Joint Cyber Warfighting Architecture (JCWA)

The Joint Cyber Warfighting Architecture (JCWA) concept continues to mature, and the Services continue aggressive efforts to field critical components of the architecture without adequate OT&E. U.S. Cyber Command's (USCYBERCOM) Joint Integration Office (JIO) continues to make significant strides towards accomplishing dedicated JCWA-level OT&E; however, the JCWA OT&E program remains in the initial planning and resourcing stages.

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

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.

The FY23 National Defense Authorization Act (NDAA) Section 1509 provides for the establishment of a JCWA Program Executive Office (PEO) within USCYBERCOM, as well as the FY22 NDAA that provides the commander of USCYBERCOM enhanced budget control starting in FY24. A JCWA PEO would be responsible for the creation and maintenance of a JCWA Governance charter, requirements, and program schedules.

USCYBERCOM currently relies on the Services for acquisition of the programs that comprise JCWA. Each program has its own release, testing, and deployment schedule, and there are no validated JCWA-level requirements nor a JCWA Governance Charter.

Three out of the four current JCWA programs leverage the software acquisition pathway, which requires annual value assessments. The assessments determine if capabilities delivered have been worth the investment. The OT&E community is coordinating closely with USCYBERCOM's Value Assessment Team to share data and findings.

» 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

Service-led programs under JCWA continue to develop and execute T&E strategies independent of the JCWA construct; however, the JIO recently identified the Joint Interoperability Test Command as the program's lead Operational Test Agency and provided initial funding to begin JCWA-level OT&E planning in FY23 for the first JCWA-level OT&E event in FY24.

In FY23, the Service-led programs under JCWA continued to conduct program-level contractor, developmental, and operational testing, including cyber assessments. DOT&E has informed and monitored testing conducted to date and will use the data in operational assessments where appropriate. DOT&E will issue an early fielding report in 2QFY24. 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. Adequate operational test and evaluation of JCWA will require USCYBERCOM to establish a cadence of test and invest in the development of test infrastructure to successfully support JCWA integration and ensure mission effectiveness and survivability as the enterprise evolves.

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. As recommended in the FY22 Annual Report, require OT&E to inform value assessments.
2. As recommended in the FY22 Annual Report, 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.
3. As recommended in the FY22 Annual Report, establish a cadence of test for dedicated OT&E, beginning in FY24, 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. Establish a JCWA Governance Charter to identify roles and responsibilities for USCYBERCOM's enhanced budget control and new acquisition authorities over Service-led JCWA subsystems.
5. Prioritize and accelerate efforts to finalize JCWA-level requirements.