Coalition Operations With the Combined Enterprise Regional Information Exchange System (CENTRIXS)

Brad Carter
Debora Harlor

Space and Naval Warfare Systems Command San Diego
C4I Programs Hawaii Code 2424
675 Lehua Avenue
Pearl City, HI 96782-3356

ABSTRACT

This paper discusses the continued development and operation of coalition networks in support of U.S. Pacific Command's initiative to provide classified, permanent network service for bilateral and multilateral communities of interest for combined and coalition operations. The Combined Operations Wide Area Networks (COWAN) project, headed by SSC San Diego personnel, continued to grow and has recently been consolidated with the Combined Enterprise Regional Information Exchange System (CENTRIXS) program, originally designed to support U.S. Central Command requirements. The consolidation of these efforts has created a dynamic team of personnel working to meet the increasing need for secure global connectivity. Challenges continue to confront the team, primarily in getting approved and accredited technical solutions for connecting multiple classified domains to facilitate the Global War on Terrorism.

BACKGROUND

Numerous coalition wide area networks (CWANs) have been built by operational commanders to support coalition operations and exercises, only to be dismantled at the completion of the objectives. This process is inefficient, requiring a long lead-time for planning and implementation. This paradigm limits the commander's ability to streamline tactics, techniques, and procedures for coalition information exchange. SSC San Diego's role has been three-fold. First, SSC San Diego developed the Combined Operation Wide Area Network (COWAN) for Commander, Pacific Fleet (COMPACFLT) and subsequently became the Navy's representative to coalition networking under the Combined Enterprise Regional Information Exchange System (CENTRIXS) program.

Second, SSC San Diego has been the technical advisor to COMPACFLT in its role as Executive Agent for coalition networking under Commander, Pacific Command (CDR USPACOM). This effort includes establishing a joint global coalition network architecture as part of the Global Information Grid in coordination with the Office of the Assistant Secretary of Defense/Command, Control, Computers, and Intelligence (ASD C3I) CENTRIXS Program Management Office, as well as representatives from U.S. Central Command (CENTCOM), U.S. European Command (EUCOM), and U.S. Southern Command (SOUTHCOM). Third, SSC San Diego's Network Centric Computing program has joined both COMPACFLT and PACOM in technology insertion efforts to demonstrate thin client technology with high-assurance network access and data separation to provide a single workstation access to multiple communities of interest (COIs).

HISTORY

In the PACOM area of responsibility, COMPACFLT, with SSC San Diego technical support, developed the first maritime CWAN in support of the Rim of the Pacific Exercise 1998 (RIMPAC 1998). This initial effort consisted of secure email using Secure Telephone Units-Third Generation (STU-IIIs) over a 2.4K International Maritime Satellite (INMARSAT) channel. Follow-on efforts expanded the functionality to allow passing of email between the Secret Internet Protocol Router Network (SIPRNET) and the CWAN through a secure mail guard, and also allowed for the sharing of data through Web browsing. This expanded capability was demonstrated during RIMPAC 2000 and

Exercise Tandem Thrust 2001, using super high-frequency and INMARSAT B connections. The CWAN architecture during Tandem Thrust 2001 allowed U.S. and Australian headquarters to communicate on a variety of levels with maritime, ground, and air component commanders. To maintain this connectivity after the exercise, COMPACFLT achieved a 3-year Department of Defense Security and Accreditation Working Group (DSAWG) approval for the mail guard between SIPRNET and the coalition network, renamed COWAN-A. The COWAN-A network supported Australia, Canada, the United Kingdom, and the United States. USPACOM determined in 2001 that there was a need to consolidate coalition network development and provide a way ahead within the theater. Making use of COMPACFLT's expertise in coalition networks, PACOM selected PACFLT as the Executive Agent for this task. In April 2001, PACFLT N6, supported by SSC San Diego, began working as PACOM's Executive Agent for coalition networking. The original goal was to demonstrate the utility of establishing permanent, classified net-work service with Pacific Rim partner nations to more quickly establish a Joint Task Force Commander's command and control when required. In this manner, COWAN-T (Thailand) was stood up and used by the III Marine Expeditionary Force to revolutionize coalition warfighting during Exercise Cobra Gold 2002, by fighting principally on the COWAN vice SIPRNET and Non-Secure Internet Protocol Router Network (NIPRNET). In addition to Cobra Gold, much of the COWAN effort by SSC San Diego included expanding COWAN-A, as it soon became the primary coalition network supporting Operation Enduring Freedom. In 2001, the office of ASD C3I and CENTCOM fielded a global multi-national information-sharing network called CENTRIXS. This was followed in January 2002 by ASD C3I's establishment of the CENTRIXS program management office to expand coalition networks in support of Operation Enduring Freedom. In October 2002, SSC San Diego implemented PACOM theater remote access to CENTCOM's CENTRIXS-Global Counter Terrorism Force (GCTF) community of interest (68+ nations) to support liaison officers, staff, and deployed or mobile units in support of Operation Enduring Freedom. In February 2003, COWAN and a PACOM intelligence-sharing program known as Pacific Bilateral Intelligence Information Exchange System changed names to CENTRIXS to begin efforts to standardize regional networks, leverage functionality, and provide standard software configurations, information assurance, and concept of operations. Figure 1 shows the COWAN overview.

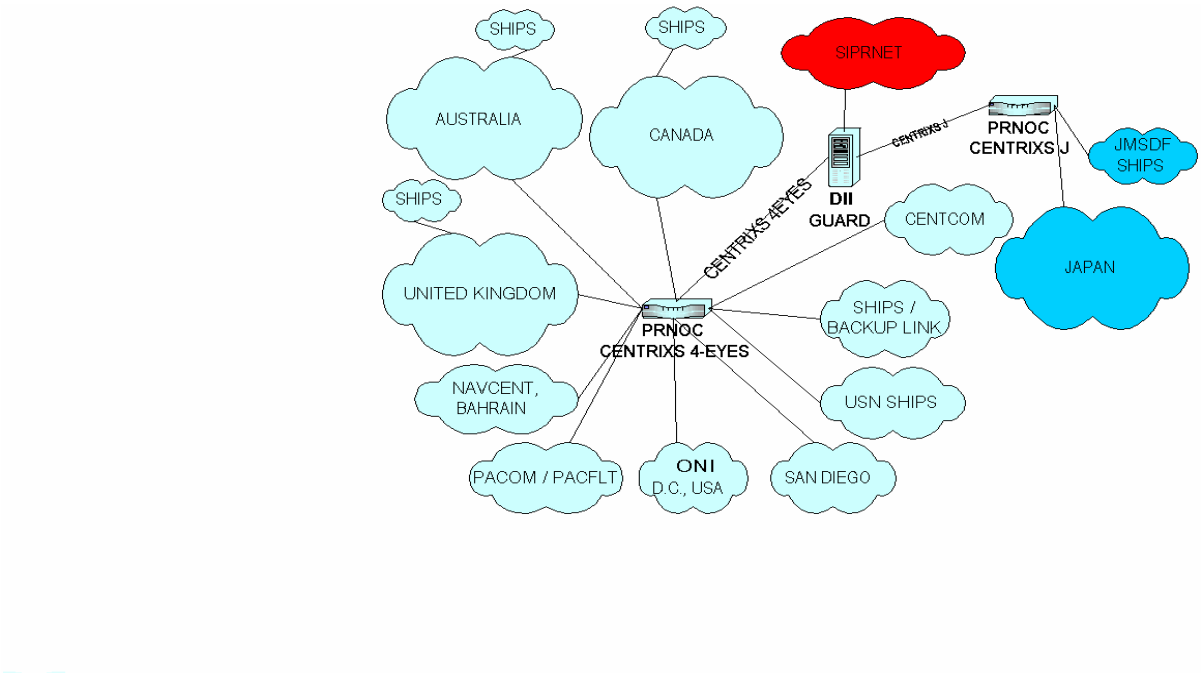

FIGURE 1. COWAN Overview

CURRENT NETWORKING APPROACH

Coalition operations demand responsive information exchange across combined forces and unified commands for planning, unity of effort, decision superiority, and decisive global operations. The CENTRIXS networks now support this operational requirement. The primary CENTRIXS networks in the PACOM AOR include CENTRIXS-4EYES (previously COWAN-A) and CENTRIXS-J (U.S./Japan), CENTRIXS-K (US/Korea). These networks initially provided connectivity with coalition maritime forces and with most of the country's maritime headquarters. CENTRIXS-4EYES, however, has been expanding into the joint arena in the U.S. and the other participating nations. For the maritime platforms, connectivity is made over INMARSAT dial-up, while the major allied shore commands have dedicated circuits. The U.S. users, including afloat units, use TACLANE tunneling over SIPRNET. CENTRIXS-4EYES and CENTRIXS-J use a secure mail guard and provide web data via Lotus Domino™ using an air-gap routine for two-way data exchange between CENTRIXS enclaves and SIPRNET. CENTRIXS-4EYES has CHAT (conversational hypertext access technology) and a common operational picture, which is not currently available on CENTRIXS-J. CHAT capability is the most operationally significant function on CENTRIXS-4EYES and is extensively used for operational coordination. CENTRIXS is web-centric and commercial off-the-shelf oriented. Core information services include email with attachments, Web browser data access, and file sharing. Information transfer employs information technology to support responsive movement of approved data from U.S. sources. This includes email guards for email, specialty guards for formatted message text data, and one-way feed for file and database transfers. Figure 2 shows the CENTRIXS architecture. The system is

intended to support multilateral information sharing as well as specific COIs. The CENTRIXS-GCTF network at CENTCOM supports more than 68 nations, which includes countries supporting the maritime mission. The GCTF network is extended into PACOM to support Pacific Rim countries participating in GCTF mission. Other CENTRIXS networks have been installed to support bilateral agreements for specific COIs. The ASD C3I CENTRIXS program office has merged the COWAN networks with CENTRIXS with both networks providing the same basic functionality. The primary difference between the two networks is the use of CHAT and Domino replication on COWAN. CHAT is used to support the rapid dissemination of time-critical information. The inability to use CHAT between different classified domains requires U.S. ships to have both SIPRNET and CENTRIXS networks to coordinate with U.S. and coalition forces. Because of limited bandwidth available to ships, Domino replication has been selected as the standard for collaboration at sea.

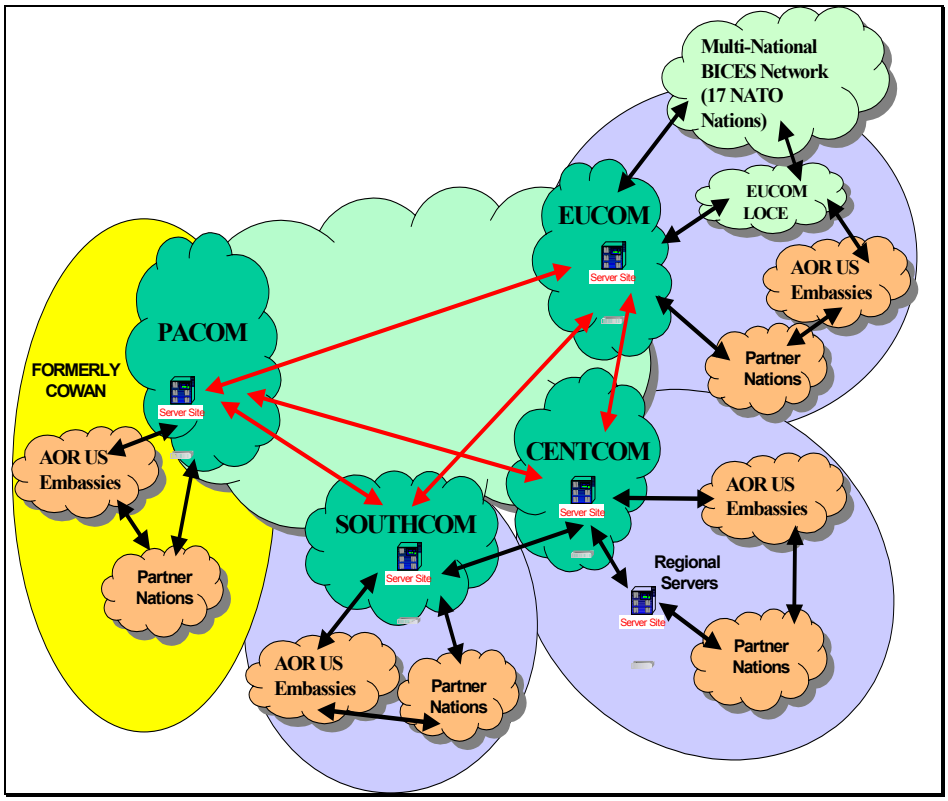

FIGURE 2. CENTRIXS architecture

CURRENT AND FUTURE EFFORTS

The Coalition Warfare Program (CWP) COWAN/CENTRIXS effort is an Office of the Secretary of Defense/PACOM-sponsored Joint Warfighter Interoperability Demonstration 2003 (JWID 2003) coalition interoperability trial to demonstrate a dynamic coalition network and security solution. Currently being developed by the Space and Naval Warfare Systems Command (SPAWAR) and industry, CWP uses net-work-centric computing technologies, ultra thin clients, smart cards, and Cryptek™ evaluation assurance level 4 (EAL 4)-certified virtual private network (VPN) devices to create networks that are flexible and secure. The main focus is to provide enhanced capability on a single workstation and ensure that the right information gets to the right person, at the right place, at the right time. Initial efforts to develop an accredited VPN device were demonstrated in JWID 2002. Using a non-classified local-area network with an ultra thin client architecture, PACOM showcased the ability to simultaneously access separate COIs with privacy. As a follow-on, in JWID 03 PACOM sponsored a classified interoperability trial focusing on agile VPN as the key to providing privacy within a coalition. This demonstration was run on the classified Combined Federated Battle Labs Network (CFBL) located within five countries. Figure 3 shows the JWID architecture overview.

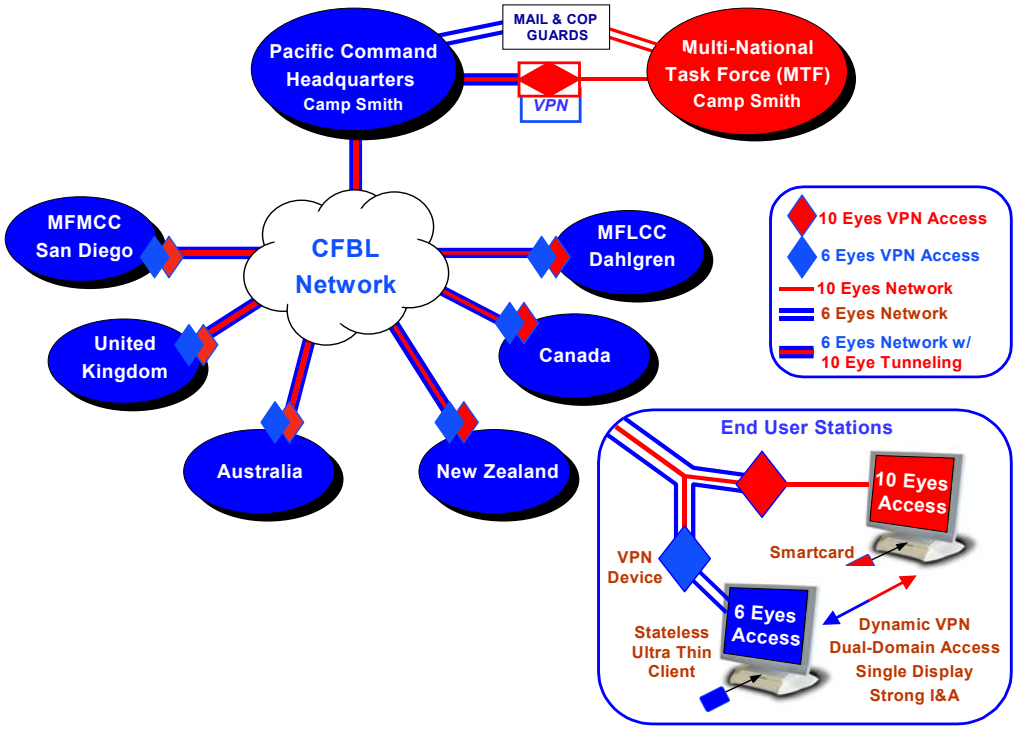

FIGURE 3. JWID architecture overview.

The National Security Agency (NSA) will consider accreditation of PACOM's JWID wide area network demonstration. It provided data separation between security domains via a Cryptek Type-II, VPN device. Defense Information Infrastructure (DII) mail guards and Radiant Mercury multilevel security guards are used to automate and safeguard email and common operational picture services. Long-term goals include inserting a Type-I version of the VPN device. Cryptek has a memorandum of agreement with the NSA and has produced preliminary design and system requirement specification documents. This

effort's schedule depends on publication of the High Assurance Internet Protocol Encryptor System (HAIPES) II specification by the NSA. The HAIPES specification will define "over-the-network keying" providing the basis for VPN agile algorithms, a Type-I algorithm for U.S. use, and an Advanced Encryption System (AES) algorithm for dissemination to coalition nations. Cryptek plans other product enhancements: integrated user identification and authentication (common access card and biometrics) and enhanced system management with centralized policy definition, audit reporting, system updates, and status monitoring.