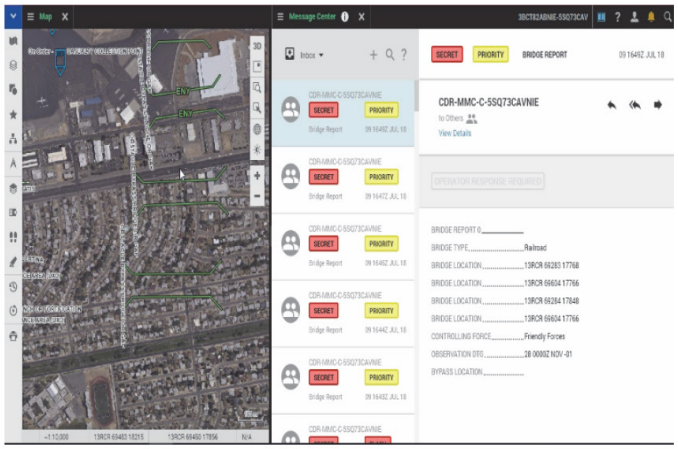
Command Post Computing Environment/ Tactical Server Infrastructure (CPCE/TSI)



In FY24, the Army conducted an operational cooperative vulnerability and penetration assessment and adversarial assessment (AA) of the Command Post Computing Environment/Tactical Server Infrastructure (CPCE/TSI). CPCE/TSI is cyber survivable when employed with trained Army cyber defense soldiers using integrated cyber defense tools. In July 2024, DOT&E published a classified CPCE cyber survivability report that finds the Increment 2 performed the same against nearsiders and outsiders compared to CPCE Increment 1. The Army continues to adopt an Agile development process for the program based on feedback from unit exercises.

SYSTEM DESCRIPTION

CPCE is a server-based software system that provides server hardware and mission command software to support commanders and staff using general-purpose client computers, located within battalion through corps Tactical Operations Centers. The Increment 2 builds upon the previously tested Increment 1 and Increment 0 capabilities. The software provides a common operational picture, a suite of web-based collaboration tools and messaging capabilities to facilitate the commander and staff to plan, prepare, execute, and assess Army operations.

The CPCE software and applications reside on TSI hardware and previously fielded Battle Command Computing Services servers at tactical echelons that span from Army Service component commands to battalion level. TSI provides the command post foundational infrastructure consisting of server hardware, computing power and storage, and applicable server software required to support Mission Command Systems.

In addition to the software, TSI also integrates and hosts the enterprise services that are required to provide mission command capability to units.

MISSION

The Army intends for commanders and staff at battalion through corps levels to use CPCE to conduct mission command throughout all four phases of the Army operations process, to include planning, preparation, execution, and continuous assessment of unit missions. As the Army further develops its Common Operating Environment, commanders and staff 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.

PROGRAM

CPCE is an Acquisition Category II major capability acquisition pathway program. A full deployment decision for Increment 1 occurred December 2021. DOT&E published an FOT&E report to support this decision. The program office developed an updated TEMP, which DOT&E approved in January 2023. The Army restructured the program in October 2023 to move to a more Agile software approach instead of pursuing a full deployment decision. This resulted in a down-scope of the original follow-on operational test to focus on the cyber portion of the software to support a software release. DOT&E published a classified CPCE cyber survivability report in July 2024. The Army is still refining the details of the Agile software approach into formal acquisition strategies.

» MAJOR CONTRACTORS

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

TEST ADEQUACY

The Army conducted a cooperative vulnerability and penetration assessment in February 2024, and an AA in March 2024, at Schofield Barracks, Hawaii. DOT&E observed both tests. The cooperative vulnerability and penetration and AA test environments leveraged the network architecture environment developed by the 25th Infantry Division.

Testing was adequate to support an assessment of the cyber survivability of CPCE. DOT&E published a classified CPCE cyber survivability report that finds the Increment 2 performed the same against nearsiders and outsiders compared to CPCE Increment 1. Testing was conducted in accordance with the DOT&E-approved test plans, however, because this event fell under a unit's training exercise, the test objectives were lower priority. As a result of this, cyber testing captured limited mission effects that stemmed from cyber compromises.

If unit exercises will be used in the future, there should be a greater emphasis toward integrating test objectives within the unit's training objectives to ensure a more robust test. Due to the down-scope of the test to focus solely on cyber, there was no instrumentation required. As recommended in the FY22 Annual Report, the Army should complete the improvement of CPCE data instrumentation to support test adequacy and confidence in data collection for determining effectiveness and suitability during future developmental and operational tests and demonstrate instrumentation effectiveness in a CPCE test event.

The Army is also in the process of changing the operational mission for CPCE. In April 2024, the Army executed Operation Lethal Eagle at Fort Campbell, Kentucky; Fort Knox, Kentucky; and Camp Atterbury, Indiana, where the Army hoped to move the system complexity from the brigade up to the division and obtain key observations from the unit. These observations will impact many network and command and control systems beyond CPCE. While not a formal test, the Army is leveraging this exercise and a Joint Readiness Training Center rotation to inform future Army programs. The Army should codify this process formally going forward and develop a future TEMP to better inform acquisition decision making.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

In December 2021, DOT&E published a FOT&E Report that found CPCE Increment 1 operationally effective and not suitable due to reliability issues. FY24 testing did not support an additional assessment of operational effectiveness and suitability.

» SURVIVABILITY

CPCE Increment 2 is cyber survivable in a cyber-contested environment compared to the Increment 1. CPCE maintained a strong cybersecurity defense posture when employed with trained Army cyber defense soldiers using integrated cyber defense tools. The full description of CPCE cyber survivability against an operationally realistic cyber threat is detailed in the classified cyber survivability report published in July 2024.

RECOMMENDATIONS

The Army should:

1. Continue the improvement of CPCE data instrumentation to support test adequacy and confidence in data collection during future developmental and operational tests and demonstrate its effectiveness in a CPCE test event, as recommended in the FY22 Annual Report.
2. Ensure that any future test event that leverages a unit training exercises also prioritizes test objectives.
3. Codify future Army exercises and training events that will be used to support acquisition decisions within a TEMP and submit it to DOT&E for approval.