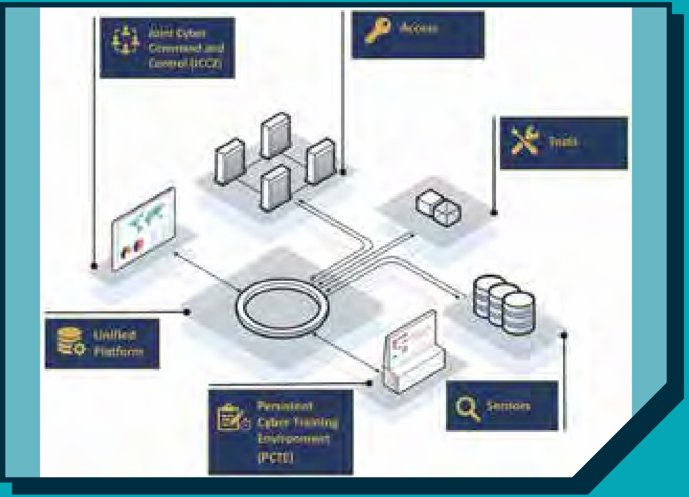
Joint Cyber Warfighting Architecture (JCWA)

United States Cyber Command (USCYBERCOM) continues to define the Joint Cyber Warfighting Architecture (JCWA) concept, but a lack of governance has led to an ad-hoc alignment of T&E efforts for the systems JCWA encompasses. This will result in fielding capabilities without demonstrating or understanding their contribution to JCWA operational effectiveness, suitability, or survivability. USCYBERCOM has not designated an Operational Test Agency to define and develop metrics needed to conduct integrated JCWA-level OT&E. T&E strategies and processes are maturing, but not fast enough to support initial delivery of capability and features.


Joint Cyber Command and Control (JCC2)
Access
Tools
Unified Platform
Persistent Cyber Training Environment (PCTE)
Sensors

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. Given this construct, JCWA is also expected to illuminate cyber capability shortfalls to guide the acquisition of needed cyber warfighting capabilities.

Program

JCWA is not a program of record itself but currently encompasses the following four acquisition programs:

- **Unified Platform (UP)** 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 (JCC2)** will provide situational awareness, battle management, and cyber forces' management for full-spectrum cyber operations.
- **Persistent Cyber Training Environment (PCTE)** 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 established the JCWA Integration Office and the JCWA Capabilities Management Office. Both lack the authority or resources to effectively manage critical JCWA-level activities. Each program has different release and deployment schedules, and there are no validated JCWA-level mission thread requirements or plans for an integrated JCWA-level operational test.

Major Contractors

Each Service uses a multitude of contracts and contractors for the acquisition of UP, JCC2, PCTE and JCWA's access component. A complete list of major contractors is provided in the Controlled Unclassified Information edition of this report.

Test Adequacy

In FY20, the JCWA Integration Office initiated the development of a JCWA T&E strategy by establishing multiple working groups to inform test infrastructure requirements and develop test scenarios based on mission threads. The development of the JCWA test strategy is still maturing and needs greater support from USCYBERCOM and the Services to plan and resource dedicated operational testing to validate COF mission thread effectiveness, suitability, and survivability in support of the deployment of capability. In parallel, each of the programs is developing T&E strategies independent of the JCWA construct, which may lead to inefficiencies and test inadequacies. In FY21, multiple JCWA components conducted early program-level T&E, including early cybersecurity assessments. DOT&E informed and monitored testing conducted to date and will use the data in its operational assessments where appropriate.

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

No data have yet been collected to enable an evaluation of JCWA mission resilience in a cyber-contested environment.

Recommendations

1. The DOD should identify, resource, and empower a JCWA-level acquisition management organization to coordinate the integration of JCWA capability. Lack of JCWA governance has resulted in ad-hoc efforts to synchronize T&E across the architecture.
2. USCYBERCOM, in coordination with DOT&E and the Services, should develop, resource, and execute a JCWA-level T&E strategy.
3. USCYBERCOM, in coordination with DOT&E, the National Security Agency, and the Services, should plan and conduct robust cyber testing of JCWA and its subcomponents.