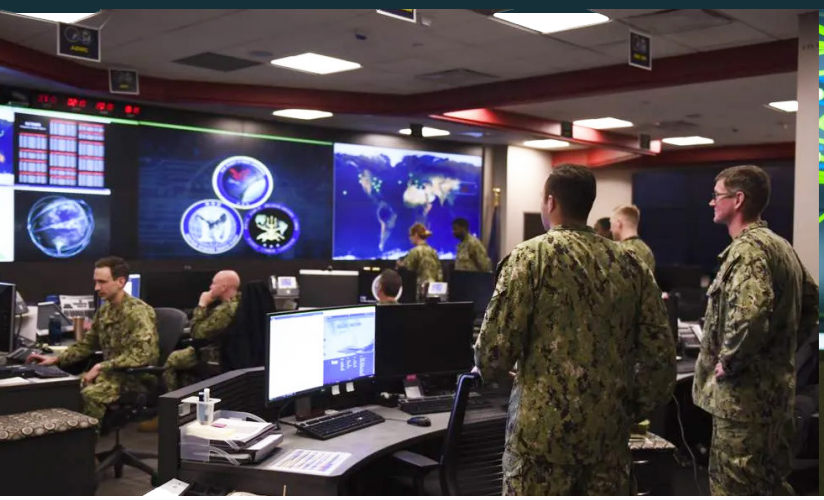
Joint Cyber Warfighting Architecture (JCWA)



With enhanced budget control and the intent to establish a Program Executive Office (PEO), U.S. Cyber Command's (USCYBERCOM) Joint Cyber Warfighting Architecture (JCWA) Integration Office (JIO) is at a critical juncture, with the goal of establishing a more agile, scalable, and interoperable JCWA. JCWA remains a concept that lacks the requirements, testing, proper governance, workforce, and authorities to successfully enable global cyber operations. The Services continue to aggressively field critical components of the architecture without adequate OT&E, and lessons learned from classified early operations indicate that this process must change. It is critical that USCYBERCOM finalize and submit the JCWA TES to DOT&E for approval. The JCWA TES has been in development for several years and once approved will aide in securing the T&E resources required to successfully verify JCWA system performance; inform critical training; and develop operational tactics, techniques, and procedures across all levels of JCWA global cyber operations.

SYSTEM DESCRIPTION

JCWA is designed to collect, fuse, and process data and intelligence 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 components:

- Unified Platform integrates cyber capabilities and systems as well as collaboration tools to enable cyber data processing, analysis, exploitation, and dissemination to support full spectrum cyber operations.
- Joint Cyber Command and Control will provide situational awareness, battle management, and cyber forces' management for full-spectrum cyber operations.
- The 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.
- Other projects and methodologies used to develop and deploy tools and sensors to cyber forces.

At this time, USCYBERCOM continues to rely on the Services for acquisition of the components that comprise JCWA. However, the Command is taking initial steps to bring the acquisition programs under its authority. Each component currently has its own release, testing, and deployment schedule, and there are no validated JCWA-level requirements nor a JCWA Governance Charter.

The National Defense Authorization Acts of FY22 and FY23 provided for both USCYBERCOM enhanced budget control in FY24 and the establishment of a JCWA PEO within USCYBERCOM. The JCWA concept is at a critical juncture, as USCYBERCOM must establish governance processes and establish the workforce to do the following with limited resources: manage acquisition authorities, transition program management activities from the Services to the Command, develop requirements, and deliver capability that has been validated through adequate T&E. In light of these significant changes, DOT&E did not publish the early fielding report in FY24, as stated in the FY23 Annual Report. In 2QFY25, DOT&E intends to issue a classified report on JCWA's ability to conduct global cyber operations.

» 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, JCWA's access component, tools, and sensors.

TEST ADEQUACY

No JCWA-level operational testing was conducted during FY24. Interoperability efforts are currently ad hoc, with all JCWA components employing different Agile methodologies and on different development and deployment schedules. Operational testing at the component-level has been insufficient. Service-led programs under JCWA continue to develop and execute TESs independent of the JCWA construct. Service Operational Test Agencies have struggled to support the individual component OT&E programs, unable to react to the technical and constantly evolving demands of Agile, software-centric programs. This has resulted in the Services fielding multiple capabilities with insufficient testing, and as in some cases, operators or program managers doing their own series of validation events to inform user acceptance and capability release. DOT&E embraces the Development Security Operations (DevSecOps) approach and will be utilizing data from multiple sources in its operational assessments.

The JIO appointed the Joint Interoperability Test Command as the JCWA lead Operational Test Agency and provided initial funding to begin JCWA-level OT&E planning in FY23, with the intent to conduct initial JCWA-level OT&E events in FY24. Changes in JIO leadership, enhanced budget control, and lack of dedicated government T&E personnel in the JIO resulted in multiple stand-downs across JCWA components and the cancellation of critical T&E planning events intended to inform long-term T&E resource requirements. However, the USCYBERCOM JIO and DOT&E are working to approve the first JCWA TES in 1QFY25, which is a critical step toward establishing the required workforce and capability to support operationally effective, suitable, and survivable cyber missions. JIO and DOT&E also agree that future versions of the JCWA TES must also include an Integrated Decision Support Key that establishes evaluation criteria for the JCWA test program.

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 OT&E 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. Planning and execution of dedicated JCWA OT&E will begin in FY25. Additionally, the DOT&E Cyber Assessment Program intends to partner with and increase its support to a USCYBERCOM Mission Approval Board over the next fiscal year, which will enable unprecedented cyber survivability assessments of USCYBERCOM's global infrastructure supporting cyber operations.

PERFORMANCE

» EFFECTIVENESS AND SUITABILITY

Insufficient data have been collected to enable a preliminary assessment of the JCWA-level operational effectiveness and suitability, or the performance of its individual components.

» 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 Annual Report, USCYBERCOM should:

1. Prioritize and accelerate efforts to finalize JCWA-level requirements.
2. Require OT&E to inform value assessments.
3. Establish a cadence of test for dedicated OT&E, beginning in FY25, to understand how the capability afforded by JCWA is evolving over time and to ensure it is an operationally effective, suitable, and survivable enabler of cyber operations.

Additionally, USCYBERCOM should:

1. Establish a dedicated, government T&E chief in the JIO/PEO.
2. Establish a Combined Developmental Test/ Operational Test Force that streamlines the T&E community.
3. Work with the T&E community to develop an Integrated Decision Support Key to establish evaluation criteria for the JCWA test program.
4. In an effort to secure and mitigate operational risk to cyber missions, partner with the DOT&E Cyber Assessment Program to immediately stand up a USCYBERCOM Mission Approval Board to enable cyber assessments of some of the architecture's most critical assets currently supporting operations.