A NATO Perspective on CENTRIXS

Introduction

The evolving nature of coalition operations is, predictably, causing evolution in the nature of the networks that support those operations. Application-specific and mission-specific networks are no longer viable with the emergence of Network Enabled Capabilities (a.k.a. Network Centric Operations), rapid reaction forces and coalitions that form and deploy quickly. Within NC3A, the development of architectures for the NATO General Communications System (NGCS), the Bi-Strategic Command Automated Information System (Bi-SC AIS), the Deployable Communication and Information System (DCIS) and the NATO Reaction Force (NRF) have been affected, and will continue to be affected by this evolution.

In the US, DOD Instruction 8110.1 "*establishes the Multinational Information Sharing (MNIS) Program within the Department of Defense; and designates the MNIS Combined Enterprise Regional Information Exchange System (MNIS CENTRIXS) as the DoD standard for multinational information sharing networks using the Global Information Grid (GIG).*"[1] The instruction indicates that " *[f]or the purposes of this Instruction "multinational" includes all interactions with foreign nations whether they be referred to as combined, coalition, allied, bilateral, multilateral, or similar terminology.* "[2] It then goes on to define MNIS CENTRIXS as including " *the CENTRIXS, the GRIFFIN (Globally Reaching Interactive Fully Functional Information Network), the CFBL (Combined Federated Battle Lab), and other MNIS network programs, as well as related cross-domain security programs associated with the sharing of information with foreign nations and forces, as an integrated MNIS solution to support the combined warfighting environment.* " [3]

While it is not clear that DODI 8110.1 has been universally embraced by all of the affected organizations and activities within the US, it is clear that CENTRIXS will have an impact on NATO architectures and operations.

[Note: This note and the accompanying diagrams have been developed from several sources and will be subject to constant revision/refinement/correction. Also, the diagrams have been developed primarily from the perspective of the Bi-SC AIS Information Exchange Gateway (IEG) / Cooperative Zone (CZ). While care has been taken to consider other NATO systems and components, omissions have undoubtedly occurred. Any contributions that would improve the accuracy or utility of the diagrams or this text would be very much appreciated.]

CENTRIXS Overview

CENTRIXS appears to be intended to build on the US Pacific Command (PACOM) and Central Command (CENTCOM) coalition infrastructure efforts, COWAN and CENTRIXS, respectively, as well as the US European Command (USEUCOM) Linked Ops-Intel Centers Europe (LOCE) system. All of these activities are overlaid on the US Defense Information Systems Network (DISN), which "*provides the wide area and metropolitan area network transport portion*"[4] of the US Global Information Grid (GIG). The GIG itself "*is the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters,*

[1] United States Department of Defense Instruction 8110.1, dated February 6, 2004; Page 1; [http://www.dtic.mil/whs/directives/corres/pdf/i81101_020604/i81101p.pdf]

[2] *ibid.*

[3] United States Department of Defense Instruction 8110.1, dated February 6, 2004; Page 15 (Enclosure 2 - Definitions); [http://www.dtic.mil/whs/directives/corres/pdf/i81101_020604/i81101p.pdf]

[4] [http://www.disa.mil/ns/disn/disn_hierarchy.html]

policy makers, and support personnel."[5] This top-level description is mostly important for setting the expectations of non-US staff who have been familiar with "getting connected to SIPRNET/DISN/GIG" as a first step in realizing information exchanges with US staff. The bottom line, though, is that **DODI 8110.1 represents CENTRIXS as the single interface between US and its coalition/treaty partners**. To understand what this means to NATO, it might be best to first get an understanding of CENTRIXS on its own.

CENTRIXS is defined in DODI 8110.1 as comprising a number of related, but somewhat independent networks and information services:

- COWAN A, which has been transitioned to CENTRIXS Four Eyes (AUS/CAN/GBR/USA);
- COWAN B and COWAN C, which appear to have been subsumed into GRIFFIN and/or CENTRIXS GCTF/CFNC or MCFI (*or may continue to be operated by US PACOM*);
- COWAN J, COWAN K and COWAN T, which continue to be operated by US PACOM;
- CENTRIXS MCFI (Multinational Coalition Forces - Iraq), which is operated by US CENTCOM;
- CENTRIXS Four Eyes (formerly COWAN A), which is operated by US PACOM;
- CENTRIXS CFNC (Combined Naval Forces Central Command), which is operated by US PACOM;
- CENTRIXS GCTF-1 (Global Counter Terrorism Force), which is operated by US CENTCOM;
- the Combined Federated Battle Laboratories Network (CFBLNet); and,
- GRIFFIN, which began as a Combined Communication-Electronics Board (CCEB) activity, but is now being developed under the authority of the Multinational Interoperability Council (MIC).

All of these operate over components of the DISN, with appropriate unauthorised disclosure protection, Community-of-Interest (COI) separation, information integrity services and availability measures. However, there are significant differences in the underlying architectural models employed in some of the components.

With respect to the operational networks (CENTRIXS / COWAN), each instantiation is composed of the network resources and the information systems required for the operation of the supported coalition, as well as the coalition information itself - **with CENTRIXS operational networks, the "network" is the destination for all information sharing/exchange**. These networks provide a suitable method for addressing PACOM's and CENTCOM's need to share information with coalition partners at the Secret level, while maintaining the integrity of US-only Secret resources like SIPRNET. However, since the set of participants is different for each coalition, each network must be operated separately**.** In some cases, this means dedicated network components and information systems, in other cases, separate information systems are shared over common network components through VPNs (Virtual Private Networks).

The Linked Operations-Intelligence Centers Europe (LOCE) network is a system operated since the early nineties by the US European Command (USEUCOM) for imagery and information sharing between the US and its NATO allies; LOCE has actually been around longer than that, but its current incarnation is rooted in the changes that occurred within the US and NATO "after the Wall came down". LOCE includes communication resources and information systems and resources like the operational CENTRIXS/COWAN systems. LOCE provides fairly robust email connectivity and web access between its user community and a number of designated NATO user and servers as well. LOCE also serves as a transport system (like GRIFFIN, described below) for interconnecting constituent organizations

[5] [http://www.disa.mil/ns/gig.html]

networks and systems, as is the case in its role with respect to the NATO Battlefield Information Collection and Exploitation System (BICES).

While the formal status of LOCE is still evolving with respect to the structures set out in DODI 8110.1, it is clear that not only was LOCE a forerunner of the systems that are called out in 8110.1, but also that LOCE fits into the MNIS CENTRIXS plan for future information sharing activities, especially with respect to NATO. Since LOCE is deployed throughout the NATO nations, it is anticipated that LOCE will be brought under the CENTRIXS program, perhaps as CENTRIXS-NATO. The significant issue for NATO is that all members of the LOCE community are from NATO Nations; the systems originally called out for MNIS CENTRIXS all include non-NATO Nations. With the exception of GRIFFIN[6], some of the constituents of the original CENTRIXS systems do not have security agreements in place with NATO that would support sharing/exchange of NATO classified information over those networks

GRIFFIN takes a different architectural approach than the other systems called out in DODI 8110.1. Originally developed among the five Combined Communication-Electronics Board (CCEB) Nations, Griffin is defined as "a permanent multinationally-developed, managed and resourced capability that enables the exchange of information between the classified networks of participating nations"[7]. That is, **GRIFFIN is a transport for information sharing/exchange, rather than a destination**. While it is not the final repository for information sharing/exchange, GRIFFIN will provide support for some applications - email (with 15 specific file attachment formats supported), web services and directory services. GRIFFIN supports multiple domains, where a domain is defined as a "common environment where participants can exchange information that is protected from intrusion from non-participants". This means that a single infrastructure can support different coalitions, with participating nations connected to multiple domains, if appropriate. Under the authority of the MIC nations - Australia, Canada, France, Germany, the United Kingdom and the United States - GRIFFIN is evolving to support coalitions composed of any set of nations.

CFBLNet is "a developing military R&D network operated by the US Joint C4ISR Battle Center (JBC)"[8]. It is "an ATM network with planned connectivity to each TTCP[9] (The Technical Cooperation Program) nation and NATO, and has the potential to offer secure high bandwidth to support TTCP experiments and demonstrations." It's most visible role is in support of the Joint Warrior Interoperability Demonstrator (JWID) experiments (*to be re-badged in 2005 as CWID - Coalition Warrior Interoperability Demonstrator*) and for experiments for transitioning prototype capabilities into operational CENTRIXS capabilities. As an experimental capability, CFBLNet enjoys some operational latitude that could not be expected on 'live' operational systems; however, system security and operations are addressed as carefully as one would expect in a fully operational system.

Given the array of resources called out under DODI 8110.1 and the differences in those resources, one of the inevitable tasks for the MNIS CENTRIXS program authority will be to resolve/rationalize the differences between the various resources called out under DODI 8110.1 and to dispel any confusion about the roles and capabilities of those resources. From the available documentation on these systems, the following picture of CENTRIXS can be inferred.

[6] At the time of this note, Australia was in the process of finalizing a security agreement with NATO; all other GRIFFIN constituents are NATO Member Nations.

[7] "Coalition Networking Strategy (CNS)"; CCEB; 23 June 2004; [*http://www.dtic.mil/jcs/j6/cceb/cnsdatedjune04.pdf*]

[8] TTCP Command, Control, Communications and Information Systems Group Web page; [*http://www.dtic.mil/ttcp/c3i.htm*].

[9] The Technical Cooperation Program - participating nations are Australia, Canada, New Zealand, the United Kingdom and the United States - see [http://www.dtic.mil/ttcp/overview.htm].

As previously noted, there are several enclaves of network and information systems components operating under the name "CENTRIXS", each supporting a different set of constituents as part of a distinct coalition. In most cases, each CENTRIXS enclave is operated as a VPN; local access within a US Command/Service/Agency (C/S/A) is provided by dedicated resources (which may include local a VPN when a common/shared network infrastructure is in place).

In each CENTRIXS enclave, access to the network and services are limited to users with bona fide clearance and Need-to-Know (NTK) for the information held/processed within that enclave, **so authorization for access to the information within a CENTRIXS enclave is implicit in being granted a connection** to that enclave. By placing only information that is releasable to all users that have been granted access to the enclave, the security requirements for implementation and operation of each CENTRIXS enclave can be met with readily available technology.

In C/S/As that require access to a single CENTRIXS enclave, a single VPN can support all CENTRIXS users easily enough. However, if access to more than one CENTRIXS enclave is required within a C/S/A, separate networks are maintained (or appropriate VPNs are provided within the local environment. Unfortunately, this can result in multiple sets of infrastructure components, raising the operations and maintenance resource requirements fir the facility in question. Users who require access to multiple CENTRIXS enclaves usually have multiple terminals. In some cases, a user with access to multiple enclaves may have a single terminal which supports periods-processing to allow access to different enclaves at different times, maintaining the separation between enclaves. Alternatively, a trusted workstation could be used to allow simultaneous access to multiple enclaves.

Two technologies are sometimes mentioned with different representations of CENTRIXS: the Multi-Level Session Server (MLSS) and the DODIIS Trusted Workstation (DTW). The MLSS - a Trusted Solaris-based system[10] - is connected on one side to all the CENTRIXS networks needed by a specific US C/S/A and on the other side to a set of (enclave/coalition-specific) Single-Level Servers, which are in turn connected to single-level clients. The advantage to this approach is that the MLSS provides a single point of control for all of a facility's CENTRIXS connections. Further, by restricting local storage of information to the Single-Level Servers and equipping end-user (client) systems with removable hard disks and assuring appropriate 'wiping' of buffer/cache space between logins (i.e., periods processing) users could access different Single-Level Servers (i.e., different CENTRIXS networks) at different times from a single workstation. In scenarios where a single multi-enclave network's management and security controls are deemed sufficient for maintaining separation between enclave, users with periods processing workstations could switch between enclaves by logging out of one domain, clearing their system of any residual data and then logging into another domain.

Unlike the sequential enclave access associated with periods-processing-based solutions to multiple enclave access, the DTW - also based on Trusted Solaris[11] - could be used to provide a user with simultaneous access to different CENTRIXS enclaves, while preventing inappropriate 'spillage' of information between the separate enclaves. While the requirement for simultaneous access might be limited, the operational convenience of being able to access different enclaves without restarting a system and swapping out the hard disk might prove irresistible.

[10] "Status of the Network"; CAPT K. Uhrich; 2004 Strike, Land Attack & Air Defense Annual Symposium, 29 Apr 04; [*http://proceedings.ndia.org/4100/Uhrich_Status_of_Networks.ppt*]

[11] "Desktop System Streamlines Analysis Work"; Henry S. Kenyon; ***Signal*** magazine; October 2004; [*http://www.afcea.org/signal/articles/anmviewer.asp?a=427*]

In addition to their CENTRIXS connectivity, the US C/S/As will continue to need GIG/DISN access (including SIPRNET) to one another and other US-classified resources. Information can be moved between the US secret environment and the Coalition environment through appropriate Content Filters (e.g., Radiant Mercury). In fact, it is conceivable that the platform supporting the MLSS or the DTW could also support a Content Filter, providing a single point of control for Coalition access and, potentially, a single terminal for US users for Coalition and SIPRNET access.

It is important to point out that, currently, these options for "reachback" connectivity to National CIS are available only to US users of CENTRIXS networks; Non-US users currently access information resources through directly connected workstations or LANs, employing the information services provided by the particular CENTRIXS enclave(s) to which they are connected. It is also worth noting that while the MLSS and the DTW (and some of the content-filtering/guard technologies, like Radiant Mercury[12]) are based on a commercially available operating system, the extensions to that base capability might be considered proprietary to the US.

The releasability of these capabilities will influence the degree of connectivity between CENTRIXS and NATO/National systems, which will affect the richness of non-US contributions to CENTRIXS-based information exchange/sharing. Realization of Network-Centric Operations/Network-Enabled Capability in a coalition environment will depend on elimination of "air-gap' and 'swivel-chair' "solutions" to the question of information exchange/sharing; network-level and system-level interconnection of non-US systems to CENTRIXS will be required, not just extension of the CENTRIXS component network VPNs into coalition partners' facilities. In the future, access via the national networks of coalition nations and access to the information systems and services on the national networks could be facilitated through a Regional Gateway, as defined under CENTRIXS. Happily for NATO, the architectures proposed for the CENTRIXS Regional Gateway closely resemble the NATO Information Exchange Gateway (IEG), NATO's approach to information exchange/sharing between NATO, its Member Nations and NATO-led Coalitions.

Figure 1 illustrates a notional US CENTRIXS architecture. Please note that the MLSS and DTW are illustrated alongside VPN-based CENTRIXS access to illustrate how they could fit into CENTRIXS installations, but that the VPN-based configuration is the norm.

The establishment of the MNIS CENTRIXS Program Management Office (PMO) within the Defense Information Systems Agency (DISA) brings all the operational and experimental CENTRIXS networks under a single technical and financial point of control. Commonality and interoperability should increase while duplication is held to a minimum. As previously noted, different coalition missions may have different participants, necessitating separate/segregated resources. And while the constituent networks that make up CENTRIXS appear to be separate, it is important to remember that they all use DISN resources as part or all of their bearer networks - consequently, DISN resources will have to increase as the number of CENTRIXS networks increases. As DISN resources are subdivided by these additional coalition networks/COIs, these increases will need to address not only the additional information traffic associated with each new coalition, but the management and overhead traffic specific to each coalition network/COI as well.

[12] "Trusted Solaris 7 Operating Environment"; [http://wwws.sun.com/software/solaris/trustedsolaris/7/ts_partners.html]

Further rationalization of the CENTRIXS resources and (some) reduction in the requirements for guard systems between US-only resources (e.g., SIPRNET) and Coalition staff can be anticipated from activities like Content-Based Information Security (CBIS) and High-Assurance Internet Protocol Interoperability Standard (HAIPIS). CBIS is slated to provide identity/role-based access control on individual pieces of data, based on encryption; this would allow data from several COIs to be stored on common systems and transmitted over common networks. HAIPIS is intended to ensure interoperability between different vendors' government/military-grade IP encryption devices, even if different degrees of protection (algorithm strength, key length) need to be employed simultaneously from one device to its various counterparts. Efforts are also underway to evolve existing user identification/authentication and authorisation capabilities to include consideration of user roles (as opposed to simply user identity) and to address access requirements that change over time. Each of these efforts may contribute to realization of true network-centric capabilities for US C4ISR systems. At the very least, the results should reduce the proliferation of separately-operated networks and systems for the various coalition operations involving the US.

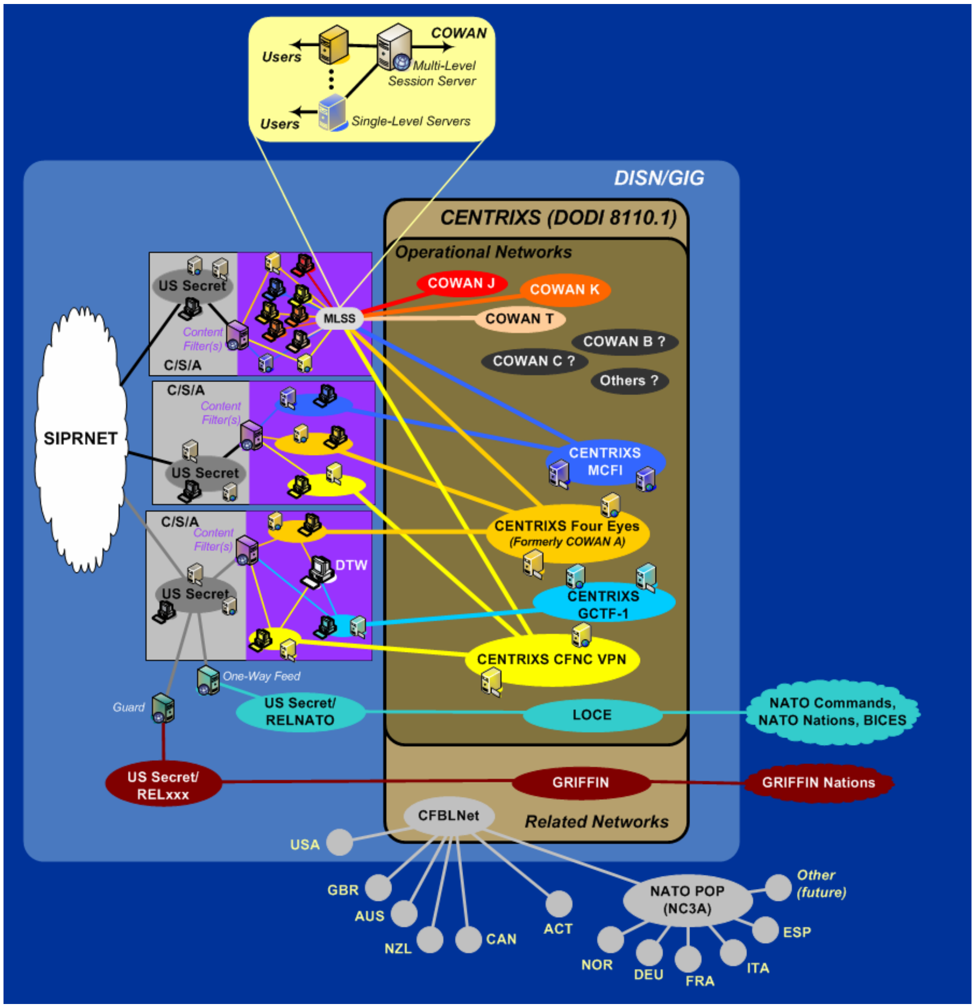

Figure 1: CENTRIXS Components

NATO CJTF Concept and Supporting Systems

The US has the financial and technical resources to pursue this approach, but NATO does not. NATO also has a different model for coalition operations, based on policy and directives developed between the 26 sovereign Nations that make up the Alliance (including , of course, the US). Consequently, NATO has had to take a different approach to coalition networks/AIS. Discovering how information exchange/sharing can be accomplished between US staff resources and those of NATO via CENTRIXS is the real challenge.

The NATO Military Committee has defined the NATO Combined Joint Task Force (CJTF) concept in MC 389/1, dated 26 June 2000. Within the constraints of the NATO C3 specification and acquisition process (*see inset*), NATO has developed several infrastructure systems in support of the CJTF Concept: the NATO General Communications System (NGCS), the Bi-Strategic Command Automated Information System (Bi-SC AIS) and the Deployable Communication and Information System (DCIS).

C3 System Specification and Acquisition in NATO

Realization of the NATO CJTF concept has been subject to some NATO-specific budget and political constraints: NATO is composed of 26 sovereign Nations, each of which has an equal voice in Alliance decisions; NATO C3 has historically focussed on **Consultation**, Command and Control versus the US DOD focus on Command, Control, Computers, Communications, Intelligence, Surveillance and Reconnaissance (C4ISR); and, crucially, the NATO C3 budget is relatively small in comparison with the US defence budget, as are the defence budgets of several of the Member Nations. (It is worth noting that ACT has recently begun to take a C4I focus as they take on the role of transformation command within NATO.)

The treaties that underpin the NATO Alliance provide an equal voice for each Member Nation in the process of building consensus for political, technical and financial decisions. The NATO C3 Board (NC3B) oversees C3 system specification and , in conjunction with the Military Budget Committee (MBC), C3 acquisition.

The NC3B is supported in its efforts by a number of Subcommittees, each of which focuses on a particular aspect of NATO C3 (e.g., Communications Systems, Information Systems, INFOSEC, etc.), developing/validating requirements statements for C3 systems and components as well as reviewing specifications and architectures as they are developed.

The MBC relies on its Working Group of National Technical Experts (WGNTE - sometimes informally referred to as '*the Wingnuts*') for assessment of the technical viability of acquisition proposals (Cost Estimates).

The NATO CIS Service Agency (NCSA) performs assessments of National candidate equipment against the requirements endorsed by the NC3B and the NATO-approved devices are selected from the successful candidates.

Unfortunately, this process can be long and the candidate equipment is not always the very best that the Member Nations have in their national inventories. This means that the capability in NATO almost always lags National capability. However, the

When it is fully deployed, NGCS will provide the basic communications infrastructure for all NATO communications. It addresses voice and data transmission requirements, circuit-switched and packet-switched, for both unclassified and classified (up to NATO SECRET) communications. Initially, NGCS will focus on delivery of NATO SECRET system-high operations, with NATO Restricted and Unclassified operations (including access to Internet resources) to be made available at a later date. NGCS will make use of a variety of transmission media and sources, with the capability to shift loads between transmission links for performance and cost considerations. The ability to dynamically manage the communications resources available to NATO is one of the key requirements of the NGCS design. The management of NGCS covers: ISDN, ATM, and SATCOM circuit allocation; security management for circuit-based and packet-based encryption devices; router and switch management; Intrusion Detection System (IDS) operation; and, a host of other tasks to numerous to list. NGCS connectivity ranges from Norway to Greece and from Norfolk, Virginia in the US to Kabul in Afghanistan. The operation and maintenance of NGCS is the responsibility of the NATO CIS Services Agency (NCSA, formerly

NACOSA - NATO CIS Operating and Support Agency), but this is just one of many systems for which NCSA has responsibility. Besides delivering a modern flexible communications system to NATO, key considerations in the NGCS design have included limiting the workload on the finite resources of the NCSA staff.

The Bi-SC AIS covers provision of Core Services for NATO fixed and deployed units (including coalition operations). Initially, these services will include web-based functions, informal messaging and directory services; formal messaging will be added in the near future. A key concept within the Bi-SC AIS design is the Information Exchange Gateway (IEG), which describes the information flow between NATO facilities and those of member Nations, coalitions (NATO-led or otherwise), peer organizations (e.g., the European Union), Non-Government Organizations (NGOs, like the Red Cross/Red Crescent) and other entities (e.g., local authorities in a coalition area of operations). The IEG is based on a set of Cooperative Zones (CZs) at NATO facilities exchanging information via agreed applications, data structures and protocols with the Member Nations and the other organizations NATO works with. That said, a CZ is essentially an extended border protection device, providing application proxies as well as firewall capability and intrusion detection services. Each non-NATO CZ will be paired with both a primary and secondary NATO CZ, allowing NATO to coordinate information exchange parameters (application / version / configuration / protocols / data structures) and to enforce some basic flow control for communications between NATO facilities and their correspondents. This last aspect is necessary to accommodate all require information exchanges within the finite resources of the NGCS; some NATO facilities have very limited communications bandwidth (particularly deployed operations) and it is more efficient to proxy/relay information to and from those facilities via other NATO facilities with more robust resources. As with NGCS, management functions of the Bi-SC AIS and the NCSA role and workload associated with those functions are a major consideration. Naturally, CZs for different interconnections will be somewhat different in configuration and operation. For example, NATO-Secret-to-NATO-Member-Nation-Secret exchanges are not expected to release label checking functions[13], while NATO-Secret-to-Coalition-Secret exchanges will almost certainly include some sort of release label checking. In both cases, though, the basic information flow will be supported through appropriately certified filter devices - filtering routers, firewalls and guards - in conjunction with proxy servers.

At its simplest, DCIS provides the components and the architecture to support Bi-SC core services and NATO Functional Services[14] (FSs) over NGCS in a deployed facility. DCIS is aimed at all deployable assets within the overall NATO CJTF concept, but has an immediate and particular concern with support to the NATO Response Force (NRF). The NRF is an evolving "coherent, high-readiness, joint, multinational force package, technologically advanced, flexible, deployable, interoperable and sustainable."[15] With a projected capability to deploy and become operational within 5 days in support of both Article 5 and non-Article 5, either as stand-alone unit or as part of a larger force, NRF is clearly the largest deployable challenge for NATO CIS. While the range of missions and operating concepts for NRF are well defined in MC 477, "Military Concept for the NATO Response Force", NRF itself is an evolving capability. While Final Operating Capability is expected in 2005, a bi-annual review and ongoing evolution is envisaged. The emergence of network-centric capabilities within NATO's infrastructure

More on Infrastructure Systems and Capabilities in NATO

The descriptions of the NGCS, Bi-SC AIS and DCIS in this note are necessarily brief, but there is significantly more information available. Interested parties may wish to contact the Chief Architect (Dr. Tom Buckman) at the NATO C3 Agency through their National NATO Representatives for further details

Documents of particular interest will include: The NGCS Reference Architecture; The Bi-SC AIS Reference Architecture and the DCIS Target Architecture.

al security devices (e.g., an application Guard) into the CZ

D transformation"; [http://www.nato.int/issues/nrf/index.html] systems and FSs will contribute to this evolution, as will the changing nature of NATO's missions.

Figure 2 illustrates these NATO infrastructure systems in relation to one another in a notional architecture, representing significant steps in the transformation evolution of NATO C3 to modern application and communications support of transformation of NATO from a Cold-War-Era institution into the Alliance's emerging set of roles and missions. However, NGCS, Bi-SC AIS and DCIS are also evolving together as intermediate steps towards a NATO Network-Enabled Capability (NNEC). A study is currently underway within NATO to determine the appropriate manner for bringing NATO's various communications and information systems capabilities together in a network-centric approach. Essentially, NNEC will transform NGCS, Bi-SC AIS, DCIS and the NATO FSs into a seamless infrastructure supporting "information pull" capability (as opposed to the traditional "information push" capability) from any point in "the NATO Grid".

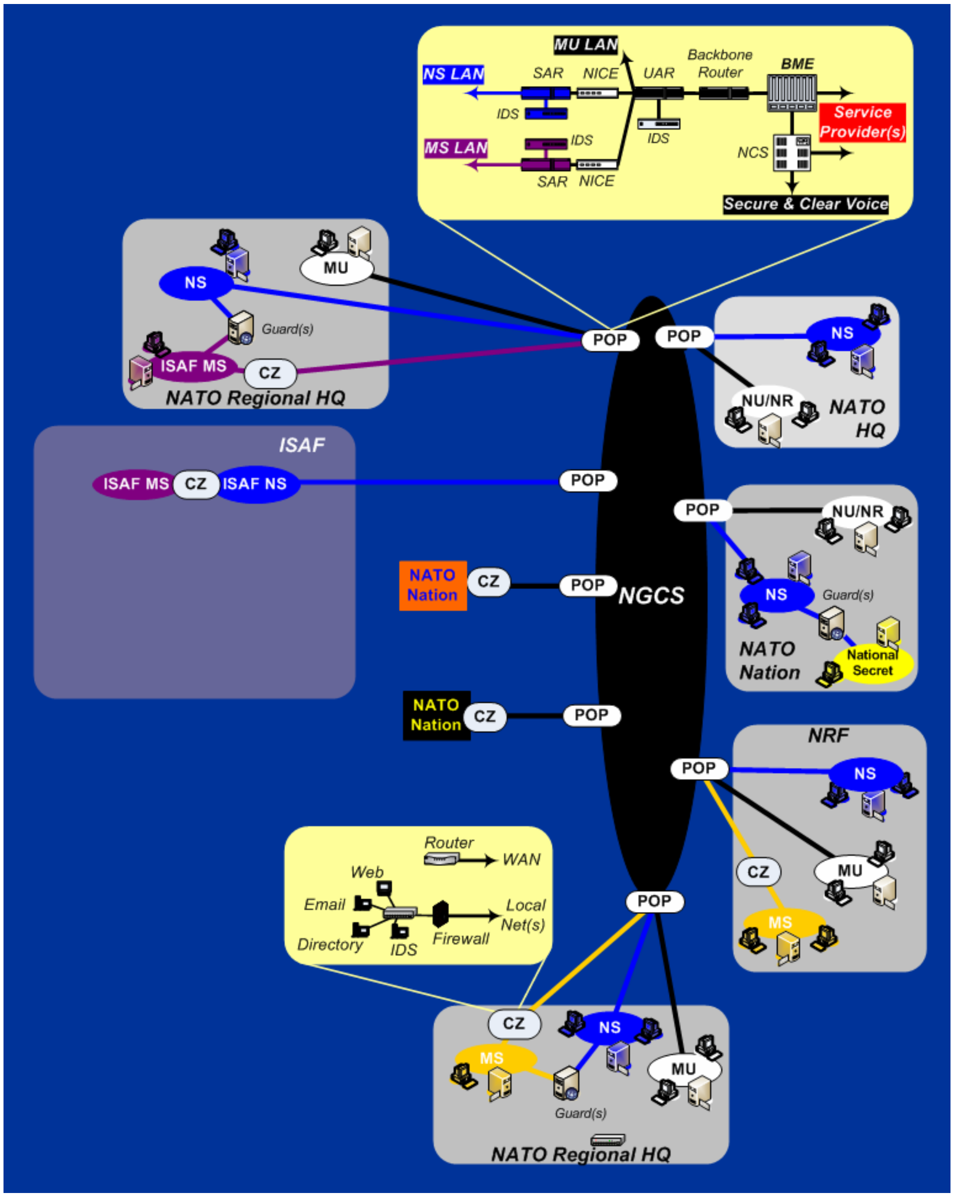

Figure 2: NATO CJTF Infrastructure Systems

One simple example of "information pull" under assessment within NATO is an OpenMap[16] java applet developed by the US Joint National Integration Center (JNIC). The JNIC applet takes air tracking information (such as one would find in a Recognized Air Picture) and allows users to request data on demand in a Web Browser via Client/Server relays (traditionally, air track display has required special client software and dedicated, server-imitated "information push" data streams).Not only does OpenMap allow users to access air tracks without specialized software, all the end user needs is the ability to discover an information source (e.g., via a link on some web page) in order to access the data - no configuration or authorization is necessary on the part of the originating server. As the output of efforts like these, along with CBIS and HAIPIS from the US and other NATO Member Nations, can be brought to bear on the NATO CJTF Concept, together with key functionality like time-variable, role-based access controls, NNEC will become a reality. The end result is envisaged as a ubiquitous communications subsystem, providing end-to-end secure transport, linking together a series of information exchange points where users will be able to locate and access information as they require it.

While the NNEC study is expected to define the transition strategy for achieving network-centric operations from the existing infrastructure systems and FSs, it is necessary, in the near-term, to understand how existing systems support information exchanges/sharing with/via CENTRIXS in the near-term.

Information Exchange Between US and NATO

Currently, information exchange/sharing between NATO and the US is primarily limited to placing a number of somewhat isolated terminals from one organizations CIS to the other organization's operations areas. The notable exceptions to this are a number of 'special' mail gateways that exist at some specific points (viz., ACO, ACT, USEUCOM and USN2F/JSF). The limited numbers of these terminals and the need to 'air-gap' information from one CIS to another make information exchange somewhat difficult. And, while these deployed terminals allow some rudimentary information exchange, this 'solution' falls well short of the capability envisaged for network-centric operations. To overcome this limitation, it will be necessary to implement network interconnections between CENTRIXS and NGCS/Bi-SC AIS/DCIS, supporting web-enabled, data-pull information sharing and user-to-user exchange via server-to-server communications.

In the CENTRIXS model, this interconnection is achieved through a Regional Gateway[17]. In the NATO model, it is achieved through an IEG and an NGCS Point of Presence (POP). In at least one characterization of email exchange between GRIFFIN[18] (one of the CENTRIXS component networks) and another coalition network, there is a remarkable similarity between the configuration and functionality of the Regional Gateway (US Multinational Space) and the IEG. It would seem that the US and NATO have actually developed similar approaches to the same problem, although there are some technical and terminology details to be sorted out:

- CENTRIXS is primarily based on multiple shared wide area networks (WAN), with all participants controlling their own interface to coalition-specific CIS resources. The NATO model is based on nationally controlled interfaces to a single NATO-managed WAN that serves as a

[16] OpenMap™ is an Open Source JavaBeans™ based programmer's toolkit for developing mapping applications from BBN Technologies; [*http://openmap.bbn.com*]

[17] JITC Interoperability Conference brief on CENTRIXS; 23 April 2003; R Radcliffe; [*http://jitc.fhu.disa.mil/iop_conf/2003/downloads/radcliffe.zip*]

[18] "The GRIFFIN Network and Coalition Information Sharing"; Lt Col D Simpson; [*http://jitc.fhu.disa.mil/iop_conf/2003/downloads/simpson.zip*]

transport network for accessing coalition local area networks (much like GRIFFIN). The NATO requirements for flow control over this shared WAN stem from realities of finite resources and the fact that NATO also employs the same WAN resources for multiple purposes, including its own internal classified CIS.

- Some discussions on CENTRIXS include the MLSS to address access within a US facility to more than one enclave via a single interface and the DTW to provide simultaneous user access to multiple enclaves. The MLSS is based, in part, on a pragmatic re-definition of the term "MLS" to mean "multiple levels of security" rather than the classic, Orange Book definition "multi-level security", combined with technology with its roots in the DIA Compartmented Mode workstation to segregate multiple coalition interfaces through a single device, the MLSS. NATO has not yet formulated solutions to meet these requirements and might be well served by considering this approach for its IEG/CZ support for multiple coalitions within a single facility.

In spite of these differences, there appears to be no significant technological impediment to coordinating the US and NATO approaches in a fashion that will support network-level interconnection between CENTRIXS networks and NATO. Figure 3 illustrates one possible approach to this resolution. Note that a single interface is illustrated for simplicity, multiple instantiations may be required to maintain appropriate separation between different CENTRIXS enclaves within NATO, assuming that access to multiple CENTRIXS enclaves is appropriate/necessary within NATO.

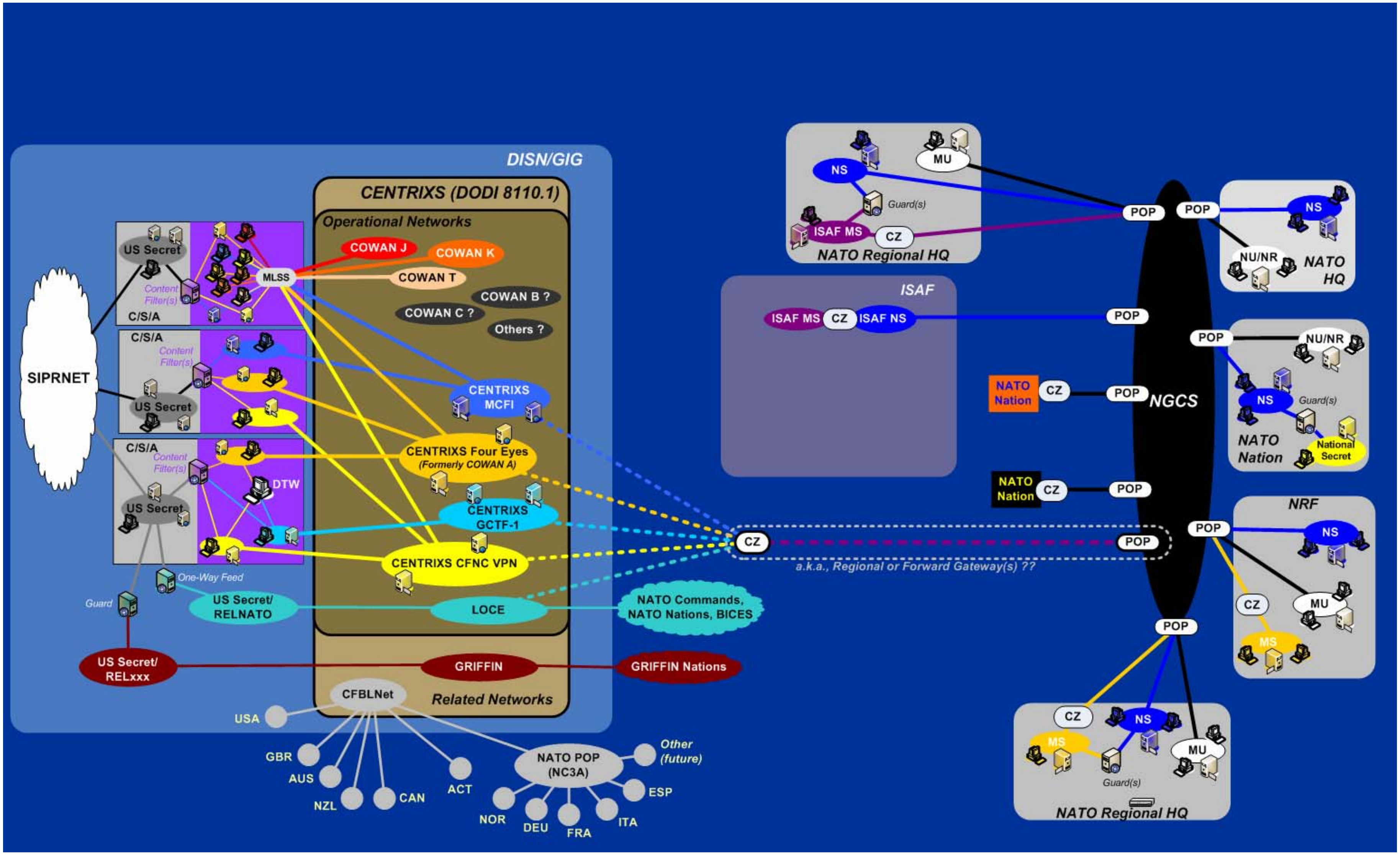

Figure 3: Potential NATO and CENTRIXS interconnection

Conclusions & Recommendations

As previously noted, the concept of a Regional Gateway is already part of the CENTRIXS architectural model. Closing the 'perception gap' between this gateway and the functionality of the IEG/CZ and the NGCS POP might be a successful approach. Additionally, integration of some of the capabilities of the MLSS into the IEG/CZ could lead to an interface that would support access to multiple CENTRIXS nets for appropriate NATO users. Whether the US/NATO integration effort occurs within an MNIS experiment or some other MNIS-sanctioned activity, this approach would appear to be the most viable for achieving information exchanges between US components and NATO components without having to resort to dedicated terminals and air-gaps.

Resolution of the differences in architectural approach of the various CENTRIXS component systems will be an item of interest for NATO. While the GRIFFIN model most closely matched the NATO CJTF architecture, the IEG can be adapted to fit the CENTRIXS operational architecture, the LOCE architecture or whatever hybrid emerges from the MNIS CENTRIXS program.

A near-term approach for information exchange employing CENTRIXS and the Bi-SC AIS IEG/CZ may be to pursue a Multinational Experiment (MNE) or a LIVEX (e.g., JTFEX 05/06) that will support transition of the IEG from an experimental activity under JWID/CWID to an operational capability on one of the CENTRIXS networks. While MNIS experiments will likely employ CFBLNet like JWID/CWID, there appears to be a fundamental difference between the two sets of activities - JWID/CWID is a technology demonstrator; MNIS experiments are focused on integration of operational capabilities. Activities employing networks that include non-NATO nations may present a challenge, but VPN-segregation may provide a suitable workaround for the purposes of experimentation and integration.

For operational US-NATO information sharing to be achieved over CENTRIXS, the endpoints (staff/location) should be identified and an appropriate information exchange (data) should be defined in support of an operational capability. Establishment of an applied research (integration) testbed within NC3A in support of a validation (demonstration) testbed at ACT may be the most expedient way of quickly transitioning capabilities from 'experimental' status to 'operational'.

While some differences will inevitably continue to exist between NATO and US approaches to coalition information exchange/sharing, it would appear that the differences may not be so difficult to surmount, particularly in light of some significant technical similarities that mostly employ different terminology. Hopefully, this note has shed some light on the differences and the similarities and the attached diagrams can serve as illustrations of the "playing field" within which information exchange/sharing requirements and solutions can be resolved.

REFERENCES

- United States Department of Defense Instruction (DODI) 8110.1; 6 February 2004; [http://www.dtic.mil/whs/directives/corres/pdf/i81101_020604/i81101p.pdf]
- "Status of the Network"; CAPT K. Uhrich; 2004 Strike, Land Attack & Air Defense Annual Symposium, 29 Apr 04; [http://proceedings.ndia.org/4100/Uhrich_Status_of_Networks.ppt]
- JITC Interoperability Conference brief on CENTRIXS; 23 April 2003; R Radcliffe; [http://jitc.fhu.disa.mil/iop_conf/2003/downloads/radcliffe.zip]
- "The GRIFFIN Network and Coalition Information Sharing"; Lt Col D Simpson; [http://jitc.fhu.disa.mil/iop_conf/2003/downloads/simpson.zip]
- "Combined Enterprise Regional Information Exchange System (CENTRIXS): Supporting Coalition Warfare World-Wide"; J.L. Boardman, D.W. Shuey [http://www.dodccrp.org/events/2004/ICCRTS_Denmark/CD/papers/003.pdf]
- Interoperability Senior Steering Group Efforts to Build a Global Data Network for Joint Coalition Warfighting"; J.L. Boardman; [http://www.dodccrp.org/events/2002/ICCRTS_Monterey/Tracks/pdf/075.pdf]
- "Coalition Networking Strategy (CNS)"; CCEB; 23 June 2004; [http://www.dtic.mil/jcs/j6/cceb/cnsdatedjune04.pdf]
- Network Multinational Interoperability Working Group (MIWG) Terms of Reference (TOR); 6 March 2003; [http://www.defenselink.mil/nii/org/c3is/ccbm/Network-TOR.doc]
- "The NATO Response Force: At the centre of NATO transformation"; [http://www.nato.int/issues/nrf/index.html]
- "Desktop System Streamlines Analysis Work"; Henry S. Kenyon; ***Signal*** magazine; October 2004; [http://www.afcea.org/signal/articles/anmviewer.asp?a=427]
- TTCP overview web page; [http://www.dtic.mil/ttcp/overview.htm]
- TTCP Command, Control, Communications and Information Systems Group ; [http://www.dtic.mil/ttcp/c3i.htm]
- "Trusted Solaris 7 Operating Environment"; [http://wwws.sun.com/software/solaris/trustedsolaris/7/ts_partners.html]
- "Griffin for Dummies"; R. O'Sullivan, September 2004
- “MC Policy on NATO’s Combined Joint Task Force (CJTF) Capability”; MC 389/1; 26 June 2000
- "The Bi-SC Deployable CIS Concept (DCC)"; AC/322-D/0069; 2 Oct 02
- “Guidelines for the Use of NATO CIS Assets and Services by NATO Nations, Co-operation Partners, and PfP Partners or International Organisations for Peacekeeping Purposes”; AC/317-N/683 (Revised); 23 Nov 1994
- “Implementation Plan for Initial Deployable CIS Capability”; SHCPI/07/09/12/02 ; 22 Mar 02
- "The Military Concept for the NATO Response Force"; MC477; 10 Apr 03
- "Support to the Development of NATO Response Force (NRF) CIS Capability"; AC/322(SC/2-WG/5)N(2004)0003 (INV); 4 February 2004
- "NATO AIS Cooperative Zone Technologies"; M. Diepstraten & R. Parker; Proceedings of the 4th NATO Regional Conference on Military Communications and Information Systems (RCMCIS); pp 207-216; October 2002

ACKNOWLEDGEMENTS

A number of my colleagues at the NATO C3 Agency have been helpful in reviewing this document as it its develop from an initial rough sketch, particularly: Chris Raynor, Jon Wilkes, Einar Thorsen, Anthony Newton and John Henwood. I would also like to acknowledge the assistance of Martin Diepstraten and Dr. Tom Buckman, also from NC3A, both of whom contributed significantly to the scope and direction of the analysis presented here.

ACRONYMS AND ABBREVIATIONS	
ACO	Allied Command, Operations (formerly SHAPE)
ACT	Allied Command, Transformation (formerly ACLANT)
ATM	Asynchronous Transmission Mode
BICES	Battlefield Information Collection and Exploitation System
Bi-SC AIS	Bi-Strategic Command Automated Information System
C/S/A	(US) Command/Service/Agency
C3	Consultation, Command and Control
C4ISR	Command, Control, Computers, Communications, Intelligence, Surveillance and Reconnaissance (USA)
CAESAR	Coalition Aerial Surveillance and Reconnaissance
CBIS	Content-Based Information Security
CENTRIXS	Combined Enterprise Regional Information Exchange System
CFBLNet	Combined Federated Battle Lab Network
CIS	Communications and Information System(s)
CNFC	Combined Naval Forces Central Command
COI	Community of Interest
COSINE	Coalition Shared Intelligence-Network Environment
COWAN	Combined Operations / Coalition WAN
CWID	Coalition Warrior Interoperability Demonstrator
CZ	Cooperative Zone
DCIS	Deployable Communications and Information Systems
DISA	Defense Information Systems Agency (USA)
DISN	Defense Information Systems Network (USA)
DODIIS	Department of Defense Intelligence Information System
DTW	DODIIS Trusted Workstation
EUCOM	US European Command
Four Eyes	AUS, CAN, GBR & USA
FS	Functional Services
GCTF	Global Counter Terrorism Force
GIG	Global Information Grid (USA)
GRIFFIN	Globally Reaching Interactive Fully Functional Information Network
HAIPIS	High-Assurance Internet Protocol Interoperability Standard
IDS	Intrusion Detection System

Acronyms and Abbreviations	
IEG	Information Exchange Gateway
ISAF	International Security Assistance Force
ISDN	Integrated Services Digital Network
JNIC	Joint National Integration Center
JWID	Joint Warrior Interoperability Demonstrator
LIVEX	Live Exercise
LOCE	Linked Operations-Intelligence Centers Europe
MCFI	Multinational Coalition Forces – Iraq
MLS	Multiple Levels of Security
MLTC	Multi-Level (multi-coalition / *multi-compartment*) Thin Client
MNE	Multi-National Experiment
MNIS	Multi-National Information Sharing
MS	Mission Secret
MU	Mission Unclassified
NATO	North Atlantic Treaty Organization
NCSA	NATO CIS Services Agency (formerly NACOSA - NATO CIS Operating and Support Agency)
NGCS	NATO General Communications System
NGO	Non-Government Organization
NNEC	NATO Network-Enabled Capability
NRF	NATO Reaction Force
NS	NATO Secret
PMO	Program Management Office
POP	Point of Presence
SATCOM	Satellite Communications
SIPRNET	Secret Internet Protocol Router Network (USA)
TITAAN	Theatre Independent Tactical Army and Air Force Network
TOPFAS	Tools for Operational Planning, Force Activation and Simulation
USEUCOM	United States European Command
USN2F/JSF	United States Navy Second Fleet / Joint Strike Fleet
VPN	Virtual Private Network
WAN	Wide Area Network

APPENDIX A: COALITION INFORMATION SHARING/EXCHANGE IN ISAF - *HOW HARD COULD IT BE?*

In the absence of a regional gateway or cooperative zone between the any of the CENTRIXS networks and NGCS, information exchange is somewhat constrained within current coalition operations. One good example is the current situation with the International Security Assistance Force (ISAF) in Afghanistan.

Each of the organizational elements participating in ISAF brings their own CIS capability to ISAF. In the case of the Dutch-German Corps, this means TITAAN (Theatre Independent Tactical Army and Air Force Network) and the information systems (e.g., messaging, database, air picture, ground picture, logistics support, intelligence support, etc.) employed by that group. NATO brings its own network and information systems to the coalition and the US brings the CENTRIXS Combined Naval Forces Central Command (CNFC) virtual private network (VPN) and the information systems associated with that network.

Limited information sharing/exchange is realized through a series of ad hoc measures. Both NATO and the US offer terminals for accessing core services in their respective coalition CIS. While this measure does provide access to the messaging systems, file store and web sites that have been set up in support of coalition operations, it does not address the requirement for information exchange/sharing between the coalition systems and the systems normally used by the Nations and the units that they deploy in support of coalition activities. In some cases, special circuits and systems (e.g., mail guards and data diodes) have been set up to accommodate limited information exchange/sharing, but these are subject to constraints in terms of the range of applications and data formats that are supported, frequently due to the security policies and analyses associated with the special circuits. And in any coalition scenario, there are inevitably a number of informal, opportunistic information exchange/sharing channels. Unfortunately, these are frequently based on systems and components that were not designed (or approved) for this use and their successful operation is based on capabilities and relationships specific to a few individuals; when those individuals rotate out of coalition duty, the access, knowledge or agreements that they used to support the information exchange/sharing goes with them. Figure A-1 illustrates the some examples of these sorts of ad hoc measures that can be found between the US (white arcs), NATO (bright green arcs) and other coalition nations (orange arcs) in ISAF today.

In essence, these ad hoc measures work, but the range of information sharing/exchange is limited. Email is the most common exchange mechanism, with non-message-based information (e.g., briefings, formatted documents and illustrations/graphics images/pictures) getting sent from one user to another as attachments. Unfortunately, the exchanges are sometimes limited by the capabilities of the underlying systems (e.g., maximum attachment size), accreditation constraints on the type of file that can be attached and the (lack of) speed associated with the store-and-forward/relay nature of email systems. Compounding these technical limitations, these 'workaround' exchanges are also predicated on the recipient knowing that the information exists and having/acquiring the email address of the sender before the information can be requested. In the case of exchanges across security domains, the sender must also validate the releasability of the information requested before "pushing" it out to the recipient.

Clearly, this is not the sort of information sharing/exchange infrastructure that will be required for NNEC. In a "better world", information sharing/exchange would be facilitated by connecting these various networks and information systems together in some fashion that would not compromise the security or operational integrity of the component systems; users would be able to discover/locate information and "pull" it without the intervention of another party. Both the CENTRIXS regional gateway and the NATO IEG/CZ are intended to facilitate just such a set of connections.

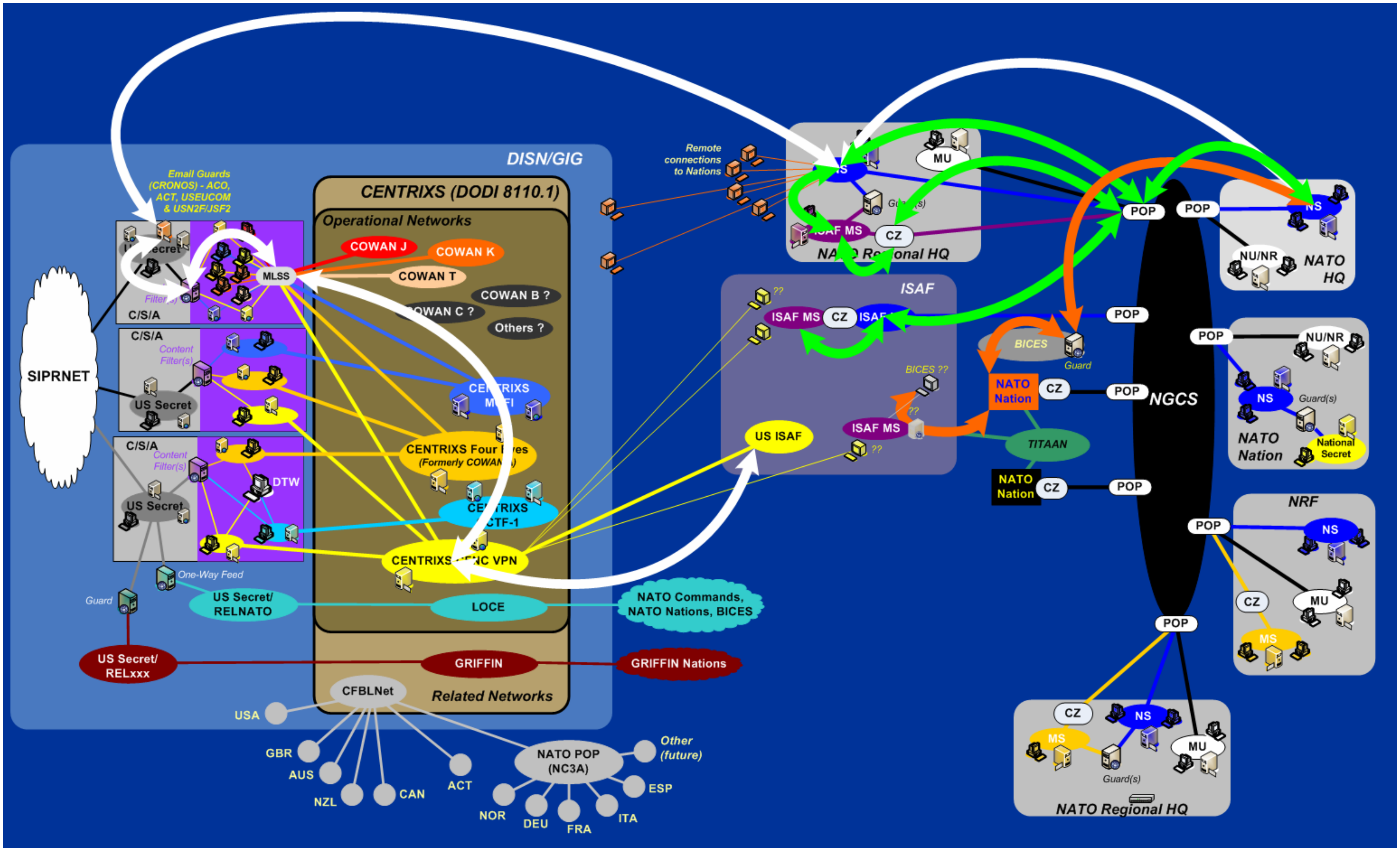

Figure A-1: (Lack of) NATO-CENTRIXS Connectivity within ISAF