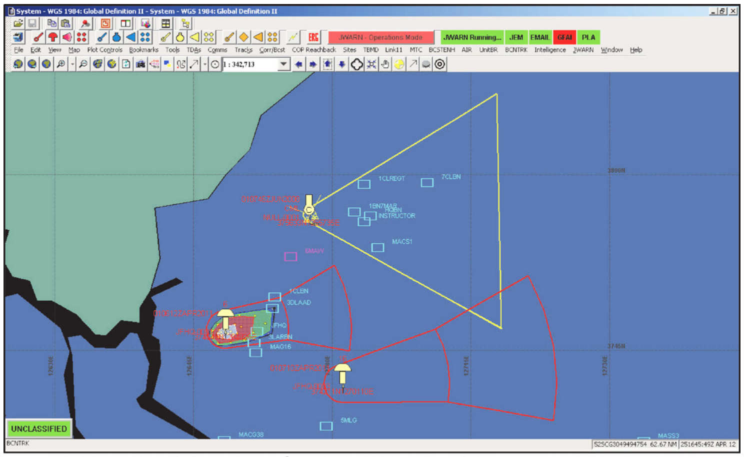
Joint Warning and Reporting Network (JWARN)

Executive Summary

- The Navy's Commander, Operational Test and Evaluation Force (COTF) conducted FOT&E of the Joint Warning and Reporting Network (JWARN) Increment 1 hosted on the Global Command and Control System (GCCS) – Maritime (GCCS-M) Force Level from April to June 2015 onboard the USS *Ronald Reagan* (CVN 76), USS *John C. Stennis* (CVN 74), and JWARN hosted on GCCS – Joint at the Navy Third Fleet Maritime Operations Center (MOC).
- JWARN is an operationally effective tool for the Navy to provide timely hazard warning to Navy ships and other Service units operating 18 kilometers or more away from the initial chemical, biological, radiological, and nuclear (CBRN) release to institute force protective actions before encountering the hazard. Units that are less than 18 kilometers from the release should be warned by other means, such as chat or radio.
- Tactical Action Officers were able to use JWARN information to make operational decisions and recommendations to ship commanders and share CBRN hazard plots within the Combat Direction Center and with other units via the GCCS-M Common Operating Picture Synchronization Tool.
- Testers were unable to exploit JWARN on the Consolidated Afloat Network Enterprise Services (CANES) network or GCCS-M client during remote cyber-attack testing. JWARN demonstrated a 97 percent operational availability and met the requirement for 100 hours Mean Time Between Operational Mission Failure.
- Current plans for sustaining JWARN interoperability in a complex network operating environment are not adequate to sustain the JWARN capability over time.

System

- JWARN is a joint automated CBRN warning, reporting, and analysis software tool that resides on joint and Service command and control systems including the GCCS – Army, GCCS – Joint, GCCS – Maritime, and Command and Control Personal Computer/Joint Tactical Common Workstation.


System - WGS 1984: Global Definition II - System - WGS 1984: Global Definition II
JWARN - Operations Mode
JWARN Running...
JEM
EMAIL
GFAI
PLA
File Edit View Map Plot Controls Bookmarks Tools TDAs Comms Tracks Corr/Bcst COP Reachback Sites TBMD Link11 MTC BCSTENH AIR UnitBR BCNTRK Intelligence JWARN Window Help
1 : 342,713
1CLREGT
7CLBN
1BN7MAR
INSTRUCTOR
MACS1
6MAW
1CLBN
3DLAAD
JFHQ
3LARBN
MAG16
5MLG
MACG38
MASS3
3800N
3745N
12630E
12645E
12700E
12715E
12730E
UNCLASSIFIED
BCNTRK
62.67 NM
APR 12

JWARN screen shot depicting CBRN hazard overlay on the common operational map

- JWARN software automates the NATO CBRN warning and reporting process to increase the speed and accuracy of information.
- JWARN uses the common operating picture of the host command and control system or computing environment to display the location of CBRN events and the predicted or actual location of hazards.
- JWARN is an application on the GCCS-M, and is interoperable with the ship's tactical network, the CANES.

Mission

JWARN operators support the commander's force protection and operational decisions by:

- Providing analysis of potential or actual CBRN hazard areas based on operational scenarios or sensor and observer reports
- Identifying affected units and operating areas
- Transmitting warning reports

Major Contractor

Northrop Grumman Mission Systems – Orlando, Florida

Activity

- COTF conducted FOT&E of the JWARN Increment 1 hosted on the GCCS-M Force Level from April to June 2015, aboard the USS *Ronald Reagan* (CVN 76), USS *John C. Stennis* (CVN 74), and JWARN hosted on GCCS – Joint at the Navy Third Fleet MOC. Testing was conducted in accordance with the DOT&E-approved test plan.
- FOT&E consisted of:
  - Adversarial intelligence collection
  - Local and remote reconnaissance and cyber attacks
  - Initial operator training
  - JWARN installation and configuration at each test location
  - Computer-based refresher training immediately preceding the operational test
  - A logistics and maintenance demonstration
- A three-day operational test in which JWARN operators received reports of CBRN incidents and used JWARN to

analyze the information and generate hazard plots and warning messages sent to units at risk of exposure.
- COTF collected supplemental test data on the time it takes to achieve various levels of mission oriented protective posture in response to a CBRN threat during an operational exercise aboard the USS *Theodore Roosevelt* (CVN 71) in September 2014 and February 2015.

Assessment

- JWARN is an operationally effective tool for the Navy to provide timely hazard warning to Navy ships and other Service units operating 18 kilometers or more away from the initial CBRN release to institute force protective actions before encountering the hazard. Units that are less than 18 kilometers from the release should be warned by other means, such as chat or radio.
- Tactical Action Officers were able to use JWARN information to make operational decisions and recommendations to ship commanders and share CBRN hazard plots within the Combat Direction Center and with other units via the GCCS-M Common Operating Picture Synchronization Tool.
- Twenty-one percent of hazard warnings (10 of 47) were not received in time to support force protection due to CANES network problems or long message transmission times.
- JWARN demonstrated a 97 percent operational availability. Down time resulted from the need to reboot the client computer and network failures. There were no JWARN software failures during 118 hours of operation.
- The local and remote cyber reconnaissance did not expose significant vulnerabilities in the ship's network or the GCCS-M client, which hosts JWARN. Testers were unable to exploit JWARN on the CANES network or GCCS-M client during remote cyber-attack testing.
- Users found the new equipment and online computer-based training to be suitable. Course content is available on computer disks for instances where slow internet connections are a problem.
- Current Joint Program Manager – Information Systems (JPM-IS) plans are not suitable for the installation, configuration, and sustainment of JWARN capability in the complex Navy network operating environment. Prior to operational test, the JWARN software was installed on the ship's and MOC servers. Then, Program Office personnel were required to configure JWARN for operational use and fix problems at each site prior to the test.

Recommendations

- Status of Previous Recommendations. The JWARN Program Office successfully addressed all previous FY14 recommendations.
- FY15 Recommendations.
  1. The JPM-IS, in conjunction with the Program Management Office for host systems, should review plans for the installation and configuration of JWARN and ensure adequate resources and training are provided to install and sustain JWARN in the Navy network operating environments over time. This review should address a process for verifying JWARN operation and interoperability at each location after network updates and software patches and recurring deployment check outs to ensure operational capability.
  2. The Navy should establish recurring training standards for JWARN operators and CVN Tactical Action Officers and consider incorporating JWARN into fleet training exercises.
  3. The Navy should conduct recurring deployment interoperability verification.