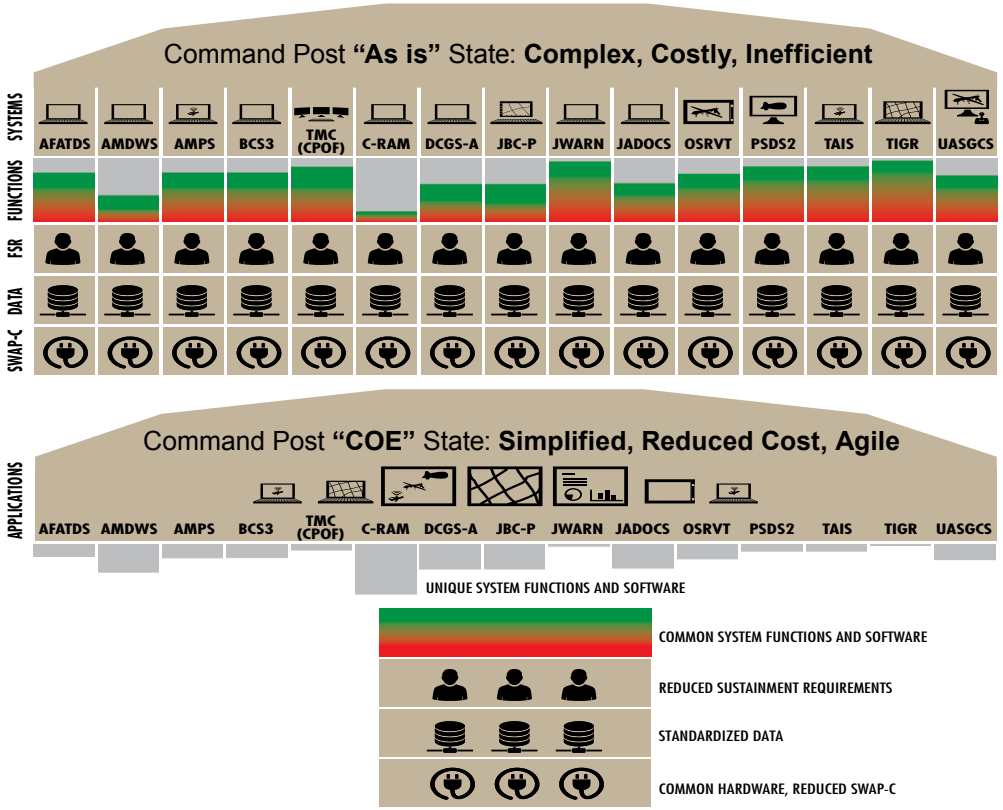
The Army is delivering the COE through an incremental approach, based on operational needs and Soldier priorities for common functions such as chat and maps. We are fielding COE compliant systems now, and we are on track to deliver an enhanced version by Fiscal Year 2019 as part of the Army's Mission Command Network of 2020.

> COE: ENABLING THE ARMY OPERATING CONCEPT

The Army Operating Concept, "Win in a Complex World," envisions an expeditionary, agile force ready to be task-organized and deployed on short notice to austere locations, and capable of conducting operations immediately upon arrival. But today's complex, hardware-dense assortment of information systems slows and weighs us down. The COE aims to change that by bringing tactical capabilities closer to what users experience with their integrated, lightweight commercial devices.

The COE requires the Army to invest in improved infrastructure, including common software and high-performing servers that can do the work previously performed by multiple stovepiped machines. But these up-front investments are what enable us to implement the new, more efficient way of doing business: a smaller hardware footprint, where stovepiped mission command systems are replaced by integrated web applications. These apps will share the same map engine, chat function, and secure underlying data, which will enhance staff collaboration and increase operational agility.

The COE also streamlines interactions with coalition partners – a core element of expeditionary operations and the Army Operating Concept. The COE will improve the Army's ability to efficiently label data and share information, thus preserving cybersecurity while reducing manual obstacles to collaboration with other nations and agencies.



The Army is following the commercial model to deliver powerful capability through software

WARFIGHTING APPS/WIDGETS

Percentage of Unique Functions

*Percentage of Common Functions**

**Not required in Apps*

> COE: STRENGTHENING CYBER SECURITY

The Army's increasingly mature networked communications systems provide the commander and troops a dominating view of the battlefield. But as the Army adds more capability to the network, it creates additional vulnerabilities for cyber threats.

The COE enables the Army to better prevent, respond to and recover from cyber attacks. COE shrinks the number of network access points to reduce vulnerability, closes the seams between systems, and improves visibility across the enterprise and tactical networks for a common operating picture that can detect intrusion.

Cyber threats must be countered in hours or days, rather than in months or years. COE allows the Army to move at the speed of cyberspace. When a security patch is needed, Soldiers will no longer have to manually install it using a CD for each system. Instead, they can receive it over the network and it will apply to all systems – just as you would download a software update on your smartphone.


TILLERY

> COE: APPLYING BETTER BUYING POWER

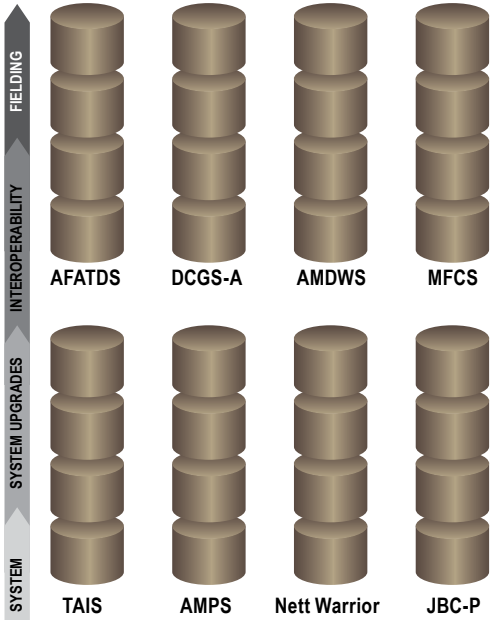
The COE allows the Army to achieve Better Buying Power (BBP) by significantly reducing system life cycle costs through up-front integration and efficient sustainment.

Under the current Software Blocking process, Army information technology systems are developed individually and integrated at a test facility after the fact. After fielding, when a program needs to upgrade hardware or software, a specialized team of Field Service Representatives (FSRs) is sent to the field to execute the update.

COE will transform this process by creating a baseline of standards, Software Development Kits (SDKs) and interfaces that engineers use to develop interoperable products from the beginning. Consistent with BBP's pursuit of a Modular Open Systems Architecture (MOSA), this commonality will streamline testing and certification, and will allow the Army to deploy updates across many systems at the same time, saving money in unique part replacements and specialized FSRs.

To encourage competition – another key goal of BBP – the COE provides SDKs enabling industry and other third parties to contribute new tactical applications to the standard baseline.

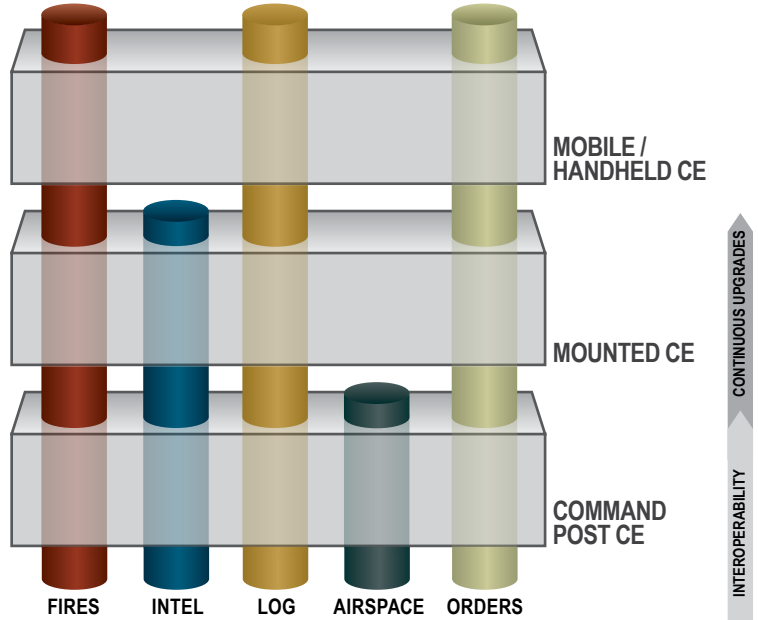
SOFTWARE BLOCKING (SWB) SYSTEMS BASED



- Stovepiped systems developed independently
- Each system fielded and updated at different times
- Integration difficult, costly and time-consuming

VS

COMMON OPERATING ENVIRONMENT (COE) INFRASTRUCTURE BASED



- Common infrastructure replaces stovepipes
- Apps and widgets integrated "out of the box"
- Streamlined test, certification and fielding

> COE: EVOLVING OVER TIME

Smartphone technology evolves rapidly and reaches customers continuously. Manufacturers regularly release new hardware and software updates, while users can download new applications as they become available on the web.

The Army is doing the same with the COE. We are following an incremental fielding strategy, based on operational needs and available resources, to continuously and progressively deliver COE across the force. Like a commercial software release, these incremental improvements in functionality are described as "versions" of the COE baseline. They also incorporate ongoing updates to the Computing Environments (CEs) that comprise the COE.

The COE fielding plan is designed to meet user demands for interoperability while synchronizing capability delivery with unit schedules and training. It accounts for the need to simultaneously sustain legacy PoR systems, field updated COE-compliant capabilities, and develop the next generation COE technologies for release.

KEY WARFIGHTING APPS

Joint C2 Content Manager

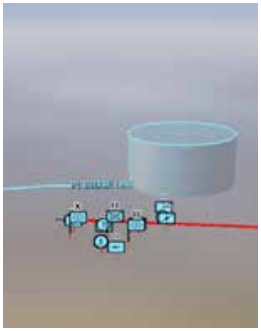
Allows Soldiers to identify, discover, retrieve and manage a customized Common Operating Picture. Accesses, filters and integrates data from Joint and Coalition sources.

Engineer Obstacles & Hazards

Allows Soldiers to input obstacles and hazards and display them on a map. Enables the user to create, receive, analyze and disseminate obstacle and hazard information to affected units.

JBC-P TiGR

Allows Soldiers to enter and display historical data including Areas, Structures, Capabilities, Organizations, People, and Events (ASCOPE) information, enabling commanders to plan, anticipate and mitigate operational risk.



Fires Command Web

Allows Soldiers to access AFATDS data and prosecute fiire missions on Command Web. Users can view and edit friendly and enemy unit data, target lists, air support requests and fires graphics.

Maneuver

Allows Soldiers to manage maneuver planning and collaboration. Enables users to create work products (overlays, graphics, etc.), collaborate on those products with others, and publish the resulting products to various formats.

"To put it simply, I have less stuff to carry and everything I need at my fingertips."

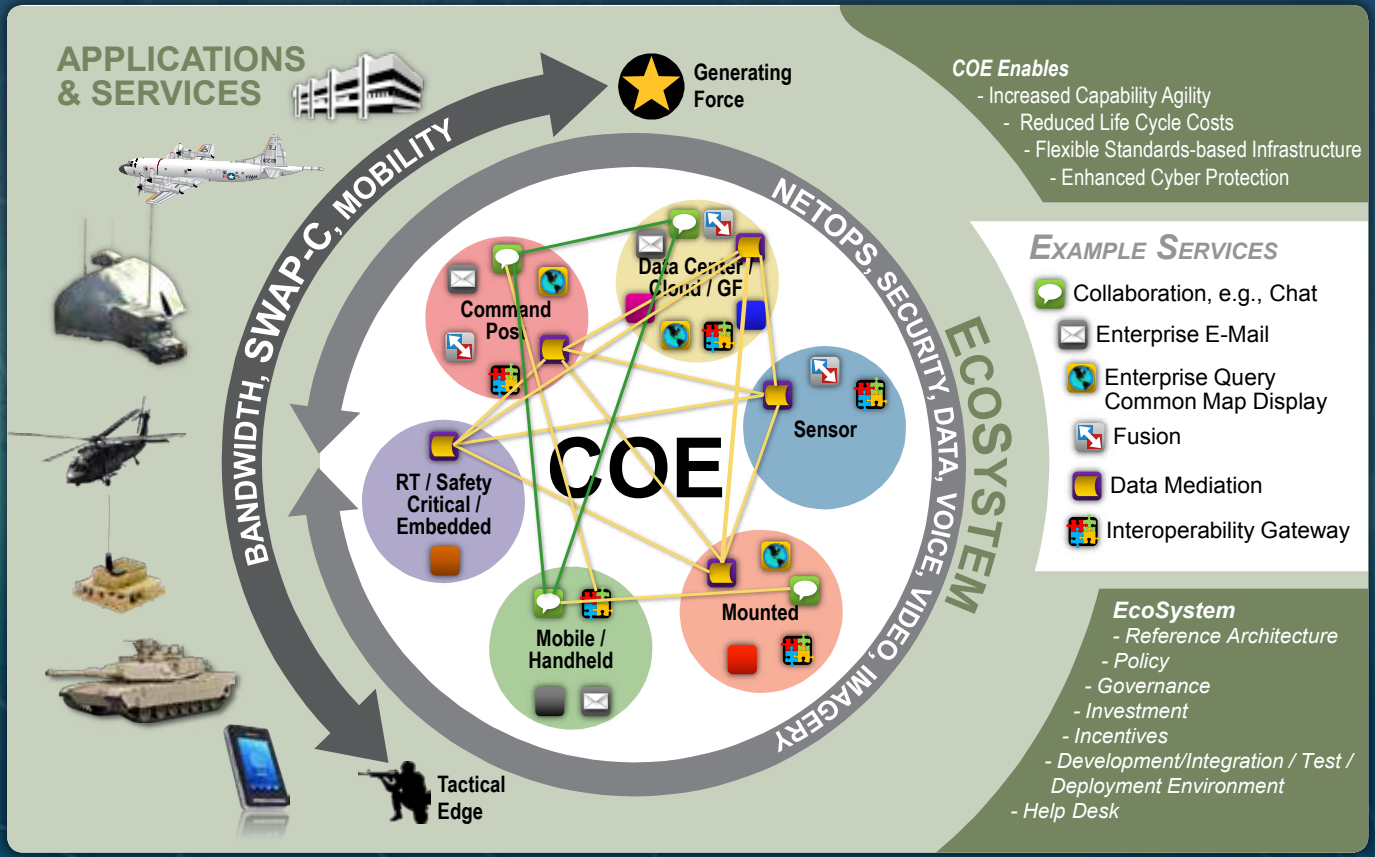
"On the move I have warfighting functions communicating accurate situational awareness that is always connected to the Command Post."

> COE: A FAMILY OF CEs

For effective management, the COE has been sorted into six Computing Environments (CEs): Command Post, Mounted, Mobile/Handheld, Data Center/Cloud/Generating Force, Sensor, and Real-Time/Safety Critical/ Embedded CEs. Assigned to program offices across the Army acquisition community, the CEs will interoperate with each other using control point specifications.

CEs are not mutually exclusive but instead work together and share the standards-based infrastructure to drive operational costs down. The COE identifies cross-cutting capabilities used by many systems, such as geospatial visualization and secure authentication, and delivers a common software baseline used by all of the CEs. The CEs are also developed in versions, which are fielded as part of the incremental updates to COE.

Together, the CEs will bring a plug-and-play experience across the force, meeting the needs of today's tech-savvy Soldiers who have grown up with technology and expect intuitive devices that are interoperable whether in a command post, vehicle, aircraft or on foot.


APPLICATIONS & SERVICES
Generating Force
BANDWIDTH, SWAP-C, MOBILITY
NETOPS, SECURITY, DATA, VOICE, VIDEO, IMAGERY
ECOSYSTEM
Command Post
Data Center / Cloud / GF
Sensor
COE
RT / Safety Critical / Embedded
Mobile / Handheld
Mounted
Tactical Edge
COE Enables
- Increased Capability Agility
- Reduced Life Cycle Costs
- Flexible Standards-based Infrastructure
- Enhanced Cyber Protection
EXAMPLE SERVICES
Collaboration, e.g., Chat
Enterprise E-Mail
Enterprise Query
Common Map Display
Fusion
Data Mediation
Interoperability Gateway
EcoSystem
- Reference Architecture
- Policy
- Governance
- Investment
- Incentives
- Development/Integration / Test / Deployment Environment
- Help Desk

COMMAND POST COMPUTING ENVIRONMENT (CP CE)

FIELDING NOW

The CP CE transforms the command post by consolidating the capabilities for missions related to fires, logistics, intelligence, airspace management and maneuver into a single, intuitive environment. The Common Services layer is the true power within CP CE, enabling a significant reduction in unique system hardware and software by leveraging integrated maps, chat and other services.

The CP CE will enable the Army to develop and field interoperable applications through a web-based marketplace. Using any government-authorized laptop connected to the appropriate classified network, operational commanders and staff can log into the marketplace, called the Ozone widget framework, to access these apps.

CP CE gives commanders a consolidated warfighting picture on a singular workstation, enhancing their ability to make rapid adjustments according to the combat situation and act decisively to achieve their mission. It also lessens the logistics trail, reduces the training burden and saves taxpayer dollars.

> MOUNTED COMPUTING ENVIRONMENT (MCE)

FIELDING NOW

The MCE sets the standard for mounted mission command on-the-move to deliver Android-based warfighting apps inside Army tactical vehicles. Based on the Joint Battle Command-Platform (JBC-P) system, MCE features a Google Earth-like interface and real-time chat rooms. With MCE, Soldiers can quickly zoom in to view precise locations, use icons to pinpoint improvised explosive devices on a map, and use instant messaging to call for medics.

Part of the MCE implementation is the Mounted Android Computing Environment (MACE), a secure framework that enables government and industry partners to build capabilities to the well-known Android ecosystem. This makes the apps easier for Soldiers to use and for developers to build. Applications only need to be developed once, and then will work seamlessly across handhelds, radios, tactical vehicles and the command post.

MCE is delivered on next generation tactical computers called the Mounted Family of Computer Systems (MFoCS), which collapses multiple mission command functions onto one screen to save space inside Army vehicles. MFoCS provides Soldiers with a range of computing options from a full vehicle-mounted workstation to a removable tactical tablet.

FIELDING NOW

The foundation of the M/HH CE is Nett Warrior, the Army's handheld mission command system that enables digital communications for dismounted leaders down to the team level. Nett Warrior is based on an Android commercial smartphone that has been adapted for military security standards and linked to the Army tactical network through the Rifleman Radio. By using a low-cost, commercially available platform and the Android software development environment, the M/HH CE delivers a secure product that Soldiers are already familiar with, reducing the training burden.

As with the CP CE and MCE, the Nett Warrior program office has published a Software Development Kit that allows other organizations to develop applications that are interoperable with COE standards. Many of these apps replace previous standalone systems. Recently developed apps for fielding on Nett Warrior devices include mobile handheld fires, machine foreign language translation, tactical combat casualty care and counterintelligence/human intelligence reporting.

The M/HH CE has collaborated extensively with the MCE to implement common messaging formats and mapping standards, ensuring that mounted and dismounted Soldiers see the same common operating picture and can exchange critical combat information like calls for Medevac, reports of sniper fire and friendly and enemy locations.


209
SMITH
U.S. ARMY
U.S. ARMY

DATA CENTER/CLOUD/GENERATING FORCE CE

The Data Center/Cloud/Generating Force CE is essential to opening doors between the Army's strategic/enterprise network and the operational network. It delivers a cloud-enabled computing infrastructure with shared network, server and storage resources, as well as a path to migrate existing applications to the cloud. Through a service-based infrastructure and common Software Development Kit, it enables a "marketplace" approach for hosting and accessing Army software applications, services and data.

Housing data in the cloud allows the Army to increase its collaborative reach across organizations, echelons and locations. This enhanced interoperability will provide deployed forces with reach-back connectivity to sanctuary locations for analysis and information products that in the past were available solely at the strategic level. It further reduces the need for on-site equipment and allows units to function as a more unified force when conducting dispersed operations. Integrating the strategic and tactical components of the network also enables distributed and realistic training as doctrine and standard operating procedures evolve, increasing readiness for potential short-notice deployments.

> SENSOR CE

The Sensor CE focuses on improving the interaction of sensors with Soldiers, platforms, and command post systems across all warfighting functions. As sensors continue to proliferate as a valuable information source across the battlespace, the Sensor CE delivers a common interoperability layer, implementing standards and technology for data services, Network Operations, and security for specialized, human-controlled and unattended sensors.

These standards will provide Soldiers with a "common vocabulary" across platforms and echelons when transmitting and using sensor information. The Sensor CE also includes a sensor service framework that will enable users to discover sensor data across the Army enterprise, register a sensor's location and capabilities, and securely manage sensors and sensor systems.

REAL-TIME/SAFETY CRITICAL/EMBEDDED CE

Unlike the other CEs, the primary goal of the Real-Time/Safety Critical/Embedded CE is not to develop hardware or software, but rather to develop a framework of standards and an ecosystem that lay the foundation for integrating future applications into Army platforms. It aims to improve upon the Army's previous "bolt-on" approach to fielding equipment on vehicles and aircraft, which often led to duplication and expensive integration efforts.

The key enablers of this CE are Vehicular Integration for C4ISR/EW Interoperability (VICTORY), Future Airborne Capability Environment (FACE), the Ordnance Interface Standard (OIS), and Engagement Operations (EO). Implementing the RT/SC/E CE means that Soldiers will find more common sets of devices, displays, and information in a wider range of platforms, ultimately making Soldiers and formations more connected, aware, and capable.

> COE: EXECUTION AND PATH AHEAD

The good news is a lot of work on the COE front has already been done. COE compliant systems such as Nett Warrior (Mobile/Handheld CE) and Joint Battle Command-Platform (Mounted CE) are already in the hands of Soldiers. The Command Post CP CE has delivered the initial convergence of operations and intelligence hardware, transitioned several standalone mission command system "boxes" to integrated software applications, and collapsed 13 separate maps down to six.

Soldiers have evaluated these improvements through several Network Integration Evaluations (NIEs), and the COE version 1 baseline is preparing for Army Interoperability Certification. As other capabilities mature, they will be evaluated at NIE and fielded incrementally as updates to COE version 1. The Army is on track to deliver the enhanced COE version 3 by Fiscal Year 2019 – when Soldiers will see the full power of COE to transform information-sharing from handhelds to the tactical cloud.

COE is based on commercial best practices, and the Army will continue to engage with industry as we deploy COE to the field. Software Development Kits are in place for several CEs, and the Army is driving forward to deliver these kits to third party developers, which will allow industry partners to create apps as needed to meet evolving missions. The COE is a better way of doing business that will provide our Soldiers the advanced, integrated capabilities they need to Win in a Complex World.

ACRONYM KEY

AFATDS: Advanced Field Artillery Tactical Data System

AMDWS: Air and Missile Defense Workstation

AMPS: Aviation Mission Planning System

BCS3: Battle Command Sustainment Support System

C4ISR / EW: : Command, Control, Communication, Computers, Intelligence, Surveillance, Reconnaissance/ Electronic Warfare

CPOF: Command Post of the Future

C-RAM: Counter-Rocket, Artillery, Mortar

DCGS-A: Distributed Common Ground System-Army

FSR: Field Service Representative

JBC-P: Joint Battle Command-Platform

JWARN: Joint Warning and Reporting Network

JADOCS: Joint Automated Deep Operations Coordination System

MFCS: Mortar Fire Control System

OSRVT: One System Remote Video Terminal

PSDS2: Persistent Surveillance and Dissemination System of Systems

SWAP-C: Size, Weight & Power-Cooling

TAIS - Tactical Airspace Integration System

TIGR: Tactical Ground Reporting

TMC: Tactical Mission Command

UASGCS: Unmanned Aircraft System Ground Control Station

HTTP://WWW.ARMY.MIL/ASAALT
HTTP://BBP.DAU.MIL/
HTTP://VICTORY-STANDARDS.ORG/
HTTP://WWW.ARCIC.ARMY.MIL/CONCEPTS/OPERATING.ASPX
HTTPS://SPCS3.KC.ARMY.MIL/SOSEI/COE/ [CAC ACCESS]