Joint Cyber Warfighting Architecture (JCWA)

The U.S. Cyber Command (USCYBERCOM) continues to refine internal processes, roles, and responsibilities as it stands up the Joint Cyber Warfighting Architecture (JCWA) Program Executive Office (PEO). Additionally, USCYBERCOM has established an offensive cyber operations hybrid program management office (PMO) to improve software development efficiencies among multiple critical JCWA components. In 4QFY25, DOT&E approved the T&E Strategy, which represents a coordinated effort to secure the resources required to verify JCWA's ability to successfully enable global resilient cyber operations. No JCWA-level operational testing was conducted in FY25, and individual components continued to field capability following limited operational testing, with most testing focused on cyber resilience.

SYSTEM DESCRIPTION

JCWA is USCYBERCOM's planned system-of-systems architecture that will provide an integrated suite of cyber capabilities and tools to the Cyber Mission Force for rehearsing and conducting offensive and defensive cyber operations. This system of systems is designed to collect, fuse, and process cyber data and intelligence to provide cyber forces with situational awareness and battle management at the strategic, operational, and tactical levels.

JCWA's new capabilities are intended to be adaptable to joint mission needs, operating environments, and evolving threats and technologies. Currently, JCWA includes six foundational components: Unified Platform (UP), Joint Cyber Command and Control (JCC2), Persistent Cyber Training Environment (PCTE), Joint Common Access Platform (JCAP), tools, and sensors.

MISSION

USCYBERCOM intends to use JCWA to support all cyberspace operations, training, tool development, data analytics, and coordinated intelligence functions.

PROGRAM

JCWA is not a program of record but encompasses the following software acquisition pathway programs:

- UP is a cloud-based set of applications, services, and resources that enable full-spectrum cyberspace operations by integrating USCYBERCOM cyber capabilities and systems. It operates and maintains the Big Data Platform for USCYBERCOM and Service components. UP is a software acquisition program.

- JCC2 is a portfolio of integrated products that provide situational awareness, battle management, and cyber force management for full-spectrum cyber operations.
- PCTE provides a standardized training platform for individuals and teams of cyberspace operators to maintain readiness and rehearse missions for cyber operations. PCTE is an Acquisition Category II program.
- JCAP provides infrastructure for USCYBERCOM and the Services to coordinate and execute cyber operations. JCAP is a software acquisition program.
- Other projects and methodologies are used to develop and deploy tools and sensors to cyber forces.

» MAJOR CONTRACTORS

Each Service uses a multitude of contracts and contractors for the acquisition of JCWA's UP, JCC2, PCTE, JCAP, tools, and sensors.

TEST ADEQUACY

Similar to last year's report, no JCWA-level operational testing was conducted in FY25, and the JCWA components continue to employ Agile methodologies on different development and deployment schedules. However, USCYBERCOM is taking key steps to enable JCWA-level testing by improving the JCWA-level requirements development process and establishing the Joint Interoperability Test Command (JITC) as the lead operational test agency.

In FY25, though some components underwent limited operational testing but was not sufficient to assess operational effectiveness and suitability. PCTE conducted regular operational testing along with cyber resilience testing. JCC2 initiated testing to support an operational utility evaluation. JCAP conducted multiple cyber resilience test events.

Service operational test agencies remain challenged to support the individual component OT&E programs and are unable to react to the constantly evolving demands of Agile software-centric programs. Thus, the Services continue to field multiple capabilities with insufficient testing. DOT&E will continue to work with JITC and USCYBERCOM to address these challenges.

As the JCWA concept matures, the scope of T&E required to support cyber warfighting efforts needs to continuously evolve so that it addresses the entire architecture and the dynamic, operational environment within which JCWA operates. Adequate OT&E of JCWA will require USCYBERCOM to establish a cadence of testing and invest in the development of test infrastructure.

The DOT&E Cyber Assessment Program (CAP) continues to partner with USCYBERCOM to identify ways in which CAP activities can support assessments of USCYBERCOM's global infrastructure for cyber operations.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

Insufficient data have been collected to enable a preliminary assessment of the JCWA-level operational effectiveness and suitability.

» SURVIVABILITY

Insufficient data have been collected to enable an evaluation of JCWA mission resilience in a cyber-contested environment.

RECOMMENDATIONS

As recommended in the FY23 and FY24 Annual Reports, USCYBERCOM should:

1. Prioritize and accelerate efforts to finalize JWCA-level requirements.
2. Require OT&E to inform value assessments.
3. Establish a cadence of testing for dedicated OT&E, beginning in FY26, to understand how the capabilities afforded by JCWA evolve over time and to ensure JCWA is an operationally effective, suitable, and survivable enabler of cyber operations.
4. Continue to partner with the DOT&E CAP to characterize the cyber posture of critical infrastructure related to JCWA.