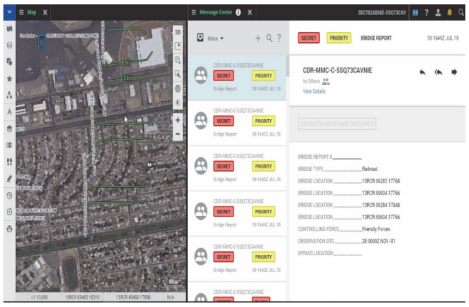
Command Post Computing Environment (CPCE)

Executive Summary

- In November 2018, the Army conducted a Command Post Computing Environment (CPCE) IOT&E to support a planned CPCE fielding decision. The CPCE IOT&E consisted of a division headquarters element and a brigade conducting operationally realistic missions at Fort Bliss, Texas, and White Sands Missile Range, New Mexico.

Tactical Server Infrastructure (TSI) Version 2.0 - Small


Mission Command Information System (MCIS) Software


Tactical Server Infrastructure (TSI) Version 2.0 - Large

- In June 2019, DOT&E published a CPCE IOT&E report that assessed CPCE as:
  - Not operationally effective. Soldiers viewed the concept of CPCE as an improvement over existing systems, but stated the system requires more development prior to fielding. CPCE did not support leaders and soldiers with sufficient scalability, collaboration, or operations management to support the mission command needs of a combat force.
  - Not operationally suitable. Soldiers viewed simple CPCE tasks as intuitive, but stated that more complex tasks were cumbersome and difficult to accomplish. Training afforded soldiers did not allow them to maintain the system, which increased the need for contract field service representatives.
  - Not survivable in a cyber-contested environment. CPCE has cybersecurity vulnerabilities that reduce mission success.
- In July 2019, the Army approved a conditional full deployment of CPCE to two divisions, two brigades, and units deploying to exercise Defender 2020. The authorization stated that conditions would be removed from full deployment upon the program demonstrating resolution to key CPCE deficiencies. The conditional full deployment directs the conduct of a developmental test to verify correction of deficiencies and assess software improvements.
- The program updated the CPCE Test and Evaluation Master Plan (TEMP) to provide a testing strategy for future increments of CPCE.

System

- CPCE is a server-based software system that provides mission command applications to support commanders and staff using general-purpose client computers, located within Tactical Operations Centers. CPCE provides soldiers a common operating picture, shared situational awareness, collaboration tools, and messaging.
- The Army developed CPCE as an evolution of existing, stove-piped mission command systems to a common, shared client-server architecture. The Army designed CPCE version 3.0 to replace and integrate the capabilities of the following existing mission command systems:
  - Command Post of the Future
  - Tactical Ground Reporting System
  - Command Web
  - Global Command and Control System – Army
- CPCE version 3.0 provides basic mission command applications required by tactical command posts as part of the Army's Common Operating Environment (COE). The Army designed CPCE to interface with other developing COE Computing Environments (CEs), and to interoperate with joint, allied, and coalition forces.

Mission

The Army intends for commanders and staff at battalion through corps level to use CPCE to conduct mission command throughout all phases of the Army operations process, to include planning, preparation, execution, and continuous assessment of unit missions. As COE CEs are developed, units will use CPCE as a collection point for data from sensors, aviation, logistics, fires, intelligence, and safety information, including mounted, dismounted, and home station command units.

Major Contractors

- Weapons Software Engineering Center – Picatinny Arsenal, New Jersey
- Systematic USA/Systematic AS – Centreville, Virginia/ Aarhus, Denmark

Activity

- The Army began this program in FY16, and DOT&E put it on oversight in FY17. This is the first time DOT&E has included this program in its annual report.
- In November 2018, the Army conducted the CPCE IOT&E as part of the Network Integration Evaluation 18.2. The test employed a division headquarters element, and the 3rd Infantry Brigade Combat Team, 82nd Airborne Division conducting operationally realistic missions at Fort Bliss, Texas, and White Sands Missile Range, New Mexico. The 1st Battalion, 508th Infantry Regiment augmented with electronic warfare and cyber capabilities served as a realistic opposing force. The Army conducted the IOT&E in accordance with a DOT&E-approved operational test plan.
- The Army included CPCE in Warfighter Exercises 19.3 and 19.4, and the Joint Warfighting Assessment (JWA) 19.1 at Joint Base Lewis-McChord, Washington, to gain observation and survey data on the system's performance. The Army's focus for JWA 19.1 was to assess CPCE joint and coalition interoperability, and demonstrate software improvements.
- In June 2019, DOT&E published a CPCE IOT&E report to support the Program Executive Office, Command Control Communications – Tactical (as designated Milestone Decision Authority) CPCE full deployment decision (FDD).
- In July 2019, the Army published an Acquisition Decision Memorandum (ADM) authorizing conditional full deployment of CPCE to two divisions, two brigades, and units participating in exercise Defender 2020. The ADM establishes conditions to allow further fielding of CPCE upon the program demonstrating resolution of key CPCE deficiencies.
- As directed in the FDD ADM, the Army is planning a laboratory-based CPCE developmental test with input from DOT&E. This test is planned for 1QFY20, and is intended to verify correction of CPCE IOT&E deficiencies and assess software improvements.
- The program updated the CPCE TEMP to provide a test strategy for planned functions being developed for future increments of CPCE, such as fire support and intelligence.
- In February 2020, the Army plans to conduct a CPCE Maintenance and Logistics Demonstration to assess system maintainability.

Assessment

- In the June 2019 CPCE IOT&E report, DOT&E assessed CPCE as:
  - Not operationally effective. Soldiers viewed the concept of CPCE as an improvement over existing systems, but stated the system requires more development prior to fielding. CPCE did not support leaders and soldiers with sufficient scalability, collaboration, or operations management to support the mission command needs of a combat force. Soldiers experienced, and data instrumentation confirmed, that mission relevant data were delayed in delivery and not correct. Soldiers resorted to alternative means to conduct portions of unit mission operations.
  - Not operationally suitable. Soldiers viewed simple CPCE tasks as intuitive (e.g. sending messages or conducting chat), but stated that more complex tasks (e.g. grouping units or preparing missions) were cumbersome and difficult to accomplish. Soldiers experienced loss of functions or complete CPCE capability, which hindered mission operations. Training afforded system administrators and maintainers did not allow them to maintain the system, which increased the need for contract field service representatives.
  - Not survivable in a cyber-contested environment. CPCE has cybersecurity vulnerabilities that reduce mission success.
- CPCE IOT&E effectiveness and suitability ratings were based upon a complete set of test data, manual and instrumented. DOT&E used the official test database as delivered by Army Test and Evaluation Command (ATEC). These data included surveys, soldier commentary, system logs, video, video capture, and instrumented data. Assessments of effectiveness and suitability were based upon multiple sources of data, both manual and instrumented. The Army collected instrumented data using software and processes validated by an ATEC-approved Test Technology Accreditation memorandum. DOT&E made far greater use of the instrumented data in its evaluation and many of these areas were not assessed by the Army. To ensure accuracy of the final report, DOT&E prepared an emerging results brief 3 months prior to the Army's FDD and met with the Army on 15 occasions to discuss findings, review data, and consider modifications to the DOT&E assessment.
- The JWA 19.1 did not provide sufficient data to assess joint and coalition interoperability. The event provided observation data of transfer of digital data, but did not provide instrumented data or useful survey data. The Army is working to improve JWA 20 to provide improved CPCE data.
- Soldier observations during the Warfighter Exercises indicated problems with CPCE collaboration and commander's briefings for corps mission operations.
- The Army has asserted correction of numerous CPCE IOT&E deficiencies. The program is providing sufficient resources to conduct a 1QFY20 CPCE developmental test to verify fixes and assess software enhancements. Once the assessment of the developmental test is complete, it should provide the opportunity to verify CPCE fixes made since the IOT&E.

Recommendations

The Army should:

1. Improve CPCE hardware and software to address IOT&E deficiencies, and verify corrections in future testing.
2. Improve CPCE cybersecurity and assess survivability in future testing.
3. Demonstrate joint and coalition interoperability.
4. Improve CPCE training to improve maintainability and decrease reliance upon contract field service representatives.