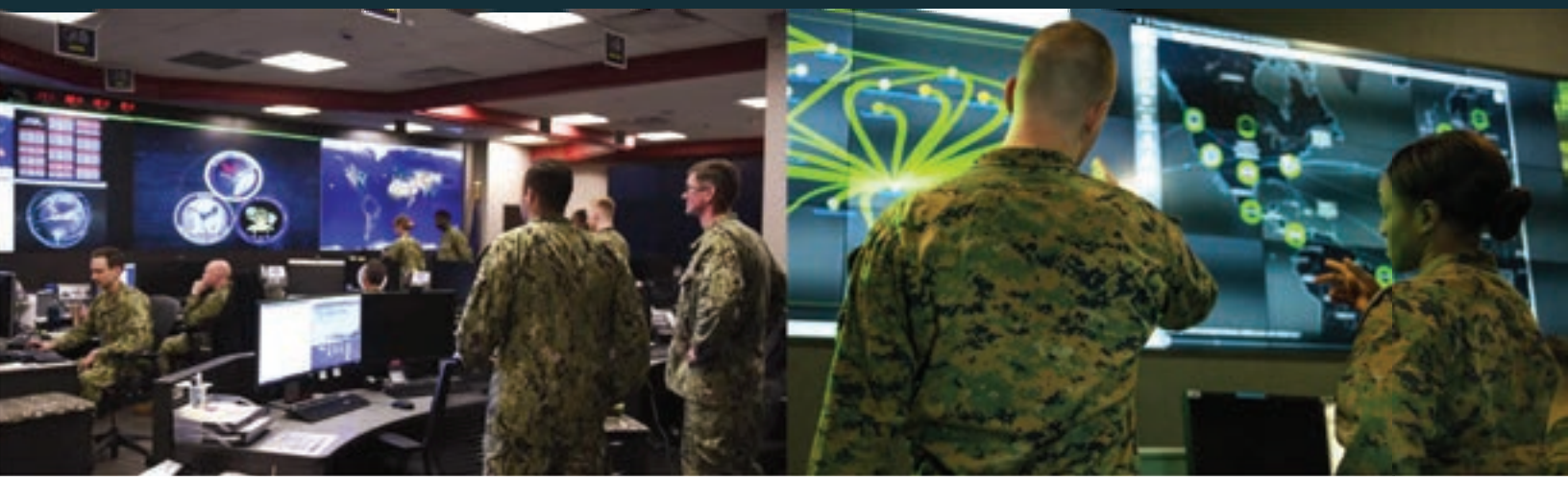
Joint Cyber Warfighting Architecture (JCWA)



The Joint Cyber Warfighting Architecture (JCWA) concept continues to mature; however, no dedicated JCWA-level operational test and evaluation (OT&E) is currently planned or resourced, despite aggressive efforts to field critical components of the architecture. This will limit the Department's ability to understand the impact of current and future capability integration on JCWA's operational effectiveness, suitability, or survivability.

SYSTEM DESCRIPTION

JCWA is designed to collect, fuse, and process data and intelligence in order to provide situational awareness and battle management at the strategic, operational, and tactical levels while also enabling access to a suite of cyber capabilities needed to rehearse and then act in cyberspace.

MISSION

U.S. Cyber Command (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 itself but currently encompasses the following four acquisition programs:

- Unified Platform will act as a data hub for JCWA, unifying disparate cyber capabilities in order to enable full-spectrum cyberspace operations.

- Joint Cyber Command and Control will provide situational awareness, battle management, and cyber forces' management for full-spectrum cyber operations.
- Persistent Cyber Training Environment will provide individual and collective training as well as mission rehearsal for cyber operations.
- An access component will provide additional capability for cyber operations.

USCYBERCOM relies heavily on the Services for acquisition of the programs that comprise JCWA. To guide these individual acquisition programs, USCYBERCOM initially established the JCWA Integration Office and the JCWA Capabilities Management Office, but in FY22 merged the two offices under one principal staff advisor for efficiencies. The resulting entity from the merge continues to lack the authority and resources to effectively manage critical JCWA-level activities. Each program has its own release and deployment schedules, and there are no validated JCWA level mission thread requirements or plans for an integrated JCWA-level operational test. Three out of the four current JCWA programs leverage the software acquisition pathway and require annual value assessments that determine if capabilities delivered have been worth the investment. USCYBERCOM has yet to leverage OT&E as a data source for these annual value assessments.

» MAJOR CONTRACTORS

Each Service uses a multitude of contracts and contractors for the acquisition of Unified Platform, Joint Cyber Command and Control, Persistent Cyber Training Environment, and JCWA's access component.

TEST ADEQUACY

JCWA programs continue to develop T&E strategies independent of the JCWA construct. In FY22, the Service-led programs continued to conduct program-level T&E, including early cybersecurity assessments. DOT&E has informed and monitored testing conducted to date and will use the data in operational assessments where appropriate.

As the JCWA concept continues to mature, the scope of OT&E required to support cyber warfighting efforts will need to continuously evolve so that it addresses the entire architecture and the dynamic, operational environment within which it operates.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

Not enough data have yet been collected to enable a preliminary assessment of the JCWA-level operational effectiveness and suitability, or the performance of its individual components.

» SURVIVABILITY

Not enough data have yet been collected to enable an evaluation of JCWA mission resilience in a cyber-contested environment.

RECOMMENDATIONS

USCYBERCOM should:

1. Immediately resource and empower the Joint Interoperability Test Command to plan, conduct, and assess integrated, JCWA-level OT&E.
2. Require OT&E to inform the JCWA value assessments.
3. Establish a cadence of test for dedicated OT&E, beginning in FY23, to understand how the capability afforded by JCWA is evolving over time and to ensure it is an effective, suitable, and survivable enabler of cyber operations.
4. Define and resource the test infrastructure required to successfully support JCWA integration, as well as T&E to support key decision points, user acceptance, and value assessments.