# COMBINED ENTERPRISE REGIONAL INFORMATION EXCHANGE SYSTEM (CENTRIXS); SUPPORTING COALITION WARFARE WORLD-WIDE

**Jill L. Boardman**
Lockheed Martin Information Technologies
**Donald W. Shuey**
Department of the Air Force
USCENTCOM
7115 S. Boundary Rd.
MACDILL AFB, FL 33621 (813) 827-1291
boardmjl@centcom.mil
shueydw@centcom.mil
April 2004

## Abstract

The joint Combatant Commanders require responsive information exchange between combined forces and the joint combatant commands region-to-region for global operations. In a concerted endeavor, the combatant commands (COCOMs) and the Assistant Secretary of Defense for Networks and Information Integration (ASD[NII]) CENTRIXS Program Office (CPMO) are building a common global multinational information sharing enterprise called CENTRIXS; Combined Enterprise Regional Information Exchange System.

CENTRIXS is the premier network for coalition interoperability in support of military operations. Ongoing coalition operations continue to test and prove the viability of the CENTRIXS enterprise. Information flow to coalition partners via the multiple versions of CENTRIXS networks achieved unprecedented volume and continues to expand. CENTRIXS dissemination capabilities must become even more robust as the trend to move more command and control operations to the coalition networks continues.

CENTRIXS is designed to one day form a single, common, global, multinational data network. To achieve this goal, a certified security technology solution to allow confidential, multi-level information sharing over a single network is desperately needed. The only option today is proliferation of multiple separate networks to support the various coalition operations and bilateral exchanges. Security technology to allow separate, simultaneous communities of interest across common network transport is key to future coalition networking.

## EXECUTIVE SUMMARY

***Problem.*** Current methods for sharing operational and intelligence information with multiple communities of interest (COI) are inefficient. Security technology to allow confidential, multi-level information sharing over a single network is not yet available.

***Discussion.*** The Combatant Commanders require responsive information exchange between combined forces and the joint combatant commands, region-to-region, for global operations. In a concerted endeavor, the combatant commands (COCOMs) and the Assistant Secretary of Defense for Networks and Information Integration (ASD [NII]) CENTRIXS Program Office (CPMO) are building a common global multinational information sharing enterprise. CENTRIXS is now the premier network for coalition interoperability in support of military operations. Ongoing coalition operations continue to test and prove the viability of the CENTRIXS enterprise. Information flow to coalition partners via the multiple versions of CENTRIXS networks achieved unprecedented volume and continues to expand. CENTRIXS dissemination capabilities must become even more robust as the trend continues to move more national command and control operations to the coalition networks.

CENTRIXS is designed to one day form a single, common, global, multinational data network. To date, no security technology solution has been certified and accredited per the Department of Defense Information Technology Certification and Accreditation Process (DITSCAP) to allow confidential, multi-level information sharing over a single network. (Confidential is defined as equivalent to the protection afforded U.S. SECRET information.) Candidate security technology solutions must be fully developed and undergo rigorous technical certification and accreditation per DITSCAP before receiving approval for use on the Defense Information System Network. As a result, USCENTCOM is fielding separate Community of Interest (COI) and individual bilateral CENTRIXS networks in support of the war on terrorism and theater specific objectives. Three global and three regional, completely separate networks for coalition COI sharing are currently operational in USCENTCOM. Each network is built to the same enterprise standard, but cannot be interconnected. This separation of networks is required to prevent inadvertent release of data to nations who are not part of specific information sharing arrangements. Until sufficient guarding technology exists, nations participating in multiple networks will have to maintain separate networks tunneling through existing communications paths to ensure information integrity and confidentiality. Once an adequate guarding solution is available, the vision is these separate CENTRIXS networks will be connected (by COCOMs under supervision of a national level executive agent) to form a global CENTRIXS network.

***Recommendation.*** The future key to coalition networking is the ability to establish separate, simultaneous communities of interest across common network transport. Development, accreditation and certification of agile-algorithm Virtual Private Networks (VPN) are essential for secure COI data sharing within a broader coalition wide area network. This technology, used in conjunction with other available systems, will allow a global coalition network solution to have inclusive and dynamic membership while maintaining the appropriate security and dissemination controls required by national policies.

***"Evolution" of the technical support required to enable effective and efficient coalition operations in a net-centric environment is taking too long. COCOMs are forced to build multiple separate networks to support coalition warfare.***

## Technology Evolution Needed Yesterday!

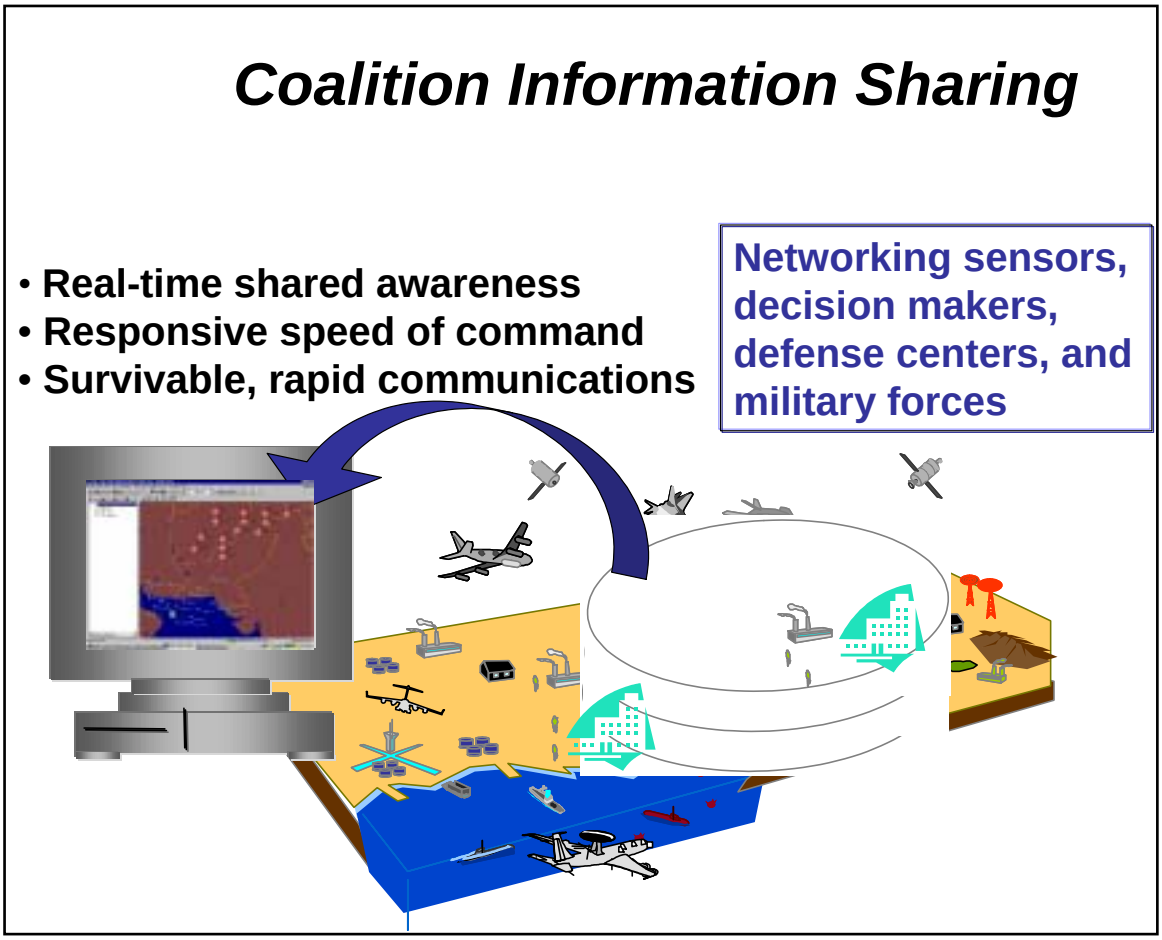
**No certified accredited technical solution that will easily combine these two worlds**
**------**
**Email, collaboration & VoIP**

- **Traditional Partners**
- **Focused on Middle East (USCENTCOM's area of responsibility)**
- **Long term Info Sharing Agreements**
- **Developed through Coalition Command and Control Interoperability Board processes**
- **Bi-Lateral networks**

- **"Community of Interest" Partners**
- **Current operations focused (OEF / OIF)**
- **Worldwide nations – many outside the AOR**
- **International coalitions**
- **"Lowest common denominator" sharing**
- **Global Counterterrorism Force (GCTF)/ Multinational Coalition Forces Iraq (MCFI) networks**

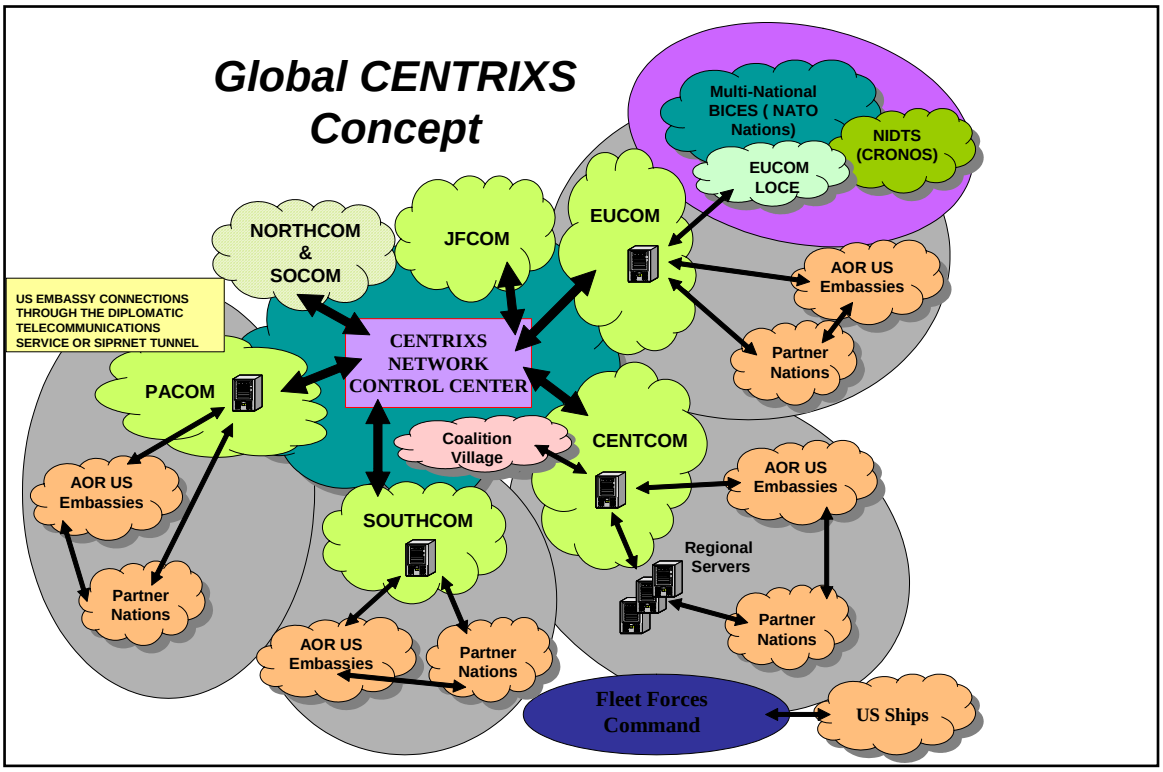
## CENTRIXS REQUIREMENT AND BACKGROUND

USCENTCOM began envisioning and exploring a coalition data-sharing network in early 1999. The primary objective for multinational information sharing was, and still is, to maintain a shared, timely, common visualization of the battlespace with our coalition and allied partners. 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; nuclear, biological and chemical (NBC) threat warning; regional military and civil air movement scheduling; battlefield campaign assessment data; force disposition; and combined force threat response data.

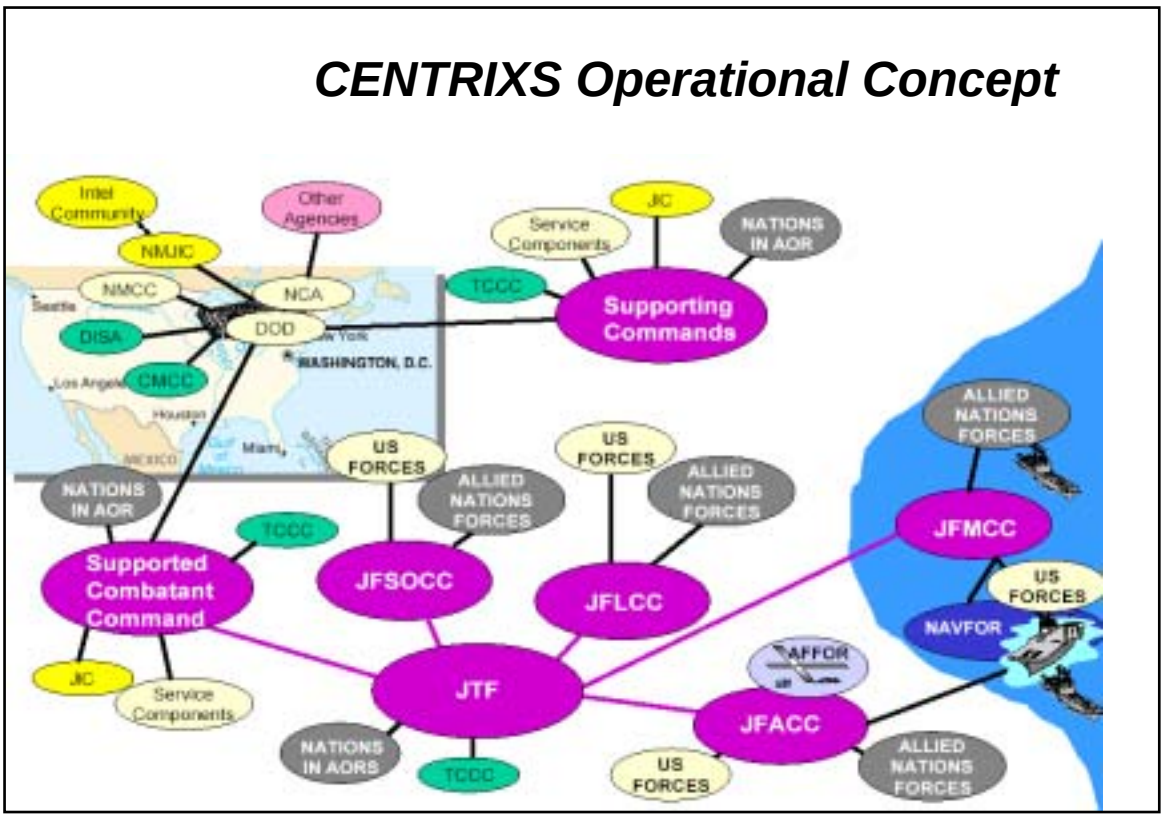



At the onset of the global war on terrorism, as USCENTCOM prepared to conduct Operation ENDURING FREEDOM (OEF) in late 2001, efforts focused on speeding the development and implementation of intelligence interoperability solutions for warfighting operations. USCENTCOM Director of Intelligence (CCJ2) 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. CENTRIXS is the Command's data network solution to support coalition operations with command, control, and intelligence information.

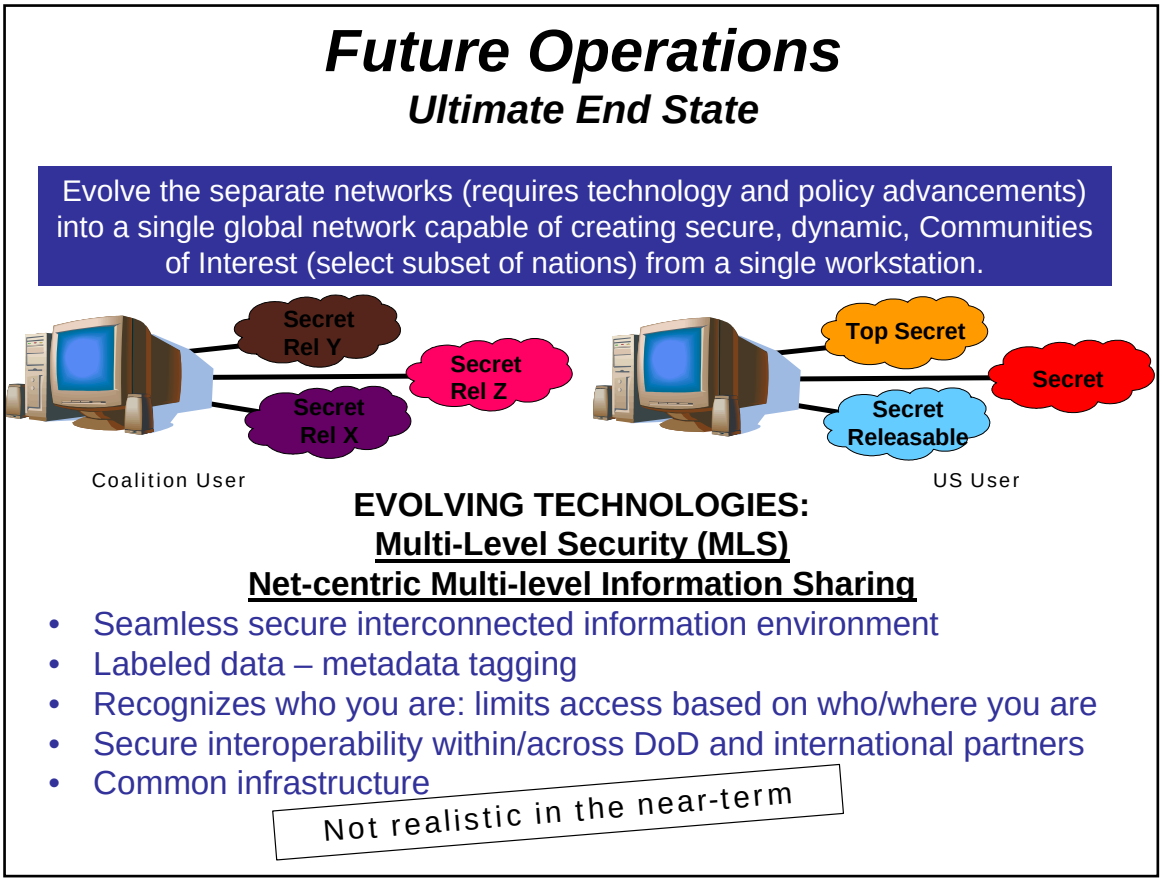
The development of a broad coalition associated with OEF led to requirements for accelerated deployment of the CENTRIXS environment at USCENTCOM Headquarters (HQ) and in the USCENTCOM area of responsibility (AOR) to include connectivity for forward deployed Service component elements. Probable expansion of OEF operations into other theater areas of responsibility (AORs) led to additional CENTRIXS gateways in U.S. Pacific Command (USPACOM) and U.S. European Command (USEUCOM).




The global nature of the war on terrorism demanded that CENTRIXS become a global multinational information sharing initiative. The Office of the Assistant Secretary of Defense (ASD) for Networks and Information Integration (NII) established the CENTRIXS Program Office (CPMO) in late January 2002 to coordinate the planning, resources, and implementation of CENTRIXS world-wide to support the combatant commands. The CPMO goal for the end of FY 04 is to establish the coalition infrastructure at combatant commands, their components, and foreign countries of interest so that a base network capability exists on which to create, and modify in near-real-time, the secure coalition communities of interest needed to meet emergent operational needs.




The end state requirement for a single global coalition network that enables secure exchanges with multiple, separate communities of interest from a single workstation was jointly articulated by the combatant commands via record message to national agencies in May 2001. After three years and increasing urgency due to world events, this requirement remains unmet.




Today, each CENTRIXS network is built to the same architectural standard but are not interconnected to prevent inadvertent release of data to nations who are not part of specific information sharing arrangements. Until sufficient accredited guarding technology exists, nations participating in multiple operations must maintain separate network terminals to ensure information integrity and confidentiality.

The future Multinational Information Sharing (MNIS) concept as laid out in DoD Instruction 8110.1, Subject: Multinational Information Sharing Networks Implementation, articulates the vision of CENTRIXS to one-day form a single, common, global, multinational data network within the Global Information Grid. This concept, however, does not address existing COCOM requirements in the short-term. USCENTCOM recently listed operational requirements in a record message (May 2004) to the Joint Chiefs of Staff J3 requesting advocacy in pressuring responsible agencies to show progress toward the long-standing requirement, as well as requesting the national community expedite the certification of cross domain solutions needed today for more effective command and control and information sharing efforts. The list of operational requirements follows:

a. Permanent web browse-down solution: SIPRNET to CENTRIXS (the limited access Multi-Domain Dissemination System (MDDS) was recently approved as an interim solution only for CENTRIXS-MCFI.) A permanent solution is not projected for another two years.

b. Cross domain chat/collaboration: SIPRNET TO CENTRIXS. A current solution is projected at the end of FY 05.

c. Reverse One Way Link (OWL) guard: CENTRIXS TO SIPRNET. A low to high file transfer between different security enclaves is not projected until FY05.

d. New generation Defense Information Infrastructure (DII) guard: between SIPRNET to CENTRIXS. A guard which allows email transfer between SIPRNET and coalition controlled CENTRIXS sites is projected for summer 2004.

e. Type 1 accredited Virtual Private Network (VPN): a type 1 VPN would allow multiple COI networks to ride the same infrastructure. No projected date has been advertised for this capability.

## *Future Operations*

*Short-Term "Way Ahead"*

Next 12 month actions:

- **Work with DoD-level agencies to integrate key-coalition member information exchange efforts**
- **Plan for multiple coalition networks to likely continue**
- **Develop/Implement a basic data tagging policy for Info Mgmt (MCFI)**
- **Continue to improve current coalition networks**
- **Continue to press hard for cross domain solutions help; guarding solutions we need now for more effective C2:**
  - Cross domain chat - Reverse OWL guard (low to high)
  - Web browse-down - New generation DII guard
  - Type 1 accredited VPN

USJFCOM made some similar recommendations as a result of their efforts to evaluate GWOT lessons learned. In November 2003 JCS tasked USJFCOM to collect and evaluate the lessons learned and to recommend material and non-material approaches for solving shortfalls. USJFCOM defined the goal of coalition information sharing as providing the ability for any member of a coalition to have timely access to releasable information. They provided specific recommendations under four general categories:

a. Change current security philosophy/policy
   - Enhance the sharing of information with foreign partners
   - Educate the warfighter on National Disclosure Policies and Implementation Procedures

b. Improve security policy implementation
   - Streamline Foreign Disclosure Implementation Process

- Streamline and standardize System Security Policy

c. Integrate technology enablers
   - Improve current multinational network standard
     - Collaboration tools
     - Language translation
   - Allow use of software encryption (i.e. Advanced Encryption Standard) on commercial off the shelf platforms for COI separation at Secret and below level

d. Develop a multi-level, secure information environment that will allow coalition partners, on-demand, to access the right information on a need to know basis.

**CENTRIXS TODAY**

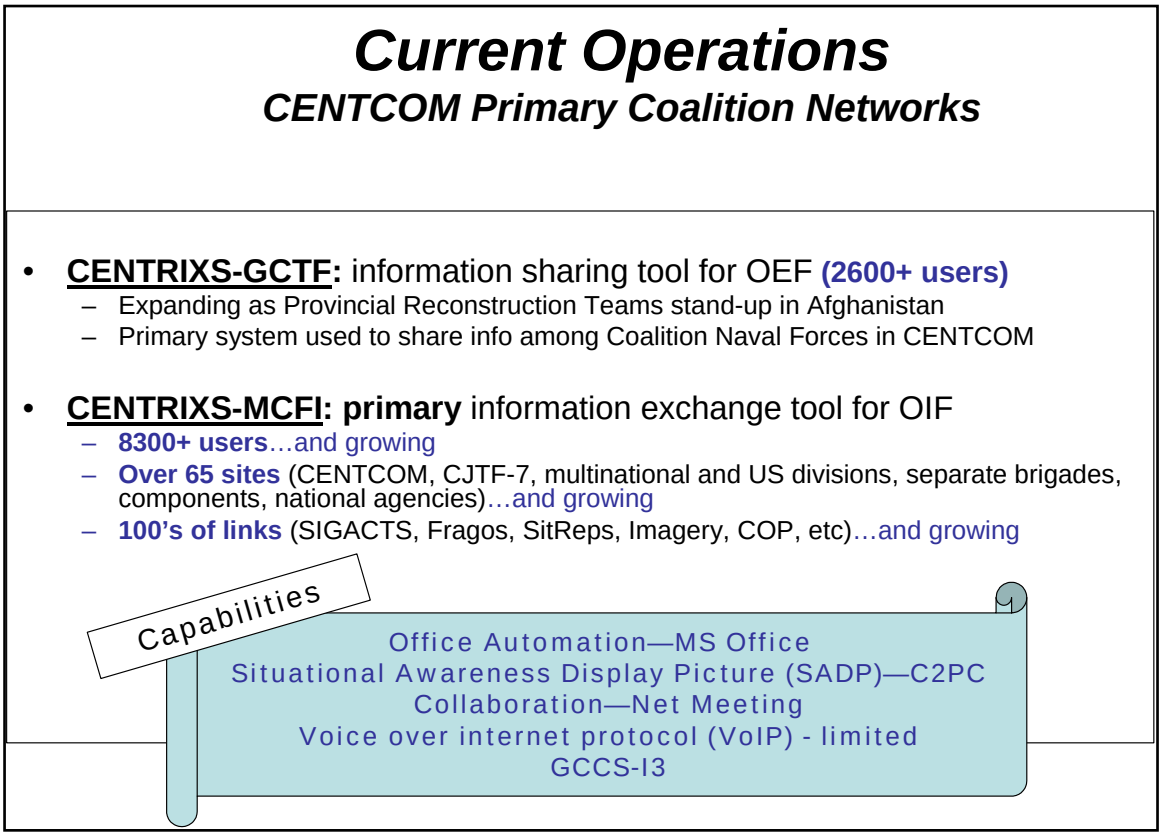
***CENTRIXS Description***. CENTRIXS is a global data network enterprise for U.S. and partner forces to share classified operational and intelligence information, region-to-region, for combined planning, unity of effort, and decision superiority in peacekeeping and contingency operations. CENTRIXS is designed to meet COCOM's requirement for day to day information sharing with multinational partners. CENTRIXS is short for Combined Enterprise Regional Information Exchange System. "Combined" refers to the combination of U.S., coalition and allied users. "Enterprise" refers to the multiple network capabilities of voice, data, and video. "Regional" is a label CENTRIXS quickly out grew. CENTRIXS will ultimately provide a seamless, interoperable, multi-classification level information exchange between the warfighting commands and key multinational players.

## *CENTRIXS Here to Stay*

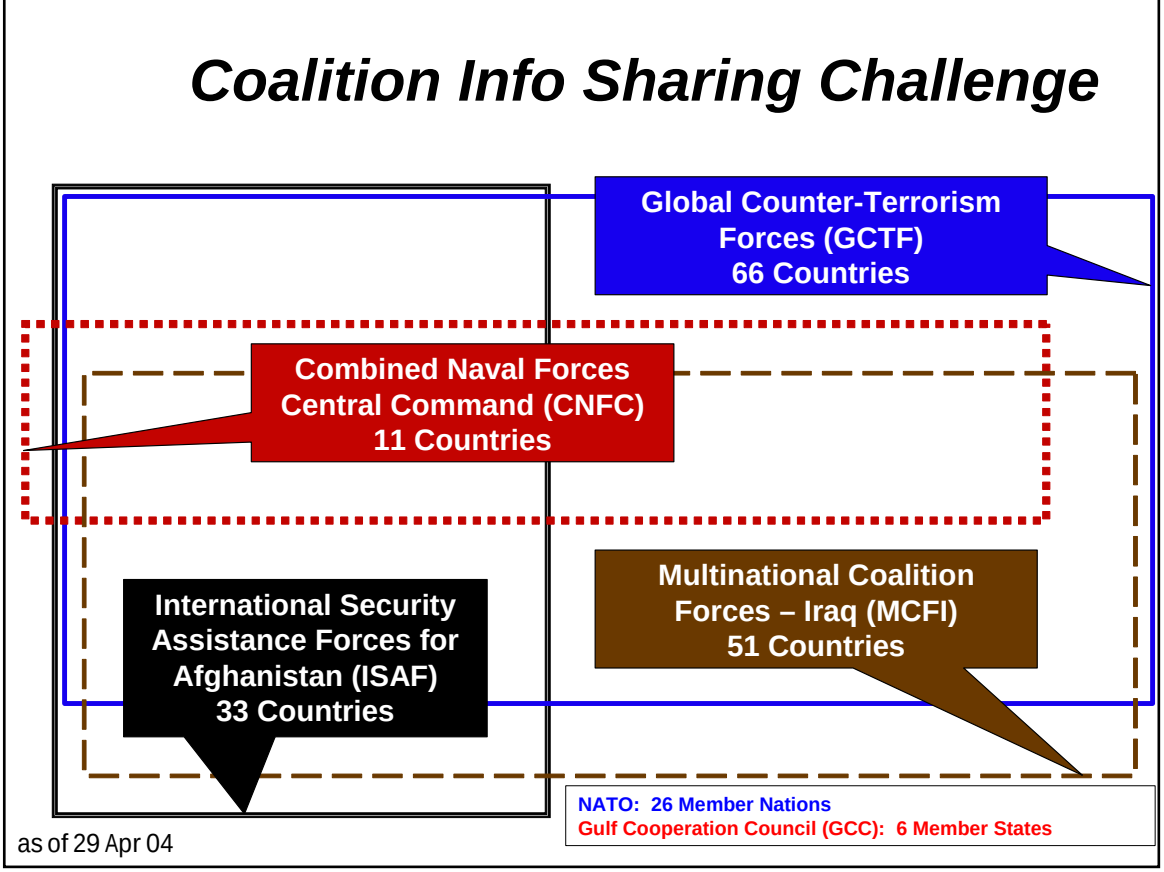
- **Current Operations:** CENTCOM relies on CENTRIXS; support must continue —it's critical to current combat operations. Major coalition partners making investments as well
- **Future Operations:** Continue to improve coalition networks and information management efforts; let DoD build/operate the network and COCOMs provide requirements and use it
- **Coalition operations will be the norm:** Policy, systems, applications, data, technology, and guarding solutions must be developed with this in mind – need the ability to operate with coalition partners in a coalition network environment

***Coalition C4I Interoperability Challenges Continue.*** 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, language difficulties, host nation technology, limited coalition infrastructure, varied proliferation of information technology and user familiarity, 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.

The current solution is for USCENTCOM to field separate COI networks and individual bilateral networks in support of the war on terrorism and theater specific objectives. The CENTRIXS-GCTF supports OPERATION Enduring Freedom and has been designated the coalition network for all maritime forces in the USCENTCOM AOR. CENTRIXS-MCFI supports OPERATION Iraqi Freedom and is the primary C2 tool/system of record for OIF security and stability operations. CENTRIXS Four Eyes (also known as CFE, CENTRIXS-X, or X-NET) supports information exchange between the United States and Commonwealth allies. It is scheduled to be the primary C2 system of record for the air component command combined air operations center by summer 2004.




For the most part, information sharing policies are adequate to support USCENTCOM's objectives. However, inconsistencies in data owner guidance from various producers, a lack of manageable technical solutions, and a cumbersome accreditation and certification process have



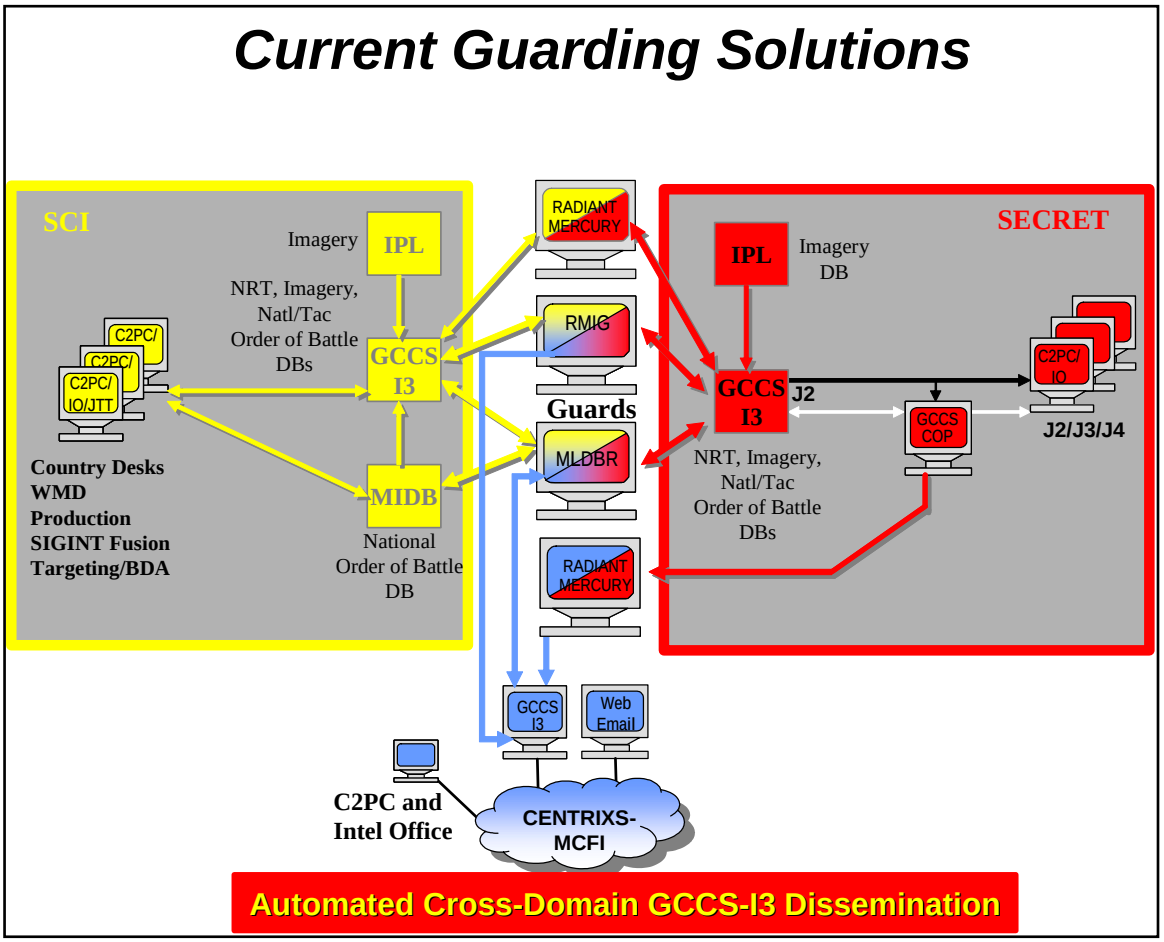

combined to frustrate seamless data dissemination via electronic networks. These problems have directly contributed to the proliferation of multiple, separate networks. The burden of additional networks has consumed limited resources and manpower and imposed an opportunity cost on USCENTCOM's coalition warfighting efforts.

Coalition forces continue to play a vital role in current, and likely all future operations in the U.S. Central Command area of responsibility (AOR). The information sharing challenge is extremely complicated with multiple coalitions, international organizations, and alliances participating in different operations. Many nations participate in multiple communities. These include the 66-nation Global Counter-terrorism Forces (GCTF), the 51-nation Multinational Coalition Forces-Iraq (MCFI), the 11-nation Combined Naval Forces Central Command (CNFC), the 33-nation International Security Assistance Forces for Afghanistan (ISAF), the 26-member nation North Atlantic Treaty Organization (NATO), as well as the traditional 6 Gulf Cooperation Council (GCC) member states and our 25 regional AOR countries. CENTCOM needs to be able to electronically share information with these various COIs quickly and efficiently to successfully conduct coalition operations.

***Information Services and Equipment.*** CENTRIXS is web-centric and commercial off-the-shelf (COTS)-focused. Implementation focuses on fielding core information services first, including electronic mail (e-mail) with attachments, web-browser-based data access, and file-sharing (office documents, text, portable document format [PDF], and image files), collaboration, and near-real time data access. These services are available for all of the current networks. The system comprises commercially available computers, and network equipment. Software applications are both COTS and government off-the-shelf (GOTS). CENTRIXS includes a web-based, thin client, multinational-releasable application set to provide the desktop and data infrastructure elements. It is a PC application set consisting of the Microsoft Office application suite, Command and Control Personal Computer (C2PC), and Integrated Imagery

and Intelligence (I3), which is also 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 NRT, order of battle and imagery databases and to display the data on a map background. A CENTRIXS workstation user is 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.

***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 with the SIPRNet, Radiant Mercury guards for formatted message text data and imagery, Multi-level Database Replication/Security Bridge for Order of battle files 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. CENTCOM uses current but limited approved guarding solutions to enhance information flow between SIPRNet and CENTRIXS.




USPACOM also continues to pursue technology insertion to improve and simplify user access to multiple, separate COI's from a single personal computer. USPACOM projects include commercial COMSEC evaluation of an agile algorithm virtual private network device, along with other technologies such as ultra thin client, common access card, biometrics and

trusted session managers. USPACOM sponsored an accredited and successful multi-COI coalition interoperability trial featuring this technology during Joint Warrior Interoperability Demonstration (JWID) 03, in JUN 03. As a result, USPACOM planned and expects to complete in FY 05, an Agile Coalition Environment (ACE) for their Joint Operations Center, Standing Joint Force HQs, service component HQs, and sub-unified HQs. The ACE end solution will allow access to multiple CENTRIXS networks from a single CENTRIXS client.

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.

## CONCLUSION

Coalition operations in support of the Global War on Terrorism will continue, as will the trend to declare coalition networks as the primary command and control systems for wartime operations. Integrating coalition members from an information sharing perspective is a huge challenge. The COCOMs need solutions today, yet most are projected years out. There is no real focus of effort or necessary investment of resources to accelerate cross-domain solutions to meet wartime requirements. Responsible agencies apply a "risk avoidance" approach and just say no to new potential solutions. By the time a responsible agency presents a solution acceptable to them, it is too late or the guarding solution is so complex that it is not feasible for the COCOM. USCENTCOM proposed a smarter "risk management" compromise and requested responsible agencies accelerate cross-domain solutions to meet wartime requirements by offering realistic “risk management” vice “risk avoidance” solutions.

The COCOMs along with the CENTRIXS Program Management Office are working together to press the national community to show progress toward the long-standing requirement to evolve the separate networks into a single global coalition network capable of creating secure, dynamic, communities of interest (select subset of nations) within the global network from a single workstation. Any guarding solution that chips away at this ultimate end-state is a step in the right direction.

## REFERENCES

Department of Defense Instruction 8110.1, *Multinational Information Sharing Networks Implementation*, February 6, 2004.

USJFCOM J8C briefing dated May 2004, titled: *OIF Lessons Learned Coalition Information Sharing*

United States Central Command (USCENTCOM), *Theater Security Cooperation Strategy*, 10 March 2003

United States Central Command (USCENTCOM), CENTRIXS Operational Architecture, 13 September 2002

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