INTEROPERABILTY SENIOR STEERING GROUP EFFORTS TO BUILD A GLOBAL DATA NETWORK FOR JOINT COALITION WARFIGHTING

Submitted for Coalition Interoperability Track by:

Jill L. Boardman
ACS Defense, Inc.
USCENTCOM
7115 S. Boundary Rd.
MACDILL AFB, FL 33621 (813) 827-1304
boardmjl@centcom.mil

Abstract

Joint warfighting operations demand responsive information exchange across combined forces and unified commands for planning, unity of effort, decision superiority, and decisive global operations. In a concerted endeavor with the other warfighting theater commands, and supported by the Office of the Assistant Secretary of Defense/Command, Control, Computers, and Intelligence and the National Security Agency, U.S. Central Command is fielding a global multinational information sharing network called Combined Enterprise Regional Information Exchange System (CENTRIXS).

CENTRIXS is web-centric and commercial off the shelf oriented. Implementation focused on fielding core information services first--e-mail with attachments, web-browser-based data access, and file sharing (office documents, txt, pdf, image files). Other required services, including collaboration and near-real time data access, are enabled as the network matures. To the extent possible, CENTRIXS will subsume and consolidate existing stove-piped coalition networks as part of a single, unified system.

Over 32 coalition nations are now operating on CENTRIXS globally. Gateways are operational at USCENTCOM Navy, Army, and Air Force component task forces and five deployed force sites, including three for Special Operations. The initial USEUCOM gateway is operational and the USPACOM gateway is in progress.

EXECUTIVE SUMMARY

Global Coalition Network Requirement. The United States Central Command Commander in Chief (USCINCCENT) requires responsive information exchange across combined forces and with other joint warfighting commands for decisive global operations. In a concerted endeavor, the warfighting theater commands are building a common global multinational information sharing enterprise. This is enabling combined force planning, unity of effort, and decisive global counter-terrorism operations.

CENTRIXS is the Solution. USCENTCOM is implementing the Combined Enterprise Regional Information Exchange System (CENTRIXS)-- a single, common global multinational data network for the warfighting commands in support of OPERATION ENDURING FREEDOM (OEF). CENTRIXS is being implemented in partnership with U.S. Pacific Command (USPACOM) and U.S. European Command (USEUCOM), and supported by the Office of the Assistant Secretary of Defense/Command, Control, Computers, and Intelligence (OSD/C3I) and the National Security Agency (NSA). CENTRIXS operates in the system high mode. The system is intended to support multilateral information sharing (i.e., GCTF) as well as feature interfaces to networks for classified information sharing with specific communities of interest.

Coalition C4I Interoperability Challenges. Political, economic, cultural, technical and military differences with partners continue to make it difficult for the theater commanders to achieve combined interoperability. Issues include bilateral agreements, foreign disclosure restrictions, data standard differences, host nation technology, limited coalition infrastructure, varied proliferation of information technology, releasability and availability of U.S. COMSEC devices, and arms transfer/technology release via direct commercial sales/foreign military sales. Ongoing shortfalls in joint interoperability also often impact achieving combined interoperability.

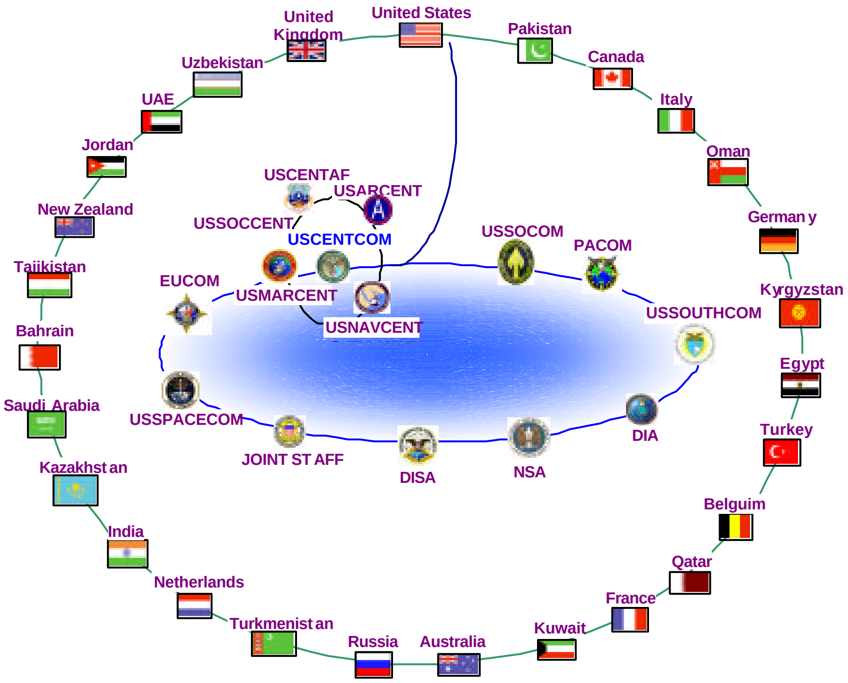
Information Sharing Requirements. Time-critical information for combined warfighting includes; operations and intelligence information for threat and battlefield awareness, mission requirements for integration and coordination of coalition forces, theater ballistic missile defense, NBC threat warning, weather data, regional military and civil air movement scheduling, battlefield campaign assessment data, force disposition and combined force threat response data.

Information Services and Equipment. CENTRIXS is web-centric and COTS-oriented. Implementation focused on fielding core information services first--e-mail with attachments, web-browser-based data access, and file sharing (office documents, txt, pdf, image files). Other required services, including collaboration and near-real time data access, are enabled as the network matures. The system comprises commercially available computers, software applications and network equipment. To the extent possible, CENTRIXS will subsume and consolidate existing theater specific coalition networks as part of a single, unified system.

Information Transfer. CENTRIXS employs certified security-enabled information technology to support responsive movement of approved data from U.S.-only sources. This includes e-mail guards for e-mail, specialty guards for formatted message text data, and one-way fiber systems for file and database transfers. Standing Foreign Disclosure procedures and training provide the structure and process for approving disclosure and release of data to foreign partners.

Community. Over 32 GCTF partner nations are operating on CENTRIXS globally. Gateways are operational at USCENTCOM Navy, Army, and Air Force component task forces and five deployed force sites, including three for Special Operations. The initial USEUCOM gateway is operational and the USPACOM gateway is in progress. The graphic representation below is for illustration only. The 27 flags shown are only a sub-set of the 32 nations now using CENTRIXS. There are 46 nations plus NATO (the organization) that currently make up the GCTF.

CENTRIXS

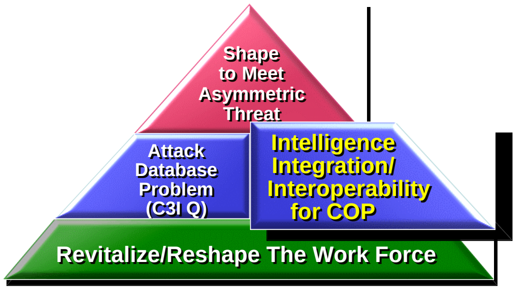


Electronic information sharing across joint commands with multinational partners... for combined global operations region-to-region 1

BACKGROUND AND PURPOSE

USCENTCOM began envisioning and exploring a coalition data-sharing network in early 1999. The primary objective for multinational information was, and still is, to maintain a shared, timely, common visualization of the battlespace with our coalition and allied partners.

By November 1999, the Interoperability Senior Steering Group (ISSG) was formed as one of the Director, Defense Intelligence Agency's (DIA) four major thrust areas to focus the efforts of the defense intelligence community. USCENTCOM was put in charge of the ISSG near-term effort, which revolves around four primary functional areas: GCCS-I3; Collection Management Mission Application (CMMA); Guard Technologies; and CENTRIXS. These four areas were the focus of three Proof of Concept (POC) evaluations conducted from 2000-2001. USCENTCOM teamed with its components, national agencies, the Services, and USJFCOM to devise a common battlespace visualization solution set of joint analytical tools that will provide utility for all the unified commands and their coalition partners.


Shape to Meet Asymmetric Threat
Attack Database Problem (C3I Q)
Intelligence Integration/ Interoperability for COP
Revitalize/Reshape The Work Force

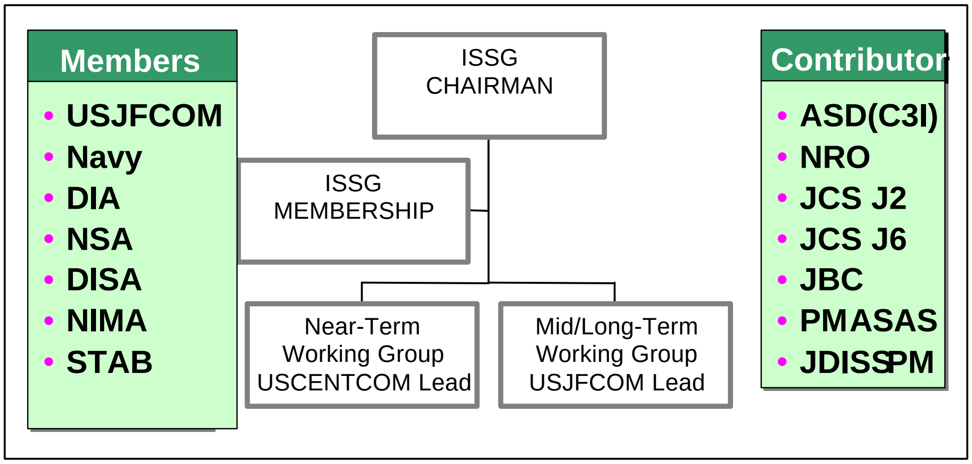
Part of the Defense Intelligence Community's Four Thrusts

ISSG Objective: Improve intelligence support to command and control environment via GCCS

ICW OEF, began implementation/operationalization of solutions in key functional areas

ISSG ONE OF DIRECTOR DIA FOUR THRUST AREAS

The ISSG efforts have focused on improving interoperability at the theater Joint Intelligence Center (JIC) in several dimensions. Initiatives focused on improving interoperability between functional areas within the JIC, between the JIC and Service component intelligence elements, between the JIC and national intelligence systems and organizations, and between the intelligence and operational environments via the Joint C2 system of record the Global Command and Control System (GCCS). The ISSG, membership is shown in the figure below.



ISSG MEMBERSHIP

In response to 11 SEP 01, as USCENTCOM prepared to conduct OPERATION ENDURING FREEDOM (OEF), ISSG efforts focused on speeding the development and implementation of intelligence interoperability solutions for warfighting operations. CENTCOM identified and prioritized the interoperability tools/solutions that were ready or near ready for operational fielding and worked with the national agencies, Services and program offices to accelerate implementation. The overarching warfare requirements supported were; the Common Intelligence/Common Operational Picture (CIP/COP) sharing, intelligence, surveillance and reconnaissance (ISR), and coalition operations. CENTRIXS is the command's data network solution to support coalition operations with command, control and intelligence information.

SCOPE

This paper focuses on intelligence sharing via CENTRIXS. The table below lists the products and information services required for multinational intelligence sharing. Most of these products and information services are self-explanatory. Further explanation of role-based access, peer-to-peer data encryption and persistent information control is contained in footnote.[1]

MULTINATIONAL INTELLIGENCE PRODUCTS AND INFORMATION SERVICES

Products ▪ Operations, intelligence, and mission data (e.g. Air Tasking Orders [ATOs], imagery) ▪ Near-real-time (NRT) data for a Common Operational/Intelligence Picture and situational awareness
Information Services ▪ Browser-based information access/sharing ▪ Electronic mail (e-mail) with attachments ▪ Automated exchange/access to releasable databases (e.g. Modernized Integrated Database [MIDB]) ▪ Collaboration ▪ Streaming Video ▪ Role-based access for bilateral and multilateral exchange of data ▪ Peer-to-peer data encryption ▪ Persistent information control

The membership of the coalition depends on the mission. The Global Counter-terrorism Force (GCTF) organized in support of OPERATION ENDURING FREEDOM includes a broad and diverse membership of 46 nations, including the USA, and NATO (as of APR 02). Pre-OEF planning requirements focused on the Gulf Cooperation Council (GCC) nations plus Egypt and Jordan (GCC+2) as USCENTCOM's potential warfighting coalition.

REQUIREMENT

USCENTCOM Theater Engagement Plan (TEP) 1999-2003 established the requirement for a multinational, information-sharing network. In response, the USCENTCOM Cooperative Defense Initiative (CDI) Campaign Plan 00-01 and the USCENTCOM Coalition Command, Control, Communications, Computers, and Intelligence (C4I) Interoperability Plan, March 2001 further defined the goal coalition network as providing "an integrated, interoperable, multi-discipline C4I/Shared Early Warning (SEW) system-of-systems" for U.S. and GCC+2 decision-makers.

[1] Role-based access basically allows an electronic application of the "need to know principle." Subscribers can only access what they are given permission to access. Peer-to-peer data encryption allows the originator of a document to encrypt and send it to a destination where it is decrypted. The encryption and decryption happen at the workstations, vice at an encryption device or a server. Persistent information control is the ability to limit and/or control what is done with a file. It allows control of copying, editing, printing, saving, and even opening of the file.

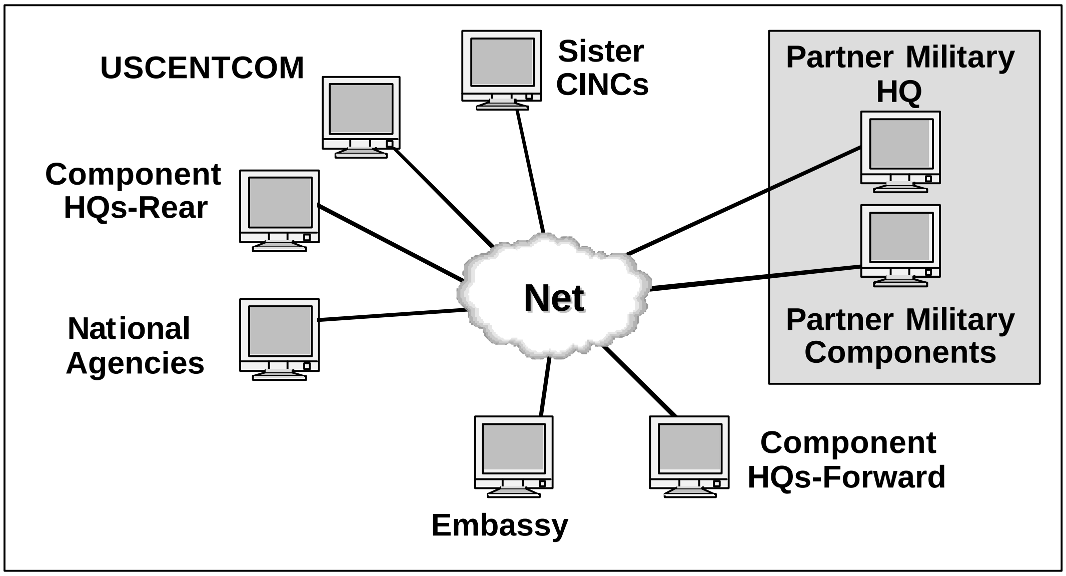
The global nature of the war on terrorism demanded that CENTRIXS become a global multinational information sharing initiative. The development of a broad coalition associated with OEF operations led to requirements for accelerated deployment of the CENTRIXS environment both at USCENTCOM headquarters and in the USCENTCOM Area of Operations (AOR) to include connectivity for Service component elements forward deployed. Probable expansion of OEF operations into other theater command AORs led to planning for additional CENTRIXS gateways in USPACOM and USEUCOM. The Office of the Assistant Secretary of Defense (ASD) Command, Control, Communications and Intelligence (C3I) established the CENTRIXS Program Office late Jan 02 to coordinate the planning, resources, and implementation of CENTRIXS world-wide to support the warfighting commands.

CENTRIXS DESCRIPTION

A global data network enterprise for U.S. and partner forces to share classified operational and intelligence information region-to-region for combined planning, unity of effort, and decision superiority in peacekeeping and contingency operations.

CENTRIXS is designed to meet USCENTCOM's requirement for day to day information sharing with multinational partners. "Combined" refers to the combination of coalition and allied users. "Enterprise" refers to the multiple network capabilities of voice, data, and video. CENTRIXS will ultimately provide a seamless, interoperable, multi-classification level information exchange between the warfighting commands and key multinational players.

The USCENTCOM Directorate of Command, Control, Communications, and Computers (CCJ6) is responsible for implementing CENTRIXS for USCENTCOM. When fully operational, this network will use automated security guards and security-enabled information technology to pass information and intelligence data between the USCENTCOM local area network (LAN) and various LANs in the AOR and the U.S.



END-STATE CENTRIXS NETWORK KEY PLAYERS

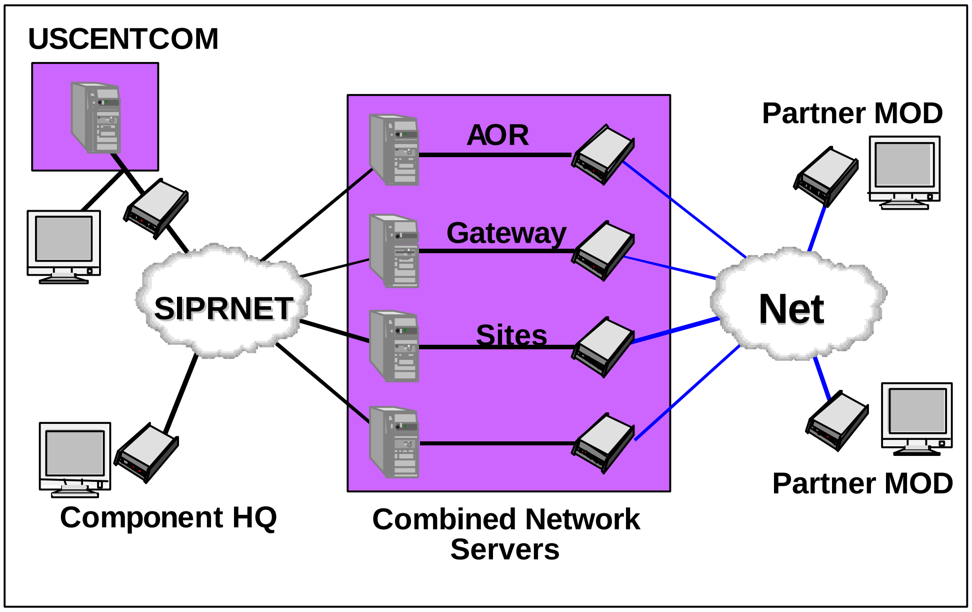
Goal CENTRIXS Network

Near-term.

- CENTRIXS implementation focused on fielding core data services (i.e., email and web browser). This included communications infrastructure with certified guarding technology to achieve an information exchange environment that improves upon present air-gapped, stand-alone network capabilities for operations as part of a multinational force.

- Headquarters USCENTCOM stood up a CENTRIXS LAN. The HQ CENTRIXS LAN connects with and provides a template for forward gateways at Service Component facilities, building on the separate coalition network systems that each Component already has in operation. Host nation CENTRIXS subscribers will access the CENTRIXS web-servers through these gateways. The figure below depicts the forward gateways and initial CENTRIXS network.

- The Headquarters will work with appropriate DoD agencies to provision a dedicated network backbone. The communications infrastructure will initially use Internet protocol (IP) encryptors (TACLANEs) tunneling through SIPRNET to establish the long haul communications connectivity. The host nation connectivity to the gateway site will use releasable TACLANEs tunneling through a host nation appropriate communication infrastructure.



CENTRIXS FORWARD GATEWAYS AND INITIAL NETWORK

- HQ USCENTCOM will establish initial Operations and Maintenance (O&M) support for a command-wide CENTRIXS capability with funding from ASD/C3I. HQ USCENTCOM has supplied deployable CENTRIXS packages that are modular and scaleable to extend data access to forward-deployed forces. The Headquarters has also initiated plans and activities to establish service to U.S. embassies and open US-controlled service access points to partner nations.

- Near-term for Partners. Achieving initial information sharing via forward U.S. CENTRIXS service gateways requires a measured investment by the partners. Economic and technical disparities among partner nations warrant limiting the up-front contribution each must make in order to promote an initial baseline multinational capability. Partners must acquire commercial off the shelf (COTS) personal computers for their users and U.S.-approved COMSEC for encrypting communications links from their facilities using their national communications infrastructure.

- Partner nation network subscribers inside of the USCENTCOM AOR will be responsible for linking up with one of these four gateways to access data. Potential subscribers include the host nation Ministry of Defense (MOD), Director of Military Intelligence (DMI) and armed forces components. Network subscribers outside of the USCENTCOM AOR would likely connect to one of the planned gateways at USEUCOM, USPACOM or USSOUTHCOM.

- The U.S. Embassies Defense Attaches Offices will have CENTRIXS workstations that can access one of the gateway server sites via the network infrastructure.

Software**.**

- CENTRIXS includes a web-based, thin client, multinational releasable application set to provide the desktop and data infrastructure elements. It is a personal computer (PC) application set consisting of the Microsoft Office application suite, Command and Control Personal Computer (C2PC) and Personal Computer Integrated Imagery and Intelligence (PCI3), which is now called Intel Office. This software provides the same basic capability as U.S. Classified Systems. The CENTRIXS applications allow the user to access the releasable Near-Real Time (NRT), order of battle (MIDB) and imagery databases and to display the data on a map background. These applications will satisfy nearly all of the command's product and information service requirements. A CENTRIXS workstation user will be able to access browser-based products and databases, receive and display NRT track data feeds on a map background, send e-mail with attachments, and conduct collaboration sessions.

- The CENTRIXS application set will not enable secure bilateral and/or community of interest information exchanges, peer to peer data encryption, or persistent information control. These functions are referred to in general terms as security-enabled information technology. Virtual Private Network technology is one example, and is being evaluated for potential use with other defense-in-depth measures to enable secure bilateral communications over the multi-lateral network.

Long-term.

- To transition fully from an air-gapped environment for seamless, robust multilateral and bilateral information sharing, CENTRIXS will expand baseline services and infrastructure to integrate commercial multi-domain and multi-level information exchange capabilities as these technologies are developed, tested, and certified.

- Long-term for Partners. As partner nations establish mature capabilities for organically managing user computers, efforts will transition to introducing partners to on-site data servers, and building and managing local area networks. These activities will facilitate partner nations improving their contribution to the combined volume of information content for a more optimum, complete information picture.

ASSUMPTIONS

Funding and resources for hardware, software, training, Operations and Maintenance (O&M), integration, and contract support will be available.

Coalition nations will execute the required Foreign Military Sales (FMS) cases and Memoranda of Agreement (MOAs) to allow information sharing. Some coalition nations will use direct commercial sales to acquire hardware, software, O&M, and training as applicable.

Communities of Interest (COI) envisioned to install CENTRIXS at their Ministries of Defense include the Gulf Cooperation Council nations. Other nations participating in OEF may request connectivity to CENTRIXS from their homeland, i.e. NATO nations.

Security-enabled information technology products will be modified, certified, and accredited to meet USCENTCOM requirements for secure bilateral/community of interest information exchange via the multi-lateral network. Candidate technology is estimated to be available for use in an interim bilateral information exchange network solution by July 2002.

Coalition nations will be trained to proficiency and will actively access and contribute information via CENTRIXS.

Coalition nations will be responsible for management and administration of the communications connectivity and infrastructure associated with CENTRIXS from their facilities to the U.S. gateway.

REFERENCES

Chairman, Joint Chiefs of Staff (CJCS), *Joint Vision 2020*, June 2000

United States Central Command (USCENTCOM), *Strategic Concept for USCINCCENT Plan 1250-01: Engagement for the Central Region Theater*, 1 April 1999 ["Theater Engagement Plan"]

United States Central Command (USCENTCOM), *Cooperative Defense Initiative (CDI) Campaign Plan*, 22 May 2000

United States Central Command (USCENTCOM), *Coalition Command, Control, Communications, Computers and Intelligence (C4I) Interoperability Plan*, March 2001

United States Central Command (USCENTCOM), *Combined Enterprise Regional Information Exchange System (CENTRIXS), for Multinational Operations, Concept of Operations (CONOPS*), 6 December 2001.

United States Central Command (USCENTCOM), *Interoperability Senior Steering Group (ISSG), Proof of Concept (POC) III, Data Collection Summary (DCS), Coordination Draft*, 30 August 2001.

United States Central Command (USCENTCOM), *Interoperability Senior Steering Group (ISSG), Proof of Concept (POC) II, Data Collection Summary (DCS)*, 14 February 2001.

United States Central Command (USCENTCOM), *Interoperability Senior Steering Group (ISSG), Proof of Concept (POC), Data Collection Summary (DCS), 6 June* 2000.