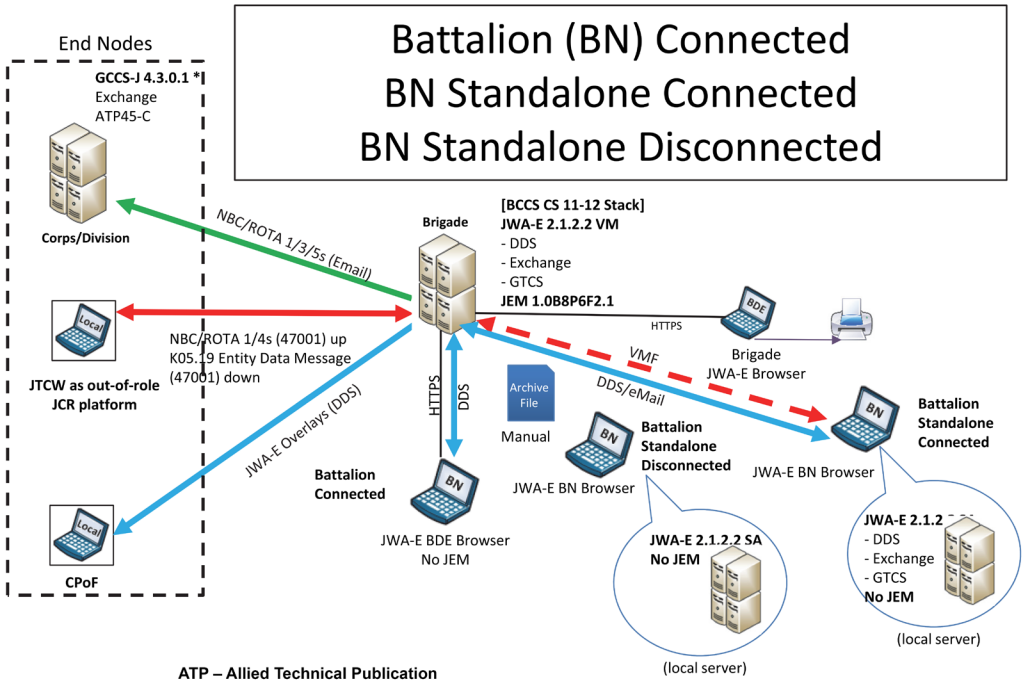
Joint Warning and Reporting Network (JWARN)



ATP – Allied Technical Publication
BCCS CS 11-12 – Battle Command Common Services Capability Set 11-12
BDE – Brigade
CPoF – Command Post of the Future
DDS – Data Dissemination Service
GCCS-J – Global Command and Control System–Joint
GTCS – Ground Tactical Communications Services
HTTPS – Hypertext Transfer Protocol Secure
JCR – Joint Capabilities Release
JEM – Joint Effects Model
JTCW – Joint Tactical Common Operating Picture Workstation
JWA – Joint Warning and Reporting Network Web Application
JWA-C – Joint Warning and Reporting Network Web Application compliant with ATP 45 C
JWA-E – Joint Warning and Reporting Network Web Application compliant with ATP 45 E
NBC – Nuclear, Biological, Chemical
ROTA – Release Other Than Attack
VM – Virtual Machine
VMF – Variable Message Format

Executive Summary

- The U.S. Army Operational Test Command (OTC) conducted an operational test of the Joint Warning and Reporting Network (JWARN) Web Application E (JWA-E) during an Armored Brigade Combat Team field training exercise from June 9 – 16, 2016, at Fort Hood, Texas.
- JWA-E software is backward compatible and interoperable with JWARN Increment 1 software.
- In a degraded communications environment, JWA-E operating on stand-alone computers provides battalion chemical, biological, radiological, and nuclear (CBRN) operators an automated capability to create, edit, and correlate CBRN reports to support battalion leadership.
- Operators of JWA-E on stand-alone Command Post of the Future (CPOF) computers could not see CBRN hazard plots and unit locations on an operational map at the same time to identify units at risk to send CBRN warning reports when not connected to the Brigade Command and Control System (BCCS) servers.

System

- JWARN is a joint automated CBRN warning, reporting, and analysis software tool. It resides on joint and Service command and control systems including the Global Command and Control System (GCCS) – Army, GCCS – Joint, GCCS – Maritime, Command and Control Personal Computer/ Joint Tactical Common Workstation, the Army's BCCS server, and on stand-alone computers.
- JWARN software automates the NATO CBRN warning and reporting process to increase the speed and accuracy of information.
- The JWARN Increment 2 program will consist of four phases named after the Requirements Definition Package (RDP) that

identifies the capabilities to be delivered. Each RDP will have multiple software capability drops.
- RDP-1 will update the JWARN Web Application code to comply with recent changes to the NATO Allied Technical Publication 45 and add planning tools previously included in Increment 1 versions of JWARN
- RDP-2 is envisioned to integrate RDP-1 capabilities into the Service command and control system/ architectures
- RDP-3 is envisioned to provide capability to integrate with networked sensors
- RDP-4 is anticipated to support modernization and emerging capabilities

Mission
A unit equipped with JWARN provides analysis of potential or actual CBRN hazard areas based on operational scenarios or sensor and observer reports, identifies affected units and operating areas, and transmits warning reports to support commanders' force protection and operational decisions.

Major Contractor
Northrop Grumman Mission Systems – Orlando, Florida

Activity
- In FY16, the Joint Program Office for Information Systems (JPM-IS) delivered the first two capability drops for JWARN Increment 2 RDP 1 referred to as JWA-E. JWA-E operates as a Web Application on the Army's BCCS server and stand-alone CPOF computers. The software is compliant with the NATO Allied Technical Publication – 45 version E.
- JPM-IS conducted developmental testing on JWA-E, at its integration laboratory in San Diego, California, from October 2015 to April 2016.
- JPM-IS and the Army Test and Evaluation Command conducted integrated testing of JWA-E from April 25 – 28, 2016.
- The Army Research Laboratory Survivability/Lethality Directorate conducted a Cooperative Vulnerability and Penetration Assessment of the JWA-E from February 1 – 5, 2016, at Aberdeen Proving Ground, Maryland.
- OTC conducted the JWARN Increment 2 Initial Operational Test – Army 1 (IOT-A1) of the first capability drop during an Armored Brigade Combat Team field training exercise from June 9 – 16, 2016, at Fort Hood, Texas.
- During IOT-A1, OTC conducted an excursion to demonstrate JWARN Increment 2 joint interoperability and backward compatibility by exchanging JWARN messages using a JWA-E operating on a battalion-level CPOF computer in Fort Hood, with the GCCS – Maritime-hosted JWARN Increment 1 operated by Navy personnel in southern California.
- OTC was unable to execute IOT-A1 in accordance with the DOT&E-approved test plan due to network configuration problems and lack of an operational GCCS – Army hosted JWARN Increment 1 system.
- The Army Threat Systems Management Office conducted a cybersecurity Adversarial Assessment during the IOT-A1 that focused on portraying the insider, near-sider, and outsider threats.

Assessment
- JWA-E software is backward compatible and interoperable with JWARN Increment 1 software.
- In a degraded communications environment, JWA-E on stand-alone CPOF computers provides battalion CBRN operators an automated capability to create, edit, and correlate CBRN reports to support battalion leadership.
- When not connected to the BCCS server, operators of the JWA-E on CPOF computers could not see CBRN hazard plots and unit locations on an operational map at the same time to identify units at risk to send CBRN warning reports.
- JWA-E planning tools provide CBRN operators with the capability to generate basic hazard prediction plots to support the development of courses of action in the event of a CBRN incident.
- The JWA-E has cybersecurity vulnerabilities that need to be corrected prior to fielding.

Recommendations
- Status of Previous Recommendations. The JWARN Program Office and the Navy addressed all FY15 recommendations.
- FY16 Recommendations. The JPM-IS should:
  1. Work with the appropriate Army Program Offices to identify a solution so that operators using JWA-E stand-alone can see CBRN hazard plots in relation to operational unit locations to enable timely identification and warning of units at risk.
  2. Correct the cybersecurity vulnerabilities discovered during IOT-A1 prior to fielding.