Spring 2008

Information Sharing Solutions for Nato Headquarters

Wade Alarie
Regis University

Regis University
College for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

Information Sharing Solutions for NATO Headquarters

Wade Alarie

Regis University

School for Professional Studies

Master of Science in Computer Information Technology

Regis University

School for Professional Studies Graduate Programs

MSCIT Program

Graduate Programs Final Project/Thesis

Certification of Authorship of Professional Project Work

Print Student's Name: Wade Alarie

Telephone: 613-231-4458 Email: wade@joana.ca

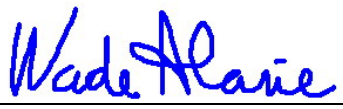
Date of Submission: 25 April 2008 Degree Program: MSCIT

Title of Submission: Information Sharing Solutions for NATO Headquarters

Advisor/Faculty Name: Daniel Likarish

Certification of Authorship:

I hereby certify that I am the author of this document and that any assistance I received in its preparation is fully acknowledged and disclosed in the document. I have also cited all sources from which I obtained data, ideas or words that are copied directly or paraphrased in the document. Sources are properly credited according to accepted standards for professional publications. I also certify that this paper was prepared by me for the purpose of partial fulfillment of requirements for the Master of Science in Computer Information Technology Degree Program.



25 April 2008

Student Signature *Date*

Regis University

School for Professional Studies Graduate Programs

MSCIT Program

Graduate Programs Final Project/Thesis

Authorization to Publish Student Work

I, Wade Alarie, the undersigned student, in the Master of Science in Computer Information Technology Degree Program hereby authorize Regis University to publish through a Regis University owned and maintained web server, the document described below ("Work"). I acknowledge and understand that the Work will be freely available to all users of the World Wide Web under the condition that it can only be used for legitimate, non-commercial academic research and study. I understand that this restriction on use will be contained in a header note on the Regis University web site but will not be otherwise policed or enforced. I understand and acknowledge that under the Family Educational Rights and Privacy Act I have no obligation to release the Work to any party for any purpose. I am authorizing the release of the Work as a voluntary act without any coercion or restraint. On behalf of myself, my heirs, personal representatives and beneficiaries, I do hereby release Regis University, its officers, employees and agents from any claims, causes, causes of action, law suits, claims for injury, defamation, or other damage to me or my family arising out of or resulting from good faith compliance with the provisions of this authorization. This authorization shall be valid and in force until rescinded in writing.

Print Title of Document(s) to be published: Information Sharing Solutions for NATO Headquarters.

Wade Alarie — 25 April 2008

Student Signature — *Date*

Check if applicable:

_____ The Work contains private or proprietary information of the following parties and their attached permission is required as well: _____

Name of Organization and/or Authorized Personnel

Regis University

School for Professional Studies Graduate Programs

MSCIT Program

Graduate Programs Final Project/Thesis

Advisor/Professional Project Faculty Approval Form

Student's Name: Wade Alarie Program: MSCIT

PLEASE PRINT

Professional Project Title: Information Sharing Solutions for NATO Headquarters

PLEASE PRINT

Advisor Name: Daniel Likarish

PLEASE PRINT

Project Faculty Name: Daniel Likarish

PLEASE PRINT

Advisor/Faculty Declaration:

I have advised this student through the Professional Project Process and approve of the final document as acceptable to be submitted as fulfillment of partial completion of requirements for the MSCIT Degree Program.

Project Advisor Approval:

D. M. Likarish

4/3/2008

Original Signature *Date*

Degree Chair Approval if:

The student has received project approval from Faculty and has followed due process in the completion of the project and subsequent documentation.

D. M. Likarish

4/3/2008

Original Degree Chair/Designee Signature *Date*

Abstract

NATO is an Alliance of 26 nations that operates on a ***consensus basis***, not a ***majority basis***. Thorough and timely information exchange between nations is fundamental to the Business Process. Current technology and practices at NATO HQ are inadequate to meet modern-day requirements despite the availability of demonstrated and accredited Cross-Domain technology solutions. This lack of integration between networks is getting more complicated with time, as nations continue to invest in IT and ignore the requirements for inter-networked gateways. This contributes to inefficiencies, fostering an atmosphere where shortcuts are taken in order to get the job done. The author recommends that NATO HQ should improve its presence on the Internet, building on the desired tenets of availability and security.

Acknowledgement

First, I would like to acknowledge the support of my wife Diane, as always, helping me to confront challenges and forge ahead with my education and my career.

Second, I would like to acknowledge the support of my employer, the Canadian Department of National Defence, who completely paid the financial costs of pursuing the MSCIT degree at Regis University and on occasion, even allowed me free time to work on my studies.

Last, I would like to thank my Academic Advisor, Assistant Professor Dan Likarish for his support in reviewing manuscripts and suggesting changes to make this document suitable as an MSCIT Project.

Revision History

Revision	Date	Description
1.0	21 February 2008	1st draft submission
2.0	5 March 2008	2nd draft, editorial changes
3.0	25 April 2008	3rd draft, following peer review

Table of Contents

Information Sharing Solutions for NATO Headquarters

The North Atlantic Treaty Organization (NATO) is an Alliance of 26 member nations that operates on a ***consensus basis***, rather than a ***majority basis***, as found in most democratic countries or organizations (the United Nations for example). The political Headquarters (HQ) of NATO is situated in Brussels, Belgium, where nations are represented by staffs of military and civilian specialists and diplomats. Complete and rapid exchange of data between nations (through both their deployed representatives in Brussels and other representatives that reside at the national capitals) and NATO staff members, and amongst nations is critical to the Business Process at the HQ. The ultimate goal is to build consensus and maintain the strength of the Alliance. Although this statement is well understood by nations' Ministries of Defense (MoDs), Ministries of Foreign Affairs (MFAs), and National Representation at NATO HQ in Brussels, Belgium – there are still noticeable information exchange deficiencies, particularly evident now with the availability of modern Information Technology (IT). If NATO and nations relied on the Internet, for example, they would be able to exchange email, develop policy material using wikis and web forums – not relying on real time interaction. Even instant messaging could be used, but there would be time zone limitations, as National Representatives need to engage with their counter-parts resident in national capitals on a frequent and recurring basis. However, the Internet would likely be found lacking adequate protection for some classified information sharing ("Common Security Vulnerabilities in e-commerce Systems", n.d.). NATO HQ needs to adopt technical solutions to enable information sharing on all networks.

A significant information exchange problem exists at NATO HQ detracting from the key business process of building consensus – and this can be mitigated through the use of available Cross-Domain technology solutions.

The need for this project became evident during the author's posting to NATO HQ in Brussels, employed in one nation's Delegation during the period July 2003 to July 2007. During this timeframe, the author challenged the issue of how the NATO HQ IT infrastructure was unable to contribute effectively to the business process. It appeared as though modern IT was in place only to replace typing pools and secretarial resources, whereas the obvious advantages of powerful networking strategies were missing. To be clear, the author's responsibility was to a single nation, whereas nearly 1,000 personnel work at NATO HQ *for the organization* as a whole. In a sense, the author was only a participant in the process and certainly not directly responsible for obtaining consensus. The author experienced first-hand the frustration with antiquated *cylinders of excellence*, as many staff members described them, stove-piped special purpose single-nation networks. NATO staff have considered the requirement for an overarching solution vis-à-vis Information Exchange Gateways (IEG) connecting the NATO classified domain with similar national domains (Diepstraten and Parker, 2003, p.1), but implementation of practical solutions are not forthcoming in the near term.

This project starts with an explanation of the business process at NATO, why it is different than many organizations and why technological solutions need to be implemented without delay. The paper will describe an existing information exchange problem and prescribe solutions based on research and literature review. Due to the obvious need to protect classified information concerning NATO and national networks, detail will be limited to the same level as

what currently exists in the public domain (“North Atlantic Treaty Organization”, 2006). Obviously, standard office footprints are currently affected by the proliferation of stove-piped networks. Some staff work in a single office where as many as five different networks are terminated. The lack of integration between networks is getting more complicated with time, as nations continue to invest in IT and ignore the requirements for inter-networked gateways. There are current, tested and accredited solutions in existence, some meeting partial requirements, some potentially satisfying the full requirement, but as well, there have been complications in their installation and maintenance. The use of HTTPS, for example, is an excellent example, and one that is in current use with banks. However, this relies upon the basic existence, omnipresence and availability of the Internet, the assurance of which may not be sufficient for NATO’s requirements. The past decades have seen several nations invest vast amounts of resources in the quest for true Multi-Level Security (MLS), but unfortunately, this technology is still not sufficiently mature for deployment. In the conclusions, the author will summarize the results and make recommendations to adopt readily available technological solutions. Finally, at the end of the paper, the back matter will include a glossary of terms and abbreviations, primarily *NATO speak*.

Chapter 1 – Review of Literature and Research

During the author’s tenure at NATO HQ, he gained first-hand experience with the business processes and use of technology in support of NATO and National staffs. The experience he gained constituted primary research conducted through meetings, briefings, conferences and review of requirements and engineering documents covering the issue of

Information Exchange Gateways (IEG), not only at NATO HQ but also throughout the entire command structure.

The attached Annotated Bibliography details a comprehensive literature review of sources available in the public domain. Kriendler, a Professor of NATO and European Security Issues at the George C Marshall European Center for Security Studies, is a former member of the NATO International Staff. His paper on NATO transformation is considered essential to confirm the De facto NATO business process of building consensus, prior to examining any potential technological solutions. Several well-known authors have published books espousing the need for change, inspiring subsequent transformation of Command and Control processes and supporting technology advancement in many nations. In particular, the authors Alberts, Gartska, Hayes, Signori, Atkinson and Moffat are well renowned experts in the area of network enabled information systems and their works have contributed to building the case for transformation, at Chapter 3. Admittedly, there still remains a vast amount of information restricted in distribution, although this mostly deals with Multi-Level Security (MLS), and in particular, detailed network configuration and encryption methods – not determined necessary for this paper.

While the ultimate goal will be one that supports MLS, one-way Data Diodes and cross-domain technical security guard solutions currently exist and have been deployed by several nations. Diepstraten and Parker, Principal scientists with NATO have written in open literature their views on obtaining network architecture constructs that build on the federation of networks, moving towards a reduction of stovepipes. They are unbiased technical experts, recognized in their national environments (The Netherlands and The United States) for information system development, vulnerability analysis and integration projects. The problem of connecting NATO

classified systems to National classified networks is not unique. Some countries have already established limited bilateral solutions to satisfy unique requirements for information exchange, particularly in coalition operations. They are often employed on a case-by-case basis ("Cross-Domain Solutions", n.d.).

The Internet contains sufficient detail on military exercises, technology demonstrators and cooperative programs in the pursuit of improved interoperability amongst Allies. Crocker, a General Dynamics Information Assurance Technical Lead, has cited definite limitations and recognizable flaws in continuing to pursue solutions that build on cross-domain technical security guards. His work has helped to establish boundaries for Chapter 6, and the requirement to seek alternative solutions at Chapter 8. Dr Reed, a Division Staff Engineer at the Mitre Corporation, has also produced works that help to define the construct of Security Guards for a future web environment.

By drawing attention to the need for cross-domain solutions and improved formal networking, this paper should be of interest to NATO HQ staff and NATO member nations, reflecting on the potential added value to the business process.

Chapter 2 – Business Process at NATO HQ

As an organization, NATO was founded in 1949: an Alliance of like minded nations committed to the high level security concepts of "democracy, individual liberty, the rule of law and the peaceful resolution of disputes, and promotes these values throughout the Euro-Atlantic area" ("North Atlantic Treaty Organization – Homepage", n.d.). NATO's membership has grown in recent years to 26 nations, each with the same weight. Why – *with the same weight*? As an Alliance, NATO is committed to reaching consensus on its policies, training and

operational activities. Decision-making at NATO is founded on the principle of achieving consensus. As a rule, voting does not occur where nations formally express their positions. Nations work together with the staff component of the HQ, and equally important, the representatives of other nations, in order to build consensus through dissemination of information and consultation. "Consensus has been accepted as the sole basis for decision-making in NATO since the creation of the Alliance" ("Consensus Decision Making at NATO - A Fundamental Principle", n.d.).

An informal network for achieving consultation has existed since 1949, not built with IT, but rather through the committee structure, a basis for consultation. It starts with the North Atlantic Council (NAC). Each nation has one representative at the NAC (an Ambassador), with the Secretary General acting as the Chairman. NATO staff members work in administrative support of this highest-level committee producing agendas, publishing decision sheets, maintaining task lists and arranging for presenters. All other committees, sub-committees, working groups and ad-hoc working groups follow a similar modus operandi. In some cases, a NATO staff member will be the Chairman, and in other cases a nation may take on the responsibility. The detail is irrelevant. What is important to understand is the basic requirement to achieve consensus and the fact that nations and NATO staff members are deeply committed to the consultative process in order to be successful.

At its most basic level, the consultative process involves "simply the exchange of information and opinions" ("The Consultation Process - Reaching Consensus", n.d.). All nations are represented at NATO HQ by Delegations; some are joint or combined Delegations that are comprised of military and diplomatic specialists, whereas some nations may use two separate

entities, focusing on political or military affairs. The two highest-level Committees are the NAC (as mentioned above) and the Military Committee (MC). Therefore, each nation is at least represented at the NAC and the MC through an Ambassador and a Military Representative (a General Officer). The process of consultation is continuous, and both formal and informal decision-making relies upon the on-site representation and availability of nations' and NATO staffs.

The technological advances available to be utilized in support of networking and decision-making are something that is of interest to Alliances, like NATO, and equally to the understood asymmetric threat. Unfortunately, concerns have been expressed that NATO may not be up to the challenge of timely decision-making. Lord Robertson, a former Secretary-General of NATO remarked, "…in an age where threats give little warning before they strike, NATO suffered from the perception in some circles that its consensual decision-making culture was too slow and cumbersome to deliver in time" (Robertson, 2004, p. 30). There are essentially three elements to this term decision-making (Kriendler, 2005, p.7):

1. The requirement to actually *reach consensus* (in some cases, this may not be possible due to national interests);
2. The *decision-making process* at NATO HQ, including the necessary staff and administrative support that goes into the process (meetings, documents, presentations, witnesses, records, consultation); and
3. Interagency *processes in national capitals* and the requisite democratic parliamentary activities that may take place (this is most often the case when a decision to employ forces is taken).

It is beyond the scope of this project to deal in particular with element 1, above, although technological solutions to support NATO's business process are certainly available to directly support element 2, with follow-on support for elements 3 and 1. Despite rumors to the contrary, "there is agreement by Allies that consensus decision-making will be preserved" (Kriendler, 2005, p.9). Deeply rooted in the business process at NATO is the *silence procedure*, a process that builds consensus through silence – an odd, but efficient concept. The way it works is that nations are considered to agree to a policy, procedure or statement – when they do not *break silence* and speak against the issue (before the closure date/time). Herein lays the importance of efficient, effective and thorough distribution and review of documents. NATO clerical staff will initially distribute a draft document to nations through their delegations on-site in Brussels. Delegation staff will peruse the paper and when/if necessary transmit the document back to national experts in their capital to determine a national position on the subject. It would be very difficult for on-site staff to competently develop national positions on these issues, since most often they become intricately entwined with national projects or operations. Consider, for example, a NATO policy on when the Alliance should transition to IPv6 on networks. Delegation staff members must consult with their counterparts in the capitals, otherwise they may end up committing their nation to a policy that forces adoption of a protocol years in advance of when it is programmed by national project managers.

Nations have the right to enact their own laws to define security classifications. The US, for example, defines three levels at Top Secret, Secret, and Confidential ("Executive Order", n.d.). In addition to these distinct classification levels, other terms like *For Official Use Only*, have gained common usage, at least in the USA. Thirty years ago, NATO papers were just that –

papers. National staff used the telephone and fax machines considerably more than today. However, times have changed and although nearly all official correspondence is still passed to nations on paper, there is more and more push of draft and official documents through internal email and file transfer over the MINERVA classified LAN (at NATO Secret). To support this process is a Document Management System (DMS) in place at NATO HQ in Brussels - a Hummingbird application on MINERVA. National clerical staff constantly receive a push of documents placed on the DMS. Since there are air gaps between the NATO and national networks, emails and DMS documents must be extracted on removable media and inserted into the appropriate networks for onward distribution to national capitals.

It would be extremely difficult to describe how each of the 26 nations makes contact with their capitals, and it would be equally hard to provide a pattern for a generic or average delegation. However, it is a useful exercise, in support of this paper, to describe what means of connectivity a national delegation might have. Recall that each nation is represented by both military (Ministry of Defense or MoD) and diplomatic staffs (Ministry of Foreign Affairs or MFA), or State Department – to use an American term.

To visualize the networks in use, it is best to first start with the NATO networks. NATO first deployed a Secret WAN in December 1995, responding to the needs of NATO's first outside area operation in the history of the Alliance – IFOR (the Implementation Force in the Balkans). This initial WAN is still in place today and permeates throughout the NATO command structure and is terminated at each nation's capital with only two workstations. Plans to introduce more workstations and/or interfaces to national networks will be discussed later. A second network often commonly available in the capitals is the Battlefield Information

Collection and Exploitation System (BICES) – a WAN that shares intelligence data posted by the *NATO plus* nations that use it. While most national capitals have only two NATO Secret (NS) WAN workstations, most have dozens of BICES workstations. However, it would be poor practice for any nation to send its material describing draft national positions on either BICES or the NS WAN, until it became official. It is important to understand that material available on either of these NATO systems is *available for the use of all nations.*

Nations are likely to use whatever means they have at their disposal in order to transfer data back to their capitals. The Internet, for example, is surely to be found in most delegations, but likely not pure Internet, but reachable through national gateways and firewalls from either a national defense or diplomatic network, one protected by web proxy servers and Intrusion Detection Systems (IDS). Most nations will have to rely upon at least one national classified network in order to facilitate the consultation process with their capitals. Figure 1 illustrates what networks might be found in a delegation, together with access to the NATO HQ classified network – MINERVA. Networks available to the NATO staff members won't include any national systems, but usually will include access to the Internet through a separate unclassified LAN. Therefore, in the worst case, national representatives may have five networks terminated in their office and NATO staff members will likely have only one or two networks.

MINERVA supports the business process. A year ago, NATO staff made the startling discovery that 85% of MINERVA traffic was only at the NATO Restricted (NR) and below level (handled in the same manner as the USA treats For Official Use Only), far lower than what it is accredited for. This statement is also likely valid for network traffic on the NS WAN, the only NATO WAN. There is no other NATO WAN. Therefore, there is no common email directory

or DNS structure in place to support an unclassified or NR WAN. Users throughout the command structure rely on the NS WAN.

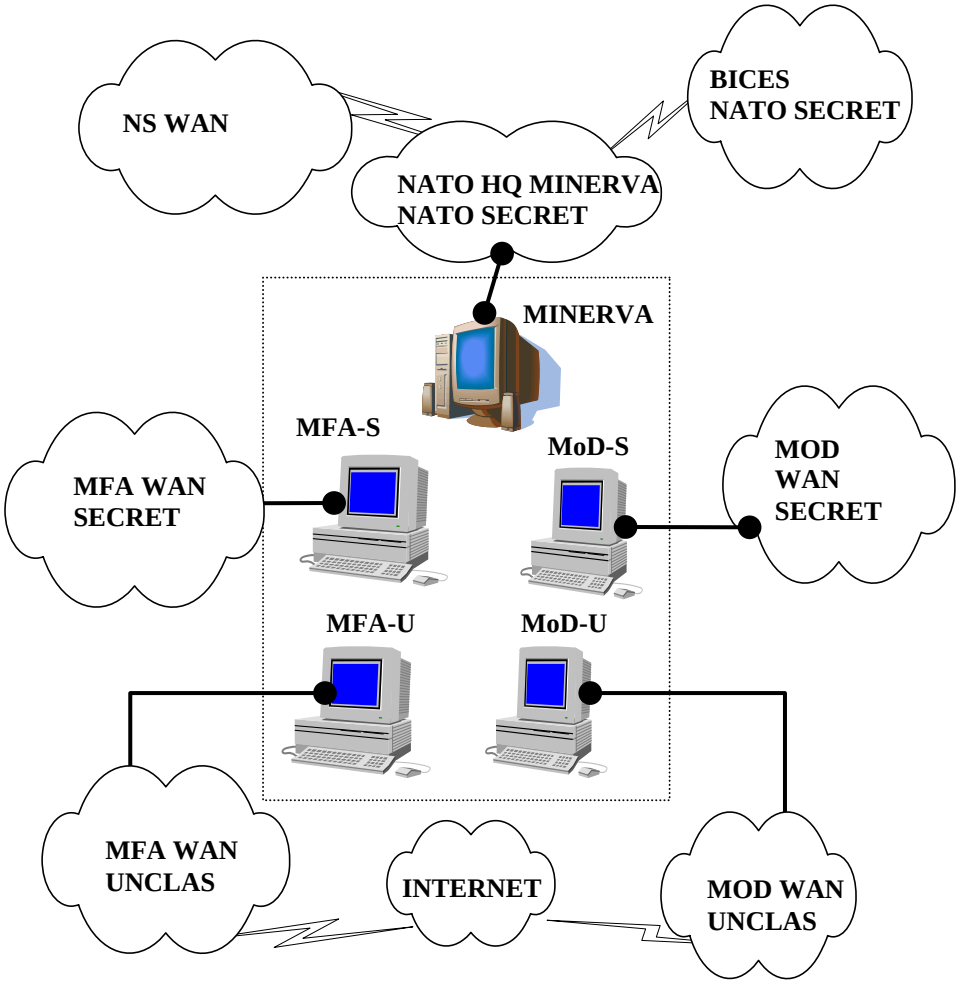


Figure 1: Possible existing delegation networks in place at NATO HQ

The staff at NATO HQ are fully aware of the networking challenges that lie ahead, not only for the HQ but nations as well. In 2003, a capital project entitled *Connectivity to Capitals* resulted in some preliminary investigative work, principally in the area of how information is moved from NATO HQ back to the capitals. However, even though this project never really

gained financial support, it did draw attention to the issue, but only from a one-sided perspective. It ignored the importance of the full business process - two-way communication, ***consultation.***

Thirty years ago, there was no evidence of a problem. NATO and national staffs, resident in Brussels, worked very well with each other in the business process. They discussed, considered and consulted together to achieve workable solutions. The proliferation of IT networks, however, has made challenges for staff. Security policies often prohibit the use of USB memory sticks, based on the large quantity of information that they can hold. Any removable media that is used to extract unclassified information from a classified network cannot be reused in the higher network, once it has been used in the lower network. Some systems are required to follow the Tempest standard (for limited electromagnetic emissions), tightening configuration changes and even printer assignments. There is no certainty that the networks are using the same version of office software, or even the same operating system. This presents user-training problems, increases the time required to move data across systems, results in no data logging – and contributes to an atmosphere of frustration and human error.

The modern asymmetric threat demands much quicker decision-making. Technology has enabled the quicker production, modification and dissemination of documents, but the networking process has seen little change, with the exception that data can move much faster back to national capitals. The next logical step should see technological solutions utilized to reduce air-gaps, track data movement and improve the consultation and decision making process.

Another area that may yet see change is the issue concerning the actual volume of classified traffic over the MINERVA network. It seems unnecessarily resource expensive to utilize MINERVA with only 15% traffic classified at NATO Confidential (NC) and higher. To

address this issue, in 2006, NATO staff announced plans to design a new Business LAN at NATO HQ to run in parallel with the MINERVA LAN. Immediate benefits should be seen in designing, implementing and maintaining a LAN at the NR level vice the NS level – as well as reducing the traffic burden on the overworked MINERVA. However, many nations countered that this will put one more workstation and one more air-gap on the desks of all staff – and it will result in a split information system. The risk of a split database, with NC/NS material on MINERVA and NR (and below) material on the new Business LAN is currently being analyzed in Brussels and won't be discussed further in this paper.

NATO embarked on a major transformation with the declaration signed by all nations at the Prague Summit of November 2002 ("Prague Summit Declaration", 2002). Significant changes to the NATO Command Structure were announced; together with a comprehensive suite of measures intended to strengthen the Alliance's ability to counter new threats, including those launched in cyber space. Clearly, NATO understood the importance of change, getting away from a defense based on pre-determined strategic locations in Central Europe and posturing to best counter the asymmetric threat of terrorism. The Prague Summit also built on the announcement at the Washington Summit of 1999 to build a new HQ "to meet the requirements of the Alliance in the 21st Century" ("NATO New Headquarters", n.d.). In fact, although it took time, this announcement has resulted in the allocation of an approved design and sufficient land, in order to achieve the desired end-state. Current plans show that the new building, that will also mean new accommodation spaces not only for NATO staff but all national delegations as well – is aimed for occupancy in 2012. If that goal is met, NATO will have an opportunity to step away

from its existing IT infrastructure, and *build-in technological solutions to support its business process*.

Chapter 3 – Requirements for Transformation

In the past decade, open sources abound with material touting the need for transformation, the need to leverage Information Age concepts and technologies and adapt business processes to make organizations much more agile and effective. Terms like Network Centric Warfare (NCW), Network Enabled Capability (NEC) and Network Enabled Warfare (NEW) have emerged to describe how nations plan to embrace this concept and *transform their forces*. A necessary goal of transformation is one described as *self-synchronization*, where an organization (Alberts and Hayes, 2005, p.27):

a. Has clear and consistent understanding of the mission;

b. Possesses high quality information and shared situational awareness;

c. Shows competence at all levels; and

d. Has trust in the information, equipment, technology, peers and higher/lower staff.

It is true that marvelous advances in technology have changed our world, and immeasurably increased our capability to collect, process, disseminate, and utilize information. However, "despite considerable advances in our ability to process information, these advances have not been rapid enough to keep pace with the increases in collection…but help is on the way" (Alberts, Gartska, Hayes, and Signori, 2001, p.44).

Readers familiar with the transformation concepts of the Information Age will recall that it is necessary to consider three domains: *physical*, *information* and *cognitive* (Alberts et al, 2001, p.24). The use of technology and changes in process and thinking are all required. A

useful way to understand the value of this transformation is to consider the desired improved effectiveness of military forces. The US DoD has embarked on a path of transformation, with notional expectations of the value to be gained. Figure 2, below, is a familiar *spider-chart* that aims to map ten operational military values in a platform-based environment against a true network centric one (Alberts et al, 2001, p.69). Although these are only assertions, the authors contest that growing evidence is being collected to support them.

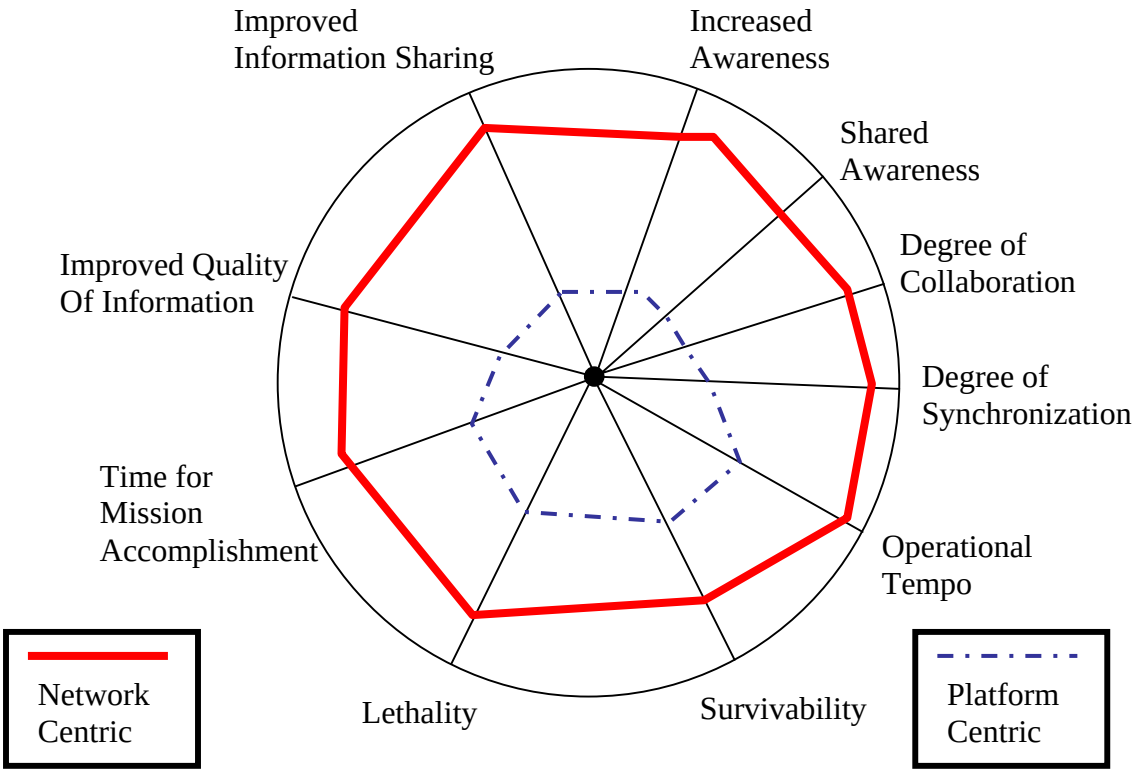


Figure 2: Comparison of warfighting models

When considering how to leverage the tenets of transformation, and strive for the benefits of self-synchronization, it is useful to start with the recognition of an existing informal network that has serviced the needs of the Alliance since its inception. An informal network is a "human, social interaction based on trust, shared values, and beliefs, and allows the sharing of

information" (Atkinson and Moffat, 2005, p.89). Together with the formal process of policy writing and document exchange, this informal network between nations and NATO staff members still serves the Alliance business process of consultation, even today.

The Industrial Age saw the evolution of military forces into "many-layered hierarchies populated with stove-piped organizations and centralized planning processes" (Alberts and Hayes, 2005, p.57). The latter half of the 20th century was characterized by the introduction of digital networks and information systems dedicated to supporting these stove-pipes, or *cylinders of excellence*. However, with the requirement for coalition warfare and renewed interest in interoperability, breaking apart these stove-pipes and building gateways between networks has become more and more essential. So important, in fact, that one quickly comes to the realization that the *benefits of transformation entirely depends on the interconnection of networks*, within or between nations. Despite the advances of the Internet and the development of open source protocols (which has made multi-domain collaboration a reality), the lack of interoperation between domain access control policies may lead to breaches in security (Shehab, Bertino, and Ghafoor, 2005).

The Chief Information Officer (CIO) for the Australian Defence Forces commented that new capabilities are being developed to allow sharing of classified information electronically between allied partners. Up until recently, "the only means to exchange messages of this classification was through the text-based formal messaging system" (O'Sullivan, 2005). A recently established alternative, is the US led Combined Enterprise Regional Information Exchange System (CENTRIXS) suite of networks supporting information sharing at the operational and tactical levels. A unique CENTRIXS domain is established to meet the

requirements of each coalition group, led by US Forces. In time, these different domains may also be inter-connected with gateways.

Beyond the initial gateway between networks, there are many other obstacles to achieving full C2 interoperability, namely (Larsen, 2007):

a. Coherent doctrine and procedures;

b. Physical connection;

c. Compatible protocols;

d. Compatible or like data structures;

e. Semantic understanding of data; and

f. Information assurance.

However, Larsen did not mention two significant hurdles to cross-domain solutions, namely *trust between nations* and nations' *capacity for embracing technological change*. Trust between nations is a difficult factor to measure. Consider, for example, that all NATO nations standardized on exactly the same security classifications – which is not actually the case since nations make these definitions themselves. Suppose, for example, that Nation X wanted to connect its classified network to a like network operated by Nation Y, particularly important to both nations involved in the same coalition operation. One problem that involves the consideration of trust is the process of obtaining and maintaining a security clearance. Suppose that Nation X requires a thorough background study and several months of investigation in order to grant a national Secret clearance. What if Nation Y does not put the same level of effort into the background check and gives out a Secret clearance after no investigative work at all? This is

clearly an area where both nations have to be completely honest when establishing their level of trust.

In an NCW environment, rather than relying upon traditional data push or pull technologies, the concept of discovery has emerged as important enabler. "Discovery generically refers to finding and retrieving actionable, decision-quality information on-the-fly" (Connors, Malloy, and Masek, 2006, p. 3). One could easily argue that the discovery process will never happen as long as there are air-gaps between networks. Similarly, even basic services like web browsing and email depend on an arrangement of mutual, pre-scripted trust between nations, embodied in their security policies.

The situation at NATO HQ is a relatively simple one, with a well-defined Alliance of 26 nations. This is not a dynamic coalition with partner nations, Non-Governmental Organizations (NGO) (Red Cross and Doctors without Borders, for example) and Other Government Departments (Coastguard, for example) drifting in and out over time. Information sharing and security in dynamic coalitions is considerably more difficult, particularly when trying to enable joint C2 services, well beyond the basics of email and web browsing (Phillips, Ting, and Demurjian, 2002).

Since NATO membership now includes 26 nations, it is relevant to comment on the potential for improving interoperability, given the effort that may be required on the part of all nations. The diversity of NATO's member nations is reflected in their geographic size, location, population demographics, levels of economic development, types of governments, and capacity for acquiring high technology. Acquisition of new technologies seems to be unproblematic. The increasing use of open standards and cross industry collaboration has nearly eliminated the

problem, but the capacity to acquire a technology does not necessarily equate to a comparable capacity to implement it. Implementation requires a subsequent threshold level of physical, human, and institutional capacity, taking into account financial resources, social, political, and even cultural will.

A study by the RAND Corporation has suggested that the impact of interoperability and technology adoption varies widely across global regions and nations (Silberglitt, AntÃ³n, Howell, and Wong, 2006). Each country's capacity to implement new technologies was considered at Figure 3, taking into account the following factors:

a. Capacity to acquire;

b. The percentage of the ten drivers for implementation applicable to that country; and

c. The percentage of the ten barriers to implementation applicable to that country.

Implementation drivers and/or barriers that were considered were (Silberglitt et al 2006):

a. Cost/financing;

b. Laws/policies;

c. Social values, public opinions, politics;

d. Infrastructure;

e. Privacy concerns;

f. Resource use and environmental health;

g. Investment in research and development;

h. Education and literacy;

i. Population and demographics; and

j. Governance and stability.

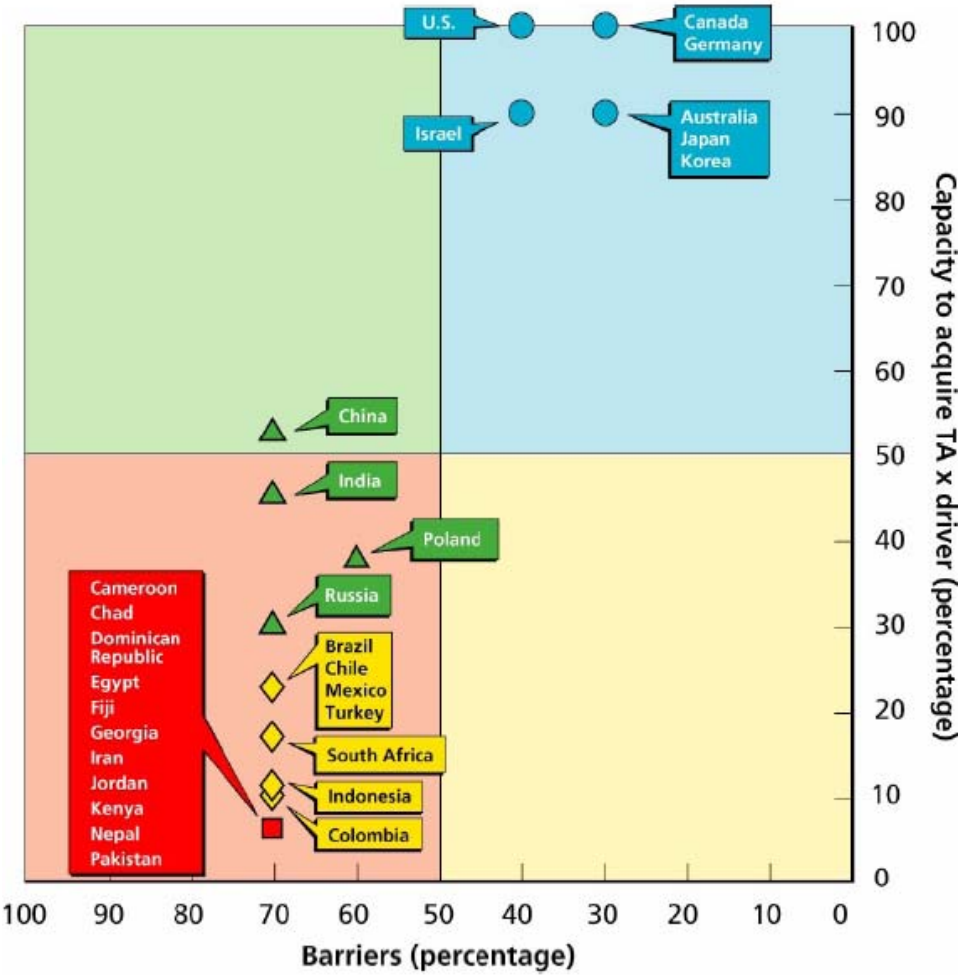


Figure 3: Selected Countries Capacity to Implement Technology

Business processes at NATO HQ need to be transformed. This transformation should start with the connection of classified networks, NATO and national, to the extent possible – given nations' will, trust and capacity to embrace the solutions available. NATO member nations will be "on their own recognizance" when it comes to implementation. The use of the Internet may also be considered, given the known limitations for security. The Internet is nearly

omni-present, and may play an important role. There may be drivers or barriers that come to play, certainly impacting on the Alliance as a whole.

Chapter 4 – Changing the Office Footprint

Typical government offices are organized into a cubicle environment. Although this contributes to an efficient and economical workspace, it goes against good practice when considering the different networks, classified telephone and personal conversations and security controls that are usually required. Typically, national and NATO staffs are not housed in bullpens or cubicles, perhaps two personnel to an office. This makes a significant difference when considering the issue of required separation distance between network equipment. There is usually a requirement for a physical separation, even between unclassified and classified networks operated by the same nation. Normally, the 1 metre rule is in effect. Network equipment, telephones, fax machines, modems, hubs, routers, servers, keyboards and even printers – are required to be at least 1 metre separate from hardware belonging to another network. This can present challenges, even within an office occupied by only one staff member.

There is likely to be a modest energy saving to be found in incorporating gateways or cross-domain solutions between networks. To get an idea of what this might represent, assume the electrical current draw of an average personal computer (PC) as 2.5A (at 120V), and the monitor at 1.0A (ignoring the energy demands of printers, servers and network appliances). An estimated 3,000 personnel work at NATO HQ. Based on the author's experience, this can be broken out into roughly 1,000 NATO staff, 600 NATO Agency staff, 1,200 National staff and 200 from the Partner Nations. NATO staff don't need cross-domain solutions. Their needs can likely be met with two computers, one for unclassified and the other for classified (currently

MINERVA). The real customer base for cross-domain solutions will be with the national delegations. Based on work in the previous chapter to describe a generic delegation, one might safely assume that three computers are in use per person amongst the 1,200 national staff. This could certainly be reduced to two computers, one at the unclassified level and the other at the classified level. Reducing the footprint of 1,200 computers would show an obvious reduction of 4,200A (504KW) throughout the building during the daytime. This will represent a considerable reduction in electrical demand over the building's power infrastructure. Over a 10-hour day, this equates to a savings of only $ 403 per day – spread across 26 nations (based on 8 cents per KW hour). Over a 220-day work year, this savings corresponds to nearly $ 89K.

Admittedly, the financial impact of reducing stove-piped networks seems trivial. However, there are also potential impacts with a reduced demand for air-conditioning in the summer, and less ambient noise. The background noise in a small office with only one computer is noticeably less than another office with three or four computers. Another simple calculation could see a reduction in the cost of baseline software, both initial licensing and ongoing maintenance costs. There could also be a reduced training burden, reflected in lower costs to the nations and improved efficiency and morale of their staff.

The existing air-gap method of data transfer is not without its shortcomings ("A Preferred Solution For High-Security Real-time Electronic Data Transfer Between Networks", n.d.). Data extracted from MINERVA to a national network (unclassified or classified) has to be copied to a removable storage medium, then physically moved and placed in another network. One might naively assume that options available to the staff are floppy disk, CD, DVD, zip drive or even USB stick. However, security policies will vary in their treatment of this. It may even be

possible that one or more of the receiving networks is closed to any removable media. According to NATO security policy, any *previously used media* is not permitted to be inserted in MINERVA (North Atlantic Treaty Organization, 2006), due to the risk of contamination from malicious code. The continuous process of moving data across air-gaps requires a considerable amount of time, effort and expense. Although the ongoing cost of having fresh CDs available may appear trivial, some personnel are required to buy, store and dispense or manage this material. Consider the impact of these air-gaps present in all 26 NATO nations' delegations. Based on the author's experience, on average, 80 official documents were transferred daily by registry staff in one delegation. However, most of the previously mentioned 1200 national staff are consumed with transferring these formal documents (in addition to informal correspondence and draft documents) and receiving replies constituting national positions on a daily basis. Globally, this clearly represents a high risk. A manual transfer of material is not conducive to automation or remote operation, although the use of data diodes, to be discussed in the next chapter, may prove to be of value. Needless to say, all of this cross-domain data transfer is currently done in private offices, with no logging of what material has been moved where – contrary to well established good practice in the handling of classified material.

Reducing air-gaps between networks isn't going to save a lot of money, but the inefficiencies and lack of control inherent with the existing manual transfers can definitely benefit from automation and logging. This will have a follow-on effect with the result being more efficient staff, and faster, more thorough consultation - something that is in line with NATO's stated ambitions.

Chapter 5 – Data Diodes

Some of the inherent weaknesses of air-gap cross-domain solutions were already mentioned in the previous chapter. Although the waste of resources is of concern, even more alarming is the lack of control and potential risky security environment. Removable media (used for the manual air-gaps) can be lost, improperly labelled, improperly stored, and accidentally disposed off – all contributing to a relaxed handling environment where classified information may end up in the wrong hands. An obvious improvement can be through the use of an automated process, a technological solution. "The physical one-way nature of the Data Diode insures that no administrator, encryption hacker, computer hardware expert, locksmith or untrained employee can move data from the inside network out" ("Multi-Domain Security and its Impact on Network Centric Operations", n.d., p.4). Typically, the higher classified network is prohibited from connection with a lower classified network. In this application involving the movement of NATO HQ produced documents, it will be assumed that MINERVA (classified at NS) will be the *lower network* and one (or several) of the national networks (classified as national secret) may function as the *higher network*. With this configuration, a Data Diode installation may control and log the one-way transfer of files, email and even web pages. There are different commercial products marketed as Data Diodes, and the following pages will present and discuss two variants.

The Fort Fox Data Diode is a hardware-based security device, designed to optically insulate two domains/networks. This technology has been installed in several countries, including within NATO networks to provide a secure one-way connection without compromising the security of the receiving network. The device operates in a unidirectional

mode, deploying a gigabit-speed light source and receiving photocell ("A Preferred Solution For High-Security Real-time Electronic Data Transfer Between Networks", n.d.). The Data Diode can be installed on its own, or together with two optional servers to provide additional features. A simplified configuration is shown below as Figure 4.

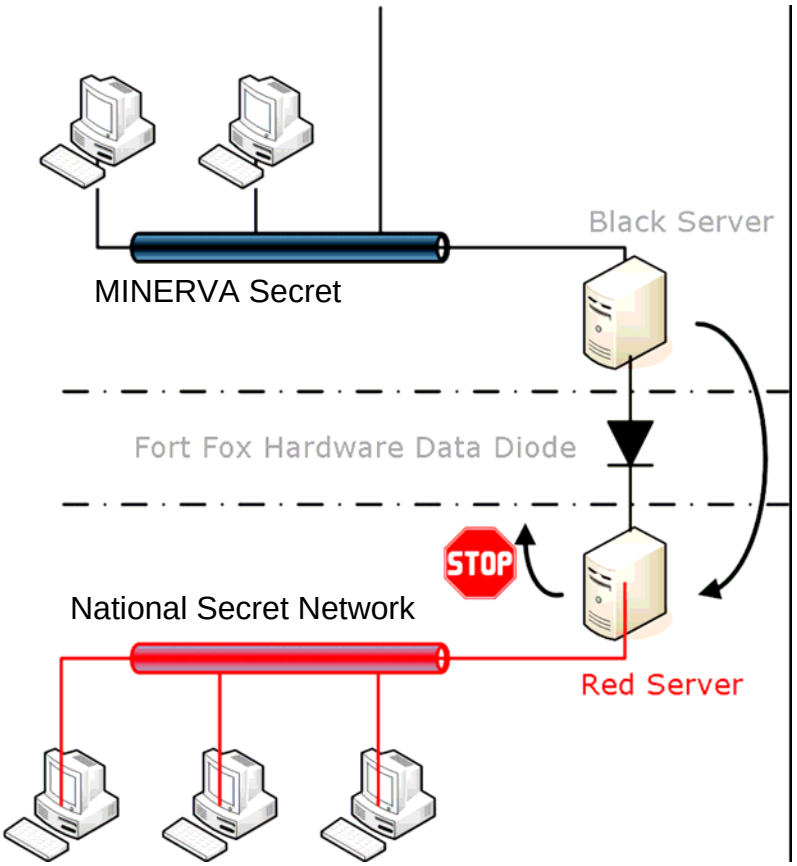


Figure 4: Typical Fort Fox Data Diode Configuration ("A Preferred Solution For High Security Real-time Electronic Data Transfer Between Networks", n.d.).

With this installation, the black network will be MINERVA and the red network will be a national network (at the Secret level). Both red and black servers come with web interfaces, allowing authorized users to define and carry out data transfers, on a case-by-case basis – if required. National network users can access automated transfer of files from MINERVA, email

sent from MINERVA to national users, and even browse down into MINERVA web pages. The process for file transfers or email is fully automated after configuration of both the black and red proxy servers. There is no need for ongoing operator intervention, unless changes are required to the configuration. The black proxy server, for example, could be set to move all NATO DMS files as they are produced and saved to the DMS. The black proxy server automatically forwards data through the Data Diode to the red proxy server, and then forwards it to the final destination in the red network. To users in the black network it appears as if they can send a file or email straight to a server or recipient in the red network. However, network traffic is strictly limited to go only from the black to the red network; in fact it is physically impossible to send information from red to black with this Data Diode installation (Rens de Wolf, personal communication 21 January 2008).

The physical connection between the red and black networks relies on the optical junction of the Data Diode. Data leakage from errors or holes in software or firmware in the Data Diode is not possible, simply because there is no decision logic present in the device. All data that moves across the diode is logged on both the black and red servers, “ensuring that all ‘events’ during a transfer are tracked and timed, and abnormal activities are detected and reported” (“A Preferred Solution For High-Security Real-time Electronic Data Transfer Between Networks”, n.d., p.11). The throughput of the optical Data Diode is designed as 1 Gbit/s, and its level of security has been approved by the Dutch information security accreditation body.

Fox-IT is working on a two-way Data Diode. This "diode" will still have the same features as the existing Fort Fox Data Diode, but will also allow pre-defined and digitally signed information to go the other way, from the red network backwards into the black network. This

would allow people in the red network to not only receive emails from the black network, but also reply - by having it digitally signed by the user and vetted by an authorized supervisor (before the information is allowed to leave the red network). In addition, a comprehensive audit trail is expected to be part of the solution. As this is currently still a development project, no final documentation is available to the public (Rens de Wolf, personal communication 21 January 2008).

The Tenix America Interactive Link Data Diode (IL-DD) "uses a systems architecture and solutions approach that allows military, intelligence and homeland security organizations to analyze and share data safely across classified and unclassified networks" ("Press Release – Accreditation of Email Transfer and Data Forwarding Applications Results in Complete Turn-Key Cross Domain Solution", n.d.). The Tenix 100MB Data Diode has received full Director of Central Intelligence Directives (DCID) accreditation. The installation and expected use of the Tenix Data Diode is similar to the Fox-IT product previously described. The Tenix Data Diode is a 100MB fiber optic hardware device, connected between two servers installed in respective security domains. Tenix data pump applications installed on these servers can be configured to provide ("Tenix Data Diode – Absolute Information Protection", n.d.):

a. One-way SMTP email transfer;
b. One-way file transfer (any size);
c. One-way transfer of IP packets; and
d. One-way transfer of clipboard data.

Although a turn-key solution can be provided by Tenix, the device requires servers using operating systems that have been tested and found to be supportive of the security device. Third party email content filters and virus scanning applications may be chosen by the purchaser, for the purpose of screening for malicious code prior to entering the high network. Figure 5

illustrates how one-way email transfer is supported with the addition of servers installed on both domains. The Email Transfer Application (ETA) interfaces with SMTP mail servers to allow email produced on the low network to flow into the high network.

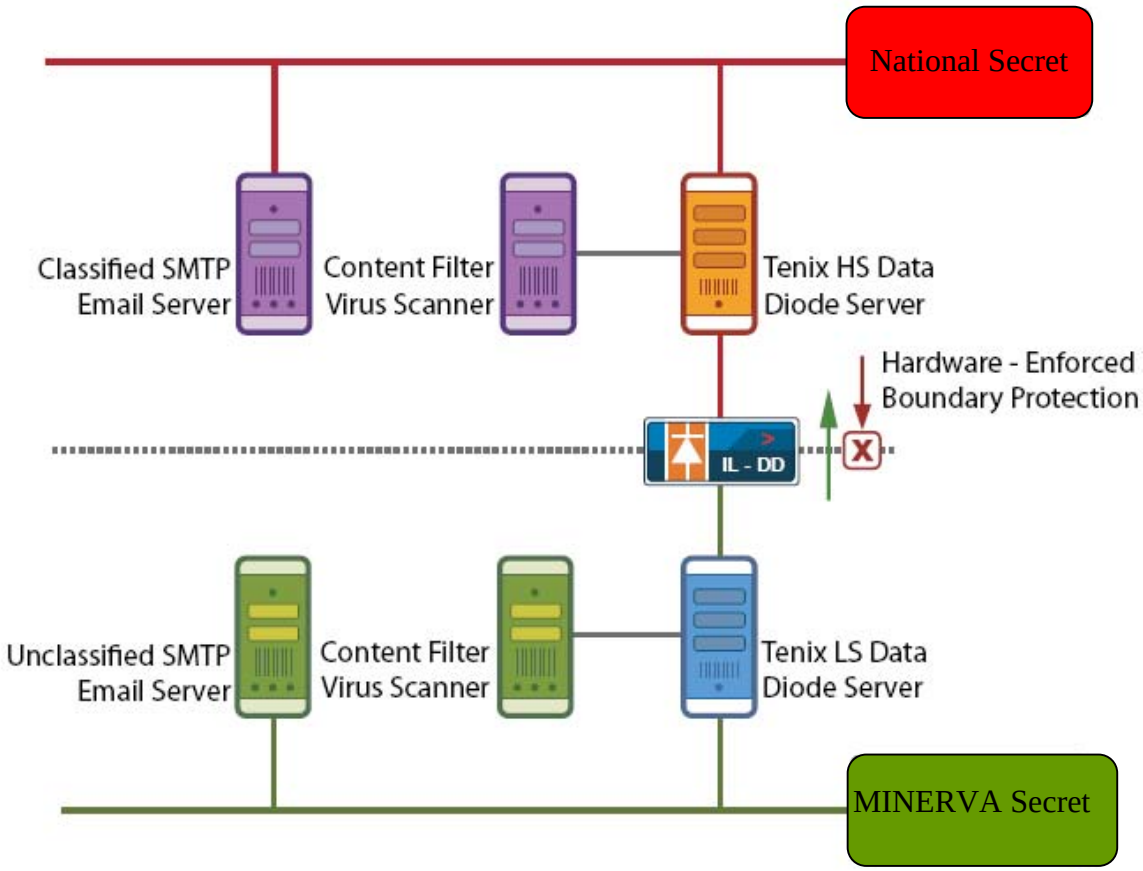


Figure 5: Tenix Data Diode Email transfer ("Tenix Data Diode – Absolute Information Protection", n.d.):

Files placed into a specific source directory on MINERVA would be automatically transferred to the National Secret network, and of course filtered for malicious content and logged. Streaming video, audio and sensor data can also be moved across this IL-DD. NATO HQ uses video production equipment to record meetings of the NAC and MC. Using the one-way feature of this product, live streaming video could be moved from MINERVA onto a

national network, for viewing by either on-site delegation staff, or even remote staff in a nation's capital.

An additional feature found with the Tenix IL-DD is the *clipboard and file transfer*. This Tenix application interfaces with a session's operating system clipboard so that a user can easily find and transfer text, images and files seamlessly, in accordance with preset rules. The configuration may be adjusted, for example, to only permit only certain file types. Users are given an easy to use drop box, allowing them to drag and drop items selected for transfer from the low to high network – while still producing extensive audit and trace logging. The Canadian Department of National Defence has specified the use of the Tenix IL-DD, complete with email, file and clipboard transfer for one-way movement of data from an unclassified domain up to two different classified domains (Thuppal, October 2007). In this specification, the Tenix Interactive Link Keyboard Switch (IL-KBS) is described, where users can access two separate networks from a single workstation, using thin client technology to actually display the less secure network in a window on the higher domain's PC. Users can access email, web and public networks without compromising security, removing the procurement and running costs associated with the second PC.

Although the features available with Data Diodes sound very promising, the raison d'être of this paper is to reduce the number of air-gaps used at NATO HQ. Whilst the installation of Data Diodes would certainly save staff time, improve the security situation, and provide an audit trail for the movement of data from MINERVA to one or more national networks – it is only one-way, and does not fully replace the existing *sneaker-nets* in use. Delegation staff are still interested in getting national positions (often scripted in the capital) from the national network

onto MINERVA for onward dissemination in the HQ itself – fulfilling the business process of consultation. Data Diodes fall short of satisfying this requirement.

Chapter 6 – Cross-Domain Security Guards

Corporations and organizations with different networks in use, at some point in time, will need to consider the benefits of inter-connecting different security domains. A security domain is "An environment or context that is defined by a security policy, security model, or security architecture to include a set of system resources and the set of system entities that have the right to access the resources" ("RFC 2828", n.d.). In the simplest of cases, where one company buys out another, this exercise can be a trivial one, particularly if both networks are owned by the same organization. In this case, it may only require adjustments to router settings, or adjustments to the configuration of a firewall separating the two networks. However, in more complex cases, such as the one described in this paper at NATO HQ, even if all networks operate at the same classification, challenges will be evident.

The strategic level NATO Security Policy comprises two comprehensive documents that describe high-level policy at NATO fixed and deployed or operational sites. In detail, it is supported through six security directives that describe policy as it relates to Personnel Security, Physical Security, Security of Information, Industrial Security and two volumes that detail Information Security (North Atlantic Treaty Organization, 2006). Security policy should comprise a comprehensive set of essential security features, assurances and practices that result in four important functions in an organization (Whitman et al, 2005, p. 68):

a. Protection of the organizations functionality;

b. Enabling the safe operation of software applications;

c. Protection of corporate data that is stored, manipulated and transmitted; and

d. Protection of investment in corporate IT equipment.

The NATO HQ MINERVA LAN is operated as a system high network. That is to say, that all personnel certified to use the network are cleared to the NS level. All data is assumed to be Secret, therefore, personnel must be cleared to this level. Within such an environment, it is accepted that some users, despite the fact that they have a valid security clearance, may not have a need to know some data. If the originators of such data want to take precautions, the onus is on them to craft suitable file sharing permissions – and this can become particularly tedious in a large organization. The advantage of such a *system high network* is that it becomes easier to use Commercial Off the Shelf (COTS) components (MacMillan, Shimko, Sellers, Mayer, Wilson, 2006). The downside of a system high network is that it must be kept strictly separated, isolated, for example from a Top Secret domain. Nonetheless, this sets the stage for the basic security guard, between two classified domains, operating at the same level. Traditional Security Guards have typically been used to control the flow of information between different security domains. Firewalls are able to perform some of the required functionality of a Security Guard, since they are able to control connections based on source and destination IP addresses, port numbers, communications protocols and sometimes user ID and authentication. A Security Guard, however, controls the content sent over a particular connection. Figure 6, on the following page depicts this basic system high, guarded architecture.

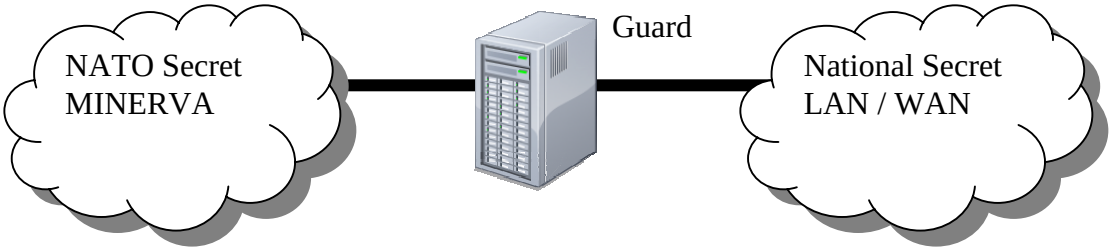


Figure 6: System High, Guarded Architecture

The purpose of this simple guard is to control the flow of information between the two different security domains in accordance with pre-determined information sharing rules. A rule could, for example, specify one-way transit of information, from MINERVA to the National LAN – with no return path (just as what you achieve with a Data Diode). Rules are primarily established with the intention of protecting both security domains (or even more domains in a complicated scenario) from unauthorized intrusion and denial of service attacks that could result from the presence of the interface. Security Guards have also been referred to as *Cross Domain Solutions* (CDS) or *Controlled Interfaces* depending on the author and product. Regardless of the nomenclature, Security Guards are known to possess a number of characteristics that define them (Reed, 2004, p. 1-3):

a. **The type of data that can be passed.** Some guards only support transfer of highly structured text; while others support transfer of unstructured or semi-structured data.
b. **The method used to check the content of items.** Some guards rely on human review of all data content; some use an automated review, and some bump the review to a human only when it fails to pass through a *dirty word filter*.
c. **The direction of the data flow.** Some guards are designed to transfer data from a lower classified domain to a higher one. In this case, the guard will be focused on the

risk of allowing malicious content into the higher domain. Some guards work to filter information moving from a higher to lower classified domain, and in this case, will be concerned with unauthorized data release. Some guards support bi-directional flow, whereas some are uni-directional. Some guards transfer data between equivalent peers, focusing their effort on checking for both malicious content and the unauthorized release of data.

d. **The delivery method used to transfer the data.** Some guards use File Transport Protocol (FTP), some use Simple Mail Transport Protocol (SMTP); some use Hypertext Transport Protocol (HTTP); some use other protocols.

In the case of a National interface to the MINERVA network, one can easily imagine the requirement for two-way email and at least one-way web browsing. Given the business process in place, staff working at the grand strategic level of NATO definitely need full two-way email (with certain attachments). One-way browsing would mean that National staff could browse into MINERVA, but other nations or NATO staff would be unable to browse across into the National network. Figure 7, below, illustrates the minimum required functional data flows.

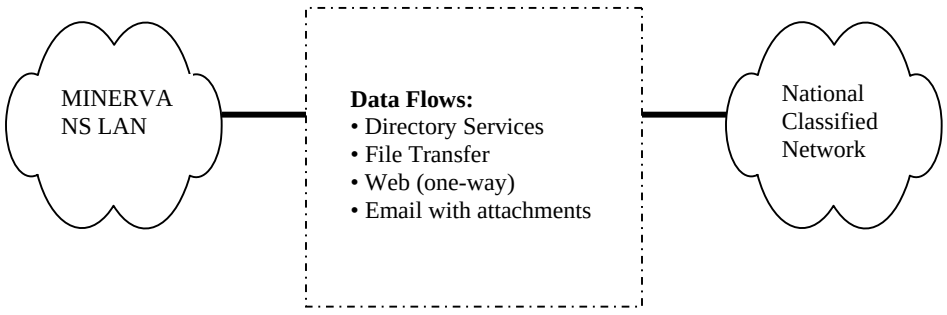


Figure 7: Required Functional Data Flows

In an operational or tactical theatre, one can easily imagine other required data flows in order to increase the synergy of coalition forces, services like Voice Over Internet Protocol (VOIP), Video Teleconference (VTC), instant messaging / chat and Joint Common Operational Picture (JCOP) combining the Land/Air/Maritime views. However, NATO HQ is a political organization and frankly does not need these additional services, cutting into the responsibility of other operational HQs. However, supporting even limited services can present challenges. Even with one-way web browsing, "vulnerabilities associated with Web technologies introduce risks" (Reed, 2004, p. 18). Poorly written web pages have been known to result in cross-site request forgery, cross-site scripting, SQL injection, buffer overflows, remote command execution, and weak authentication and authorization ("Common Security Vulnerabilities in e-commerce Systems", n.d.). Even with one-way browsing, an element of trust between the organizations responsible for networks will be required.

Expanding on the functional view of Figure 7, one can realize how these services need to be allocated into two general areas providing Boundary Protection Services (BPS) and a Demilitarized Zone (DMZ). The BPS should provide basic routing / traffic filtering so that IP traffic will follow the defined security policy rules. It might, for example, be desired to limit accessibility of MINERVA data to only those users originating at National Delegations resident at NATO HQ, denying this connectivity to the thousands of other legitimate users who are employed elsewhere. This is also where browsing from MINERVA users into the National Classified Network would be stopped. Intrusion Detection System (IDS) network sensors would normally be placed in the BPS. Next to consider will be the issue of encryption requirements (if any) of the networks as they are distributed throughout the building. Classified networks within

Delegations would not normally require encryption (because the physical space is controlled by the Delegation). Cabling, as such, would be described as RED (unencrypted) since they carry classified, unencrypted traffic. However, once the cables move outside the physical control of nations, into the common corridors at NATO HQ, there will likely be a demand for an encryption device (at each end) to provide sufficient protection for the network (likely operating at Layer 2 of the ISO model). These concepts are illustrated below in Figure 8, introducing the subsequent problems of ownership of the DMZ and BPS components, physical placement and consequential configuration control. At this point in time, it should suffice to realize that a joint or cooperative effort may not be satisfactory to both NATO and National authorities, and that each party may need to install and operate their own components. The NATO solution of cooperative zones will be discussed in a later chapter.

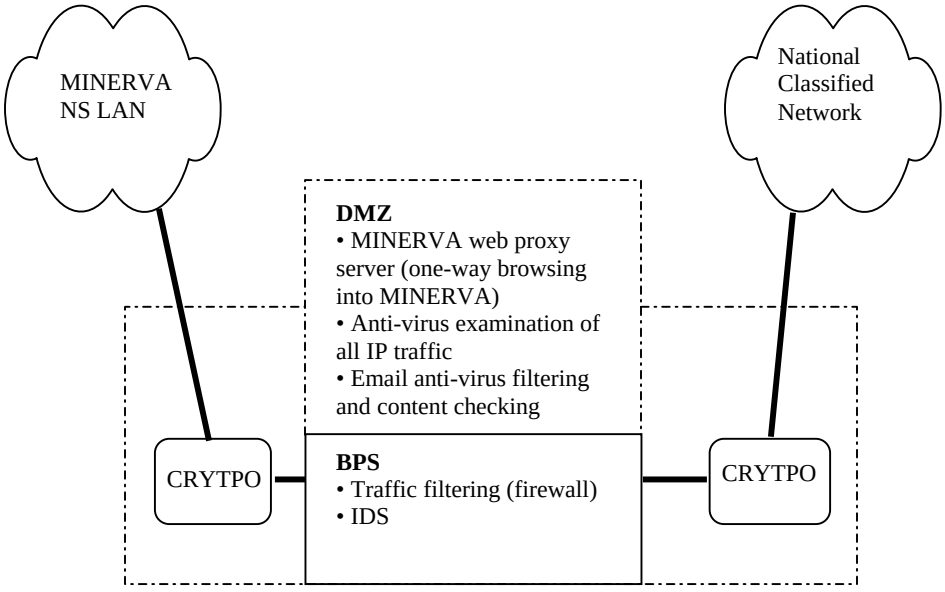


Figure 8: Required Functional Separation of DMZ and BPS

Translating the functional components described at Figure 8 into equipment resources results in a more mature depiction of the required CDS depicted below at Figure 9.

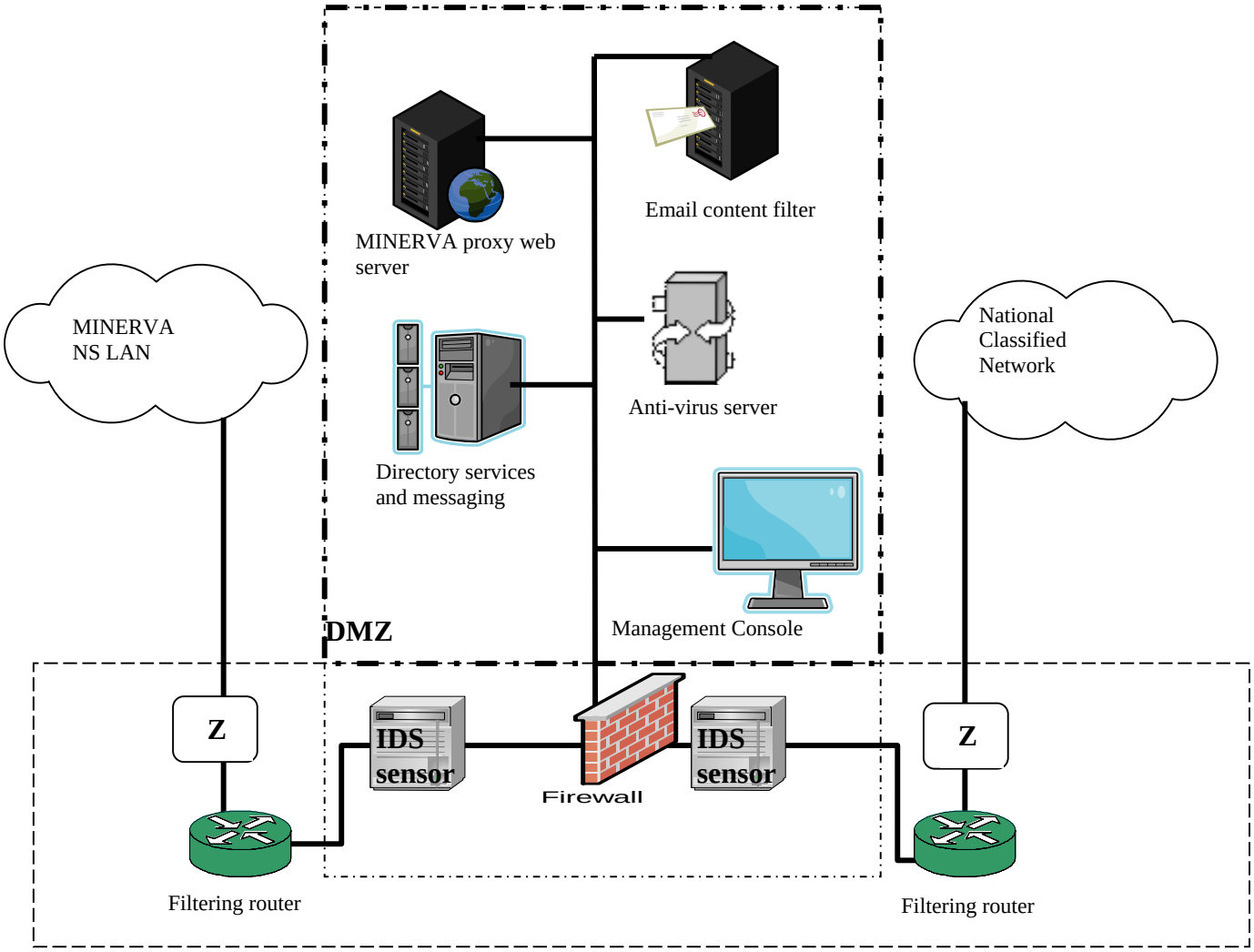


Figure 9: Equipment requirements for the CDS

If you start with the assumption that you need to create a system high network (a Secret network, for example – that contains data that is also classified at lower levels), you'll need to build on an architecture that is accredited for the highest level of data held. In the long run, this solution is less costly in terms of resources, simply because it guards all data the same and avoids

the high cost of human review – something that may be necessary downstream when connections to lower networks are required (“Cross Domain Solutions”, n.d.). The importance that the underlying server operating system holds is “undeniable, the underlying operating system is responsible for protecting application-space mechanisms against tampering, bypassing and spoofing attacks” (Loscocco, Smalley, Muckelbauer, Taylor, Turner, and Farrel, 1998, p. 1). In addition to the robustness of the operating system, residual technical problems, incorrect installations and implementation and erroneous assumptions are often to blame for resultant vulnerabilities.

A foundation for modern cross-domain Security guards has come to be the BAE XTS-300 and the Secure Trusted Operating System (STOP) - collectively referred to as the Defense Information Infrastructure (DII) High Assurance Guard (“Integrated Information Assurance - XTS 300 Solution Suite”, n.d.). An XTS-300 hosting the DataSync Guard application offers web browsing, email with attachments, directory sharing and secure message transfers between the two domains. The BAE XTS-300 is touted as a Multi-Level System, originally developed by BAE Systems, and has transitioned from proprietary, mini-computer hardware to COTS hardware. The XTS-300 completed security evaluation in 1994 and is (or has been) in common use in CDS for up to Secret level, with example installations as follows (“XTS-400 - BAE Systems”, n.d.):

a. National Security Agency’s (NSA) DII Guard;
b. Defense Information System Agency’s (DISA) C2 Guard;
c. Federal Bureau of Investigation’s (FBI) Cyclone Guard;
d. State Department’s Unclassified Telegram Guard Processor;

e. Air Force's F-22 Secure Interface System;

f. Department of Energy's FTP Guard;

g. Novell Corporation's NICI Public Key Infrastructure (PKI);

h. United States Intelligence Community; and

i. Canadian Department of National Defence (DND) and Department of Foreign Affairs, Industry and Trade (DFAIT).

The DII High Assurance Guard is now being superseded by the next generation, the XTS-400, a combination of Intel x86 hardware and STOP. The latest version of STOP, version 6, uses an Intel construct referred to as exclusive *domains of isolation*. For example, Domain 0 (the security kernel) has the system's highest level of security, inaccessible to users. Inside Domain 0, I/O drivers reside, secure from unauthorized access. Processes are also restricted by Domain privileges, and are not allowed to send messages to higher Domains. The XTS-400 can host, and be trusted to separate multiple and concurrent data sets, users and networks at different sensitivity levels and meets the Common Criteria assurance level rating of Evaluation Assurance Level (EAL) 5 (although designed to meet the stringent requirements of EAL6). Of note, there are 11 incremental differences between EAL4 and 5, and an additional 13 differences between EAL5 and 6 ("XTS-400 - BAE Systems", n.d.). EAL4 is used where developers or users require a *moderate to high level of independently assured security* in conventionally produced operating systems and are prepared to incur additional security-specific engineering costs ("Common Criteria – An Introduction", n.d.). For example, Windows 2000 and Solaris 8 are evaluated at EAL4 ("Trusted Solaris 8 Operating Environment", n.d.). EAL5, on the other hand, is applicable in "circumstances where developers or users require a high level of independently assured

security" ("XTS-400 – BAE Systems", n.d.). Version 6 of STOP incorporates Mandatory Integrity Policy (users are able to read the files they need, while the files remain protected from unauthorized modification or malicious code) and Discretionary Access Controls (users set permissions based on recipients in Access Control Lists (ACL)).

In a Trusted Guard configuration, the XTS-400 is intended to host the Standard Automated Guard Environment (SAGE), a client/server, modular, transaction-oriented infrastructure. Not surprisingly, detailed examples of Trusted Guard CDS installations are not commonly available in the public domain. The Canadian Department of Defence has specified the use of BAE's new DII Guard (XTS-400 and STOP 6) for a CDS between three classified networks operating with different release caveats, hence different domains. The CDS will support email and web browsing between the domains, all at the Secret level (Thuppal, December 2007). The number of networks that could be connected is limited primarily by the port limitation of hardware interfaces and server processing power (R. Thuppal, personal communication 27 January 2008). BAE-IT offers to help design, code and accredit Trusted Guard CDS, a feature that should be of interest to nations seeking to reduce stove-piped networks at NATO HQ.

Other examples of certified CDS are available within the public domain. Some examples are as follow:

a. ***Radiant Mercury*** - developed by Lockheed Martin. The CENTRIXS network already makes use of the Radiant Mercury CDS with one-way browsing and two-way email/chat/collaboration between SIPRNet and each CENTRIXS variant (essentially bilateral relationships between the USA and each member of the particular coalition).

Radiant Mercury guards are specifically used within CENTRIXS "for formatted message text data and imagery" (Boardman and Shuey, 2004).

b. ***Clearswift*** - a United Kingdom (UK) provider of CDS, accredited to EAL4 standard. Two products are of interest to this chapter: Bastion™ (providing assured separation of networks operating at different levels of trust), and DeepSecure™ (providing assured network boundary protection and inspected of encrypted emails). Clearswift claims (with confidence to EAL4) that with their CDS, an electronic air-gap with automated content inspection provides much higher security than a conventional air-gap (due to the human involvement in moving the media across the network gap) ("EAL4 accredited solutions for military, defense and intelligence security", n.d.).

c. ***Sentinel Trusted CDS*** – produced by Nexor (of the UK), a producer of high-grade security products and services for defense and government. Sentinel is compliant to EAL5 ("NATO Awards Nexor Contract for Provision of High Assurance Mailguards", n.d.).

d. ***Secure Office*** – developed by Trusted Computer Systems and built on a Linux server platform - is the first secure Linux operating system to enter evaluation at EAL4 ("SecureOffice Trusted Gateway on Linux", n.d.). Secure Office builds upon the Trusted Gateway System (TGS), fielded and operational for more than ten years. This solution can be used with Unix thin clients, or on Windows 2000 or above. It is not limited to any arbitrary combination of networks (could be used as 26:1 with NATO HQ for example), and provides secure, multi-directional data transfer using a graphical, web-based client interface. It has options for dirty word search and two-

person review (originator and reviewer) when moving data from a higher to lower classification. Users are able to request data movement in any direction, based on their security clearance, site security policies and user access rights.

Crocker, a General Dynamics Information Assurance Technical Lead, labels CDS as legacy technology, citing its limited but recognizable flaws. In the simplest terms, a CDS confirms the authorized downgrading of information (when moving from a higher to lower network) and that no malicious code is able to transit the networks. Unfortunately, they are programmed to be able to work with only specific data types, and rigidly apply a pre-ordained set of rules. In reality, they do nothing to mitigate the risks posed by insiders (Crocker, 2007) – often attributed to 95% of losses ("CSI/FBI Computer Crime and Security Survey", 2006). A CDS still demands accurate labeling and handling by the user community, both at the point of production and onward dissemination and distribution. Information that has been incorrectly labeled by the originator, or skillfully adjusted to be successful in passing through the content filter will not be detected, deleted and/or quarantined by the CDS. This paper, for example, may not pass through a CDS simply because it has used the phrase *Top Secret*. Although the material itself does not warrant this classification, the CDS will prevent its release from a Secret network down to an unclassified network, simply because of the rigid rule to detect and deny any data transfer containing this phrase. Most content filters are limited in their ability to screen attachments. Parsing a text file attachment for the phrase "National Eyes Only" is fairly easy, but will become a much more challenging task with a .jpg image and practically impossible with steganography (the action of hiding the existence of data/information, as well as the actual data itself, concealed within other innocuous data, in plain view) (Whitman et al, 2005, p. 385).

As discussed, the downside of typical CDS is that content checkers may be too rigid (inhibiting information sharing) in their enforcement of the cross-domain security policy. Alternatively, they may be too permissive and unable to step back and completely realize the larger picture of the information that has moved across the guard. Researchers Swamy, Hicks and Tsang (2007) have advocated the dynamic association of security labels with sensitive entities. The authors admit though that several technical challenges remain before this can be enabled:

a. A language must be designed to produce labels capable of supporting common security policies;
b. We should be able to precisely track the labels as a file is moved through different applications;
c. Consistent security policy checks should take place within applications; and
d. As documents (with their embedded labels) are moved across the network, the relationship between object and label should not be misconstrued.

In summary, a number of available and accredited solutions have been produced by both US and UK companies that could be used to provide CDS to nations seeking to reduce their existing air-gaps with the NATO classified LAN MINERVA. Limitations in their deployment and operation exist, but they do offer a more reliable, trusted solution, and should improve the overall consultation process.

Chapter 7 – The Quest for Multi-Level Security (MLS)

Government agencies and contractors have been interested and working towards developing MLS solutions since the mid-sixties. In 1973, the Bell-LaPadula model was defined

to formalize the US DoD's MLS policy and helps to narrow discussion on this potentially wide-ranging subject. The Bell-LaPadula model concentrates on confidentiality aspects of information and defines two important security axioms ("Bell-LaPadula model", n.d.):

a. A subject cannot read information for which it is not cleared, often referred to as ***no read-up***; and
b. A subject cannot move information from system-high to system-low, often referred to as ***no write-down***.

An apparent limitation of the Bell-LaPadula model is its focus on information confidentiality, neglecting to consider the integrity of the information. The Biba integrity Model attempts to address this limitation by defining the following security axioms:

a. A subject may modify an object if the security level of a subject is at least as high as the security level of the object; and
b. A system-low object may not be passed to a system-high object. This prevents the corruption of system-high information by system-low information.

The Data Diodes discussed in a previous chapter are certainly MLS products, and precisely follow the Bell LaPadula tenets of no read-up and no write-down. The DII High Assurance Guard CDS discussed in the previous chapter can also be described as an MLS product, but it does not strictly subscribe to Bell LaPadula or Biba security models since it does permit write-down. Multi-Domain Security (MDS) has been suggested as the logical evolution of the technology, aiming to meet the demands of customers that are well aware of what capabilities exist in other domains - most commonly the Internet ("Multi-Domain Security and its Impact on Network Centric Operations", n.d.). In reality, users have become very

accustomed to using Google and weblogs (blogs) for problem solving and analysis at home, and they can't understand why these tools are not commonly available on classified networks.

The US DoD has ambitions of creating a Global Information Grid (GIG), replacing the current stovepipes and inherent disadvantages of modern information systems by 2020. The GIG will be based on the utility of web services and IP, using COTS hardware and software but running over a black or protected core (Reed, 2004). This black-core network will require encryption of all data at source, based on SSL/TLS (or its successor) – and this remains "a key challenge for network architecture" (Mineweaser, 2006). The expectation with the GIG is that classified material from any source may be available all over the network, but only accessible to qualified/legitimate users.

At least three different MLS approaches have been taken to provide high assurance to MLS architectures. The systems contain some similarities in their construct, but it has been proven difficult to compare them, without "metrics or even a common framework for understanding the relative security characteristics of the different approaches" (Levin, Irvine, Weissman, and Nguyen, 2007, p.37). Levin et al compared the *Evaluated Policy* architecture (used in XTS-400) based on a security kernel, Multiple Independent Levels of Security (MILS) based on a *basic separation kernel* and the Least Privilege architecture based on *Separation Kernel Protection Profile*. Figure 10, on the following page, illustrates a current example of the MILS architecture with the Trusted Services Engine (TSE), a Government Off-the-Shelf (GOTS) open source cross-domain file/web server (under development for the US Navy).

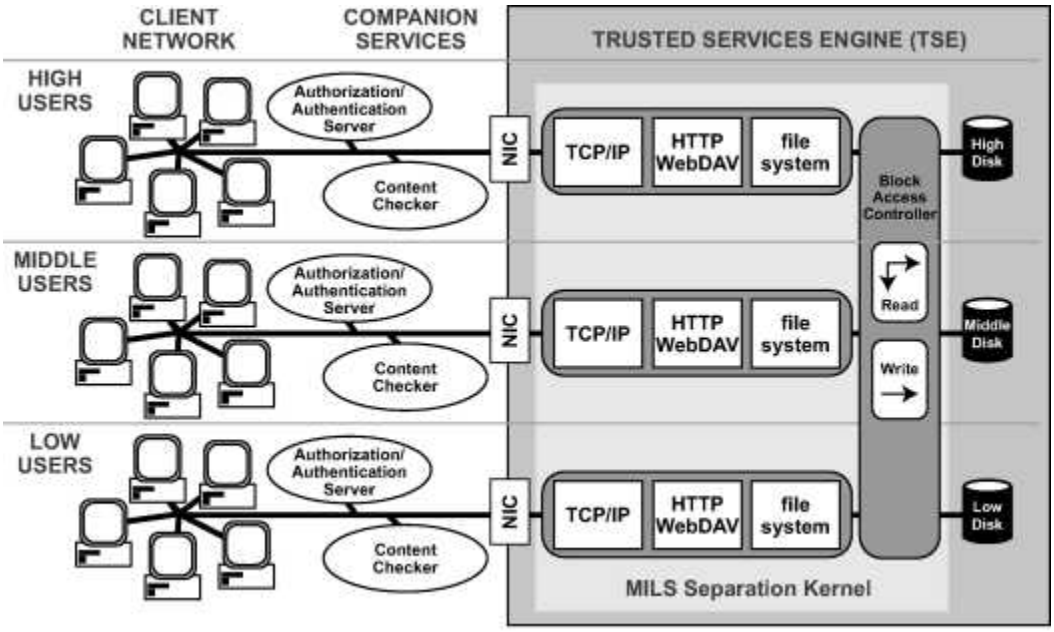


Figure 10: Trusted Services Engine (TSE) Architecture (McNamee et al, 2006)

The TSE is based on the MILS architectural concept and is targeted for EAL6 accreditation. Together with the developmental Multilevel Document Collaboration Server (DocServer), the TSE is expected to permit true cross-domain documents collaboration. Users will connect to a single *virtual* combined file and web server, where they may browse, open, edit and save documents, using available COTS editors, for example, Word 2003. The DocServer will allow XML documents stored on the file/web server to contain regions marked with varying sensitivity level annotations. This is expected to provide a secure execution environment and safe access to multi-level document storage, mediating between user workstations and multi-level document storage to ensure that multiple users can collaborate safely and securely on documents with information marked to different levels of security (McNamee et al, 2006). Since the TSE is consistent with the GIG roadmap, the DocServer application and concept is one that may support a smooth transition from multiple separate networks (the current MLS environment) to the future GIG and black core network. Figure 11, below, illustrates the *publish*, *edit* and *merge* workflow

processes of the DocServer. In this example, an originator chooses to publish a document containing Secret material to an unclassified site. The DocServer filters the document, publishing the content – less the classified material. All users are able to edit the document, based on what they have been allowed to see, with a subsequent merge containing all amendments downstream.

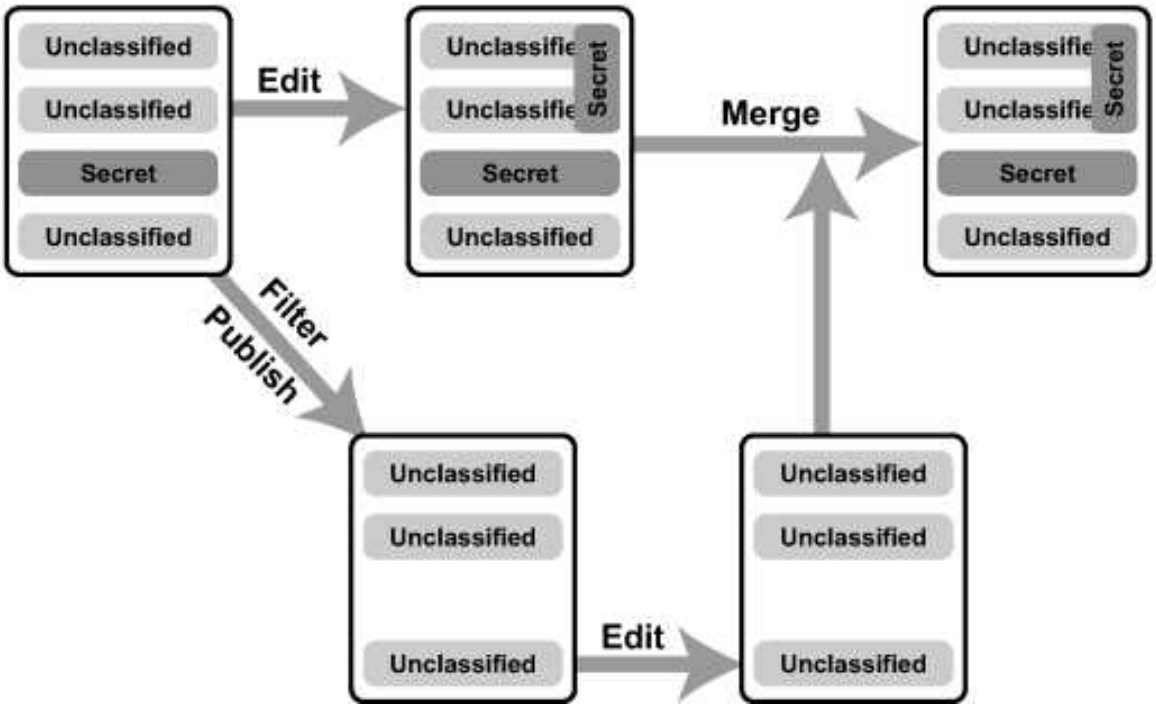


Figure 11: DocServer Workflow Processes (McNamee et al, 2006)

The TSE enforces the information flow envisioned by the Bell-LaPadula model, where users can read at their own level and lower, but can only write within their own level. The capability for read-down should eliminate the need for lower classified data to clutter the higher level's space, reducing storage requirements, making searches easier and reducing human error (McNamee et al, 2006).

Unfortunately, the promise of the GIG, a black-core network and MILS architecture solutions are essentially unavailable for implementation today. Tremendous inroads have been made in the past decade, but technology and accreditation still lag behind the demand.

Chapter 8 – Building Upon Current Technology

Proven and Available Technology

Starting with the realistic assumption that every nation has access to the Internet, either through a firewall on one of its own Intranets or through an independent Internet Service Provider (ISP) at the Delegation, one may question how this could be leveraged to support the consultation process. In fact, many of the Committees and Working Groups that make up the NATO Committee structure are already using the Internet to work on unclassified documents placed on Internet portals. NATO presence on the Internet does not reveal anything in the way of its web server's capability, but high availability and assurance are hampered, pending a significant technology refresh (currently under consideration at NATO HQ). Trusted authentication and access control mechanisms are commercially available, albeit they may be time consuming to setup and modify in consideration of the complicated committee structure (Warner, Atluri and Mukkamala, 2007). Without the use of HTTPS (based on AES, the accepted standard for protecting up to Secret data) ("Committee on National Security Systems", 2003) this contribution to the business process will be limited to unclassified material – at least in the coming year or two. Given that 85% of MINERVA traffic is classified as NR and below, the use of Secure Sockets Layer / Transport Security Layer (SSL/TSL) to secure web transactions should be seen as a potentially significant contributor to the business process, and its implementation and investment should proceed without delay. An appropriately constructed Internet presence

should also enable the use of email, chat and streaming live video (of high level conferences) through the secure site – and should not be limited to only web pages.

The protection of higher classified material with Public Key Infrastructure (PKI) could result in an evolutionary improvement, but considerable work would need to be done to establish the required hierarchy, something that NATO has been considering for several years in order to establish a common robust military messaging system. Any organization that wishes to embrace PKI will need an entity that (Ciampa, 2005, p. 317):

a. Issues digital certificates to users and servers;

b. Provides software that integrates with applications;

c. Integrates all corporate certificate directories; and

d. Manages, renews and revokes certificates.

The use of Virtual Private Networks (VPN) is another area that warrants consideration. A VPN would allow users to establish a protected tunnel from their workplace to a NATO network, at the NR or below level (this would be more difficult to accept for an NC or NS network). However, the bane of VPNs is the potential for an unprotected back door to the Internet, exposing the network to the threat of malicious code. Clients configured for VPN should be "clamped down" so that a user is not able to access the Internet concurrently, through a second network connection – preventing the condition known as *split tunneling* (Weaver, 2007, p. 205). Normally, the protected network faces the Internet with its firewall, IDS, proxy servers, and DMZ. To expose the network to the Internet through a split tunneled VPN connection would put it at risk. While the use of VPNs established through office or home

desktop/laptop computers seems to be commonplace in industry, it is also common for the company that owns the network to own the hardware/software, or at least control the configuration and reduce corporate exposure. Nations are not likely to permit NATO staff to install and configure VPN software on national platforms, for the purpose of reducing NATO risk – particularly when the same equipment needs to be configured for national purposes. Also, national staff would not be interested in setting up a VPN to a NATO network unless they could do so in parallel with connection to one or more of their own national networks, an obviously risky situation.

Coalition Technology Demonstrations and Exercises

Exercise Combined Endeavor and Coalition Warrior Interoperability Demonstration (CWID) provide NATO nations and partners annual opportunities to test current and emerging solutions to address interoperability challenges. Interoperability is certainly a dynamic field, changing every year as nations replace legacy systems and bring into service new equipment. From 2006 onwards, CWID was hosted outside the Continental US, and focused on forward deployments and multi-partner coalitions. Many nations conduct exercises focusing on net-centric operations and multi-national coalition sharing through secure networks ("Global Connections - Coalition Partner Sites", n.d.).

At the May 2007 version of Exercise Combined Endeavor, cooperation between The Netherlands and Canada resulted in the design and test of an Interface Gateway Box (IGB) between the two nations (Lourens, 2007). The approach used was to configure a TACOMS Post 2000 (agreed NATO Standard) Interoperability Point (IOP) in order to enable data exchange between national domains for VOIP, a C2 Information System application (using only an agreed

common data model, but different nationally developed applications) and messaging services. This enabled telephone, email, C2 and chat services at the *mission secret* level between the two nations. Using a common database repository, both nations were able to use their own national C2 application, eliminating any staff-training burden. Future services planned for 2008 testing include web services and VTC. The functionality of the IGB is best described as a service converter from national (proprietary) data formats to generic, standardized formats agreed by NATO and Coalition Communities of Interest. Figure 12 describes the resultant functionality achieved through the configuration of the IGB concept, one for each nation (Lourens, 2007).

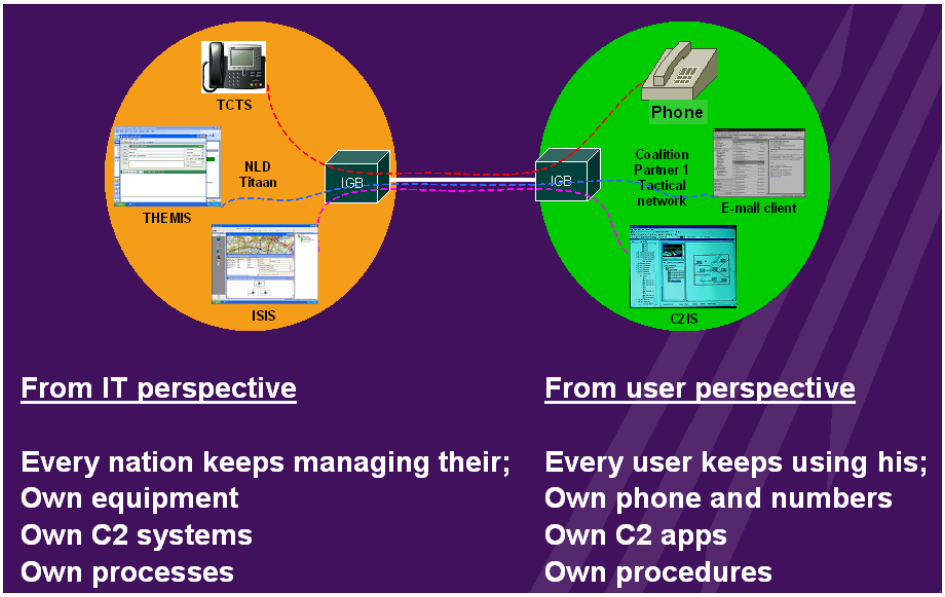


Figure 12: Function Description of an IGB (Lourens, 2007)

Coalition Secure Management and Operations System (COSMOS)

COSMOS is another multinational effort (that includes some NATO nations, but some that are not with NATO) aimed to improve secure sharing of electronic data among coalition forces. The COSMOS project is centered on setting up a Joint Task Force in a theater of

operations and “quickly enabling the sharing of essential information among the coalition partners” (Larsen, 2007). At CWID 2007, a COSMOS solution was tested, building upon the use of the same common data model as mentioned in the preceding paragraph describing the IGB (“Coalition Secure management and Operations System (COSMOS) - Technical Interoperability Results”, n.d.). The developed COSMOS Information Management Tool capabilities include “the creation, management, monitoring and control of information-sharing across Coalition C2 system boundaries” (“COSMOS Aims to Facilitate the Exchange of Data Among Allies”, n.d.).

NATO Cooperative Zones

The NATO Consultation, Command and Control (C3) Agency (NC3A) has introduced the concept of combining symmetric Cooperative Zones to form Information Exchange Gateways (IEG) (Diepstraten and Parker, 2003). This concept addresses the author’s concerns expressed at Chapter 6 vis-à-vis ownership, physical placement and configuration control of the DMZ and BPS components. From an operational point of view, the NC3A characterizes an IEG by two distinguishing features:

a. Information services that pass through the gateway (mail, web, VTC, VOIP as well as management services such as simple network management protocol (SNMP) and domain name service (DNS));

b. The difference in security domains (which can lead to developing gateways to accommodate NATO nations, and also non-NATO nations and NGOs).

The different security domains have led to the development of different “cases” or “scenarios” depending on what the network security classification is, and who operates and

manages it (“Information Exchange Gateway”, n.d.). Case B is where NATO nations connect their networks to the NS WAN. The Cooperative Zone architecture resembles a “screened subnet firewall configuration based on a bastion host that provides authentication and proxy services” (Diepstraten and Parker, 2003, p.2). The Cooperative Zone DMZ is insulated through two Boundary Protection Devices (BPD). Figure 13 depicts the deployment of the NC3A IEG concept using security and proxy functions established in the Cooperative Zone.

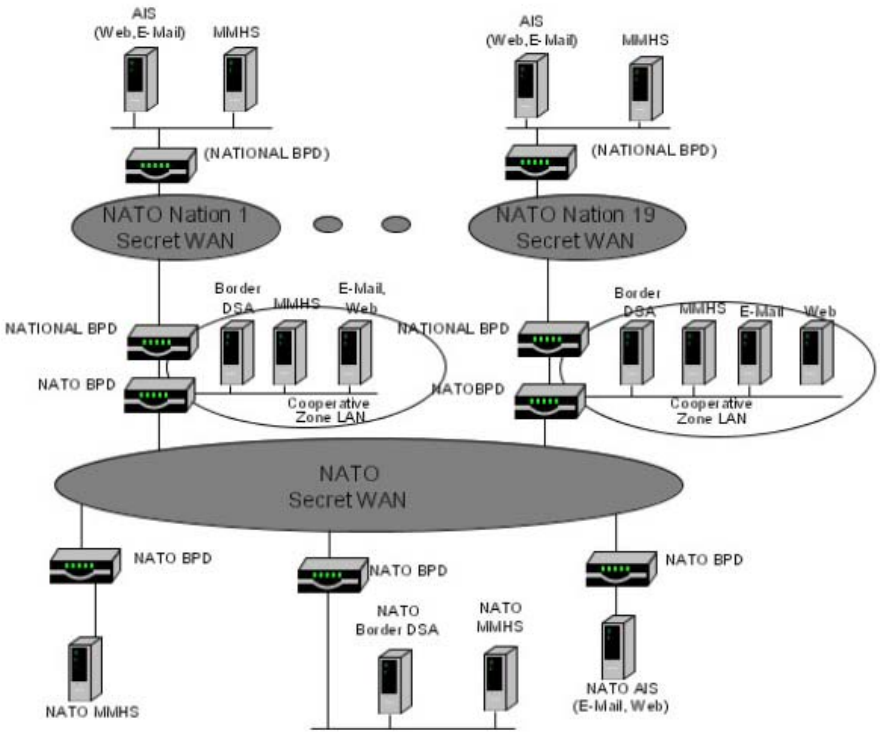


Figure 13: IEG concept with security and proxy functions established in the Cooperative Zone. (“NATO C3 Technical Architecture”, 2005, p.8)

“National systems communicate with NATO via corresponding proxy functions in the Cooperative Zone LAN. The proxy function again communicates with the corresponding NATO system or another nation’s proxy across the NS WAN” (“NATO C3 Technical Architecture”, 2005, p.7). Inside the Cooperative Zone there should be at least a DNS server, Directory Service

Agent (DSA), and Military Messaging Handling Server (MMHS). The intention is that NATO nations will connect to Regional Gateways containing Cooperative Zones ("Information Exchange Gateway", n.d.). Nations will be responsible for the costs of the National BPD and Cooperative Zone LAN, although NATO will be responsible for the NATO BPD and configuration and operation of the LAN services. Nations will also not be restricted in their selection of the National BPD, which could be an IDS or even a full CDS, as described at Chapter 6. A Cooperative Zone has also been described as essentially "an extended border protection device, providing application proxies as well as firewall capability and IDS" (Parker, 2005, p.8). The IEG concept has been developed and tested, and a contract has been awarded to construct the backbone of Regional gateways where nations may be able connect. This Regional gateway construct is consistent with the US view of CENTRIXS expansion, to include connections to NATO and member nations (Parker, 2005).

In summary, several alternative solutions for connecting different networks together in a trusted environment have already been tested on exercises and demonstrations. This cycle of configuration and testing will continue to contribute to the realization of emerging commercial products, eventually replacing the CDS described in Chapter 6. The NATO architecture of Regional IEGs and Cooperative Zones recognizes the requirement for interconnection with national networks, and in time, may result in a significant reduction in air-gaps, experienced both in the HQ and tactical environment. Improved availability and assurance by leveraging Internet transport solutions and the use of SSL/TLS will also improve the consultation process.

Chapter 9 – Findings and Analysis

The author's experience working at NATO HQ gave rise to the knowledge of an information exchange problem, detracting from the key business process of consensus building. Following a comprehensive literature review and research period, including consultations with key staff, it is apparent that technological solutions are available. The different potential solutions are briefly described in the following paragraphs.

Data Diodes

At this time, the use of one-way Data Diodes has been limited to moving data from system low to system high networks. Since the consultation process depends on the *exchange of information*, although the utility of Data Diodes cannot be dismissed, this one-way transfer hampers their potential contribution to the business process. However, at least one vendor (Fort Fox) is working on a two-way Data Diode, effectively with the inclusion of a supervisor responsible to vet material that moves down to the lower network. The pending successful accreditation and installation of this device could make a noticeable contribution to the consultation process. With a two-way Data Diode, data could be securely moved and logged between the current NATO MINERVA LAN and national networks, at practically any level.

Cross-Domain Security Guards

Several accredited CDS exist in both the North American and European markets. Despite their inherent limitations, they are the only current technological solution that can provide regulated and secure information transfer across networks. Since the expansion of CENTRIXS has envisaged a NATO variant, it is only a matter of time before this solution is available, and

ready for nations to connect with the NS WAN - consistent with the NATO IEG architecture. When CENTRIXS is ready, nations would be wise to connect with it.

MLS

When accredited, true MLS should go a long way to satisfy the problem expressed in this paper concerning air-gaps between networks. The concept of *discovery* will play an important aspect in advancing meaningful sharing amongst coalition partners. This is consistent with the vision for transition to a Web Services and Semantic Web environment (Reed, 2004). The GIG vision for a black core network, allowing virtually any classified data to be transported to any destination sounds very promising, but unfortunately, this technology is not currently available, and may not be for many several years.

Use of the Internet

Security rules governing the handling and storage of NR and below data are quite relaxed in comparison with those governing NC and above. NATO HQ is currently studying the potential benefits of configuring and installing a Business LAN at the NR level, running in parallel with MINERVA (at the NS level) – as a result of the revealing statement that 85% of MINERVA data is classified at NR and below. If the deployment of this Business LAN is done in conjunction with a significant technology refresh for the NATO presence on the Internet (to include sufficient availability and security with SSL/TLS), nations may be well poised to take advantage of this – both in the Delegations on site in Brussels as well as in the national capitals. Banking and financial institutions have been making use of HTTPS for several years, and this technology is well suited to revitalizing the consultation process. Investment at NATO HQ itself and its Internet presence would result in this improvement, with no subsequent required

investment on the national side. This assumes that nations have adequate Internet access, either through an ISP or firewalls on their Intranets. However, this would then set the conditions for split information storage, compared to the current system high method of storage on a DMS.

As a technology, VPN is an enabler when used on national and NATO networks - tunneling through the Internet. However, in order to be of any practical advantage to national staff members that are trying to exchange information with NATO and capital staff, they need to be able to work with at least two networks at one time. Unfortunately, this will setup the undesirable condition of split tunneling, not allowed by most security policies – and diminishing the practicality of using VPN.

Project Summery

In summary, this project fully met the goals of describing the information exchange problem and prescribing incremental solutions based on research and literature review. Since the business process is so dependent upon the success of consultation and the achievement of full consensus among members, even the lack of participation of a single member nation will be seen to hinder success. Additionally, even with the full cooperation of all nations, although most technological solutions will be helpful, improvements to the consultation process will be difficult to measure.

By drawing attention to the requirement to embrace technological solutions, this paper should be of interest to NATO HQ staff and NATO member nations, reflecting on the obvious potential for immeasurable added value to the business process. Follow-on work may delve into

describing a solution for a highly available and secure NATO Internet presence, citing firewall, DMZ and IP addresses in detail.

Chapter 10 - Conclusions

The proliferation of stove-piped networks over the past decade has contributed to the increase in network air-gaps or *sneaker-nets*. National staff working at NATO HQ are routinely required to review and sift data originating on either NATO or national networks and move it across domain boundaries – in support of the business process. This business process depends on the efforts and success of individual staff members in order to review documents, and consult with their national subject matter experts with the aim of achieving 100% consensus amongst Alliance members. This paper confirmed that a significant information exchange problem exists at NATO HQ detracting from the key business process of building consensus.

Following a literature review and period of research, it has been determined that solutions to mitigate the negative consequences of air-gaps are at hand, but NATO and nations need to embrace them on an incremental basis. Unfortunately, since lack of consensus can ultimately be attributed to even a single nation, all NATO members need to adopt the attitude of *duty-to-share*, vice *need-to-know*, which has existed as the predominate modus operandi for decades. Both nations and NATO staff need to consider and adopt solutions resulting from risk management, vice risk avoidance. Additionally, although options for MLS seem to be on the horizon, the length of time to achieve accreditation cannot be dismissed, and it is not recommended to wait for these products to reach maturity before taking action.

As an immediate measure, NATO HQ should improve its presence on the Internet, building on the desired tenets of availability and security. This should allow staff working either

at NATO HQ or national capitals the flexibility of downloading and uploading NATO documents classified at NR and below over the Internet in a secure fashion. The implementation of CDS between national classified networks and the NS WAN, when supported by CENTRIXS, should also result in noticeable improvements. Additional work, if required, could delve into the architectural details of an improved NATO Internet presence, embracing available and secure technology that has been in common use in the banking industry for more than a decade.

List of Figures

ANNOTATED BIBLIOGRAPHY

Alberts, D.S., Gartska, J.J., Hayes, R.E., Signori, D.A., (2001). *Understanding Information Age Warfare*. Washington. CCRP Publication Series. DoD Command and Control Research Program, 24-69.
This is a good book that sets out the initial principles for networking command and control information systems. It introduces and examines the principles of Information Superiority and Network Centric Warfare and defines the requirements for collaboration and synchronization.

Alberts, D.S., Hayes, R.E. (2005). *Power to the Edge – Command and Control in the Information Age.* Washington. CCRP Publication Series. DoD Command and Control Research Program, 27-57.
This is an excellent book for laying out the groundwork behind transformational speak and the increased effectiveness gained with networking. The authors explain why current command and control concepts, organizations and systems are lacking. It sets out that organizations that are agile will be significantly more effective. It does not offer technical solutions per se.

Atkinson, S.R., Moffat, J. (2005) *The Agile Organization – From Informal Networks to Complex Effects and Agility*. Washington. CCRP Publication Series. DoD Command and Control Research Program, 89.
This is another useful reference book on the benefits of net-centricity. The authors use more examples from nature and business to show that collaboration and self-synchronization are not only beneficial, but naturally occurring phenomenon.

A Preferred Solution For High-Security Real-time Electronic Data Transfer Between Networks. (n.d.), 11, Retrieved on 16 January 2008 from: http://www.datadiode.eu/uploads/whitepaper/foxit_ffdd_whitepaper.pdf
The vendor Fox-IT provides a hardware based data diode enabling real-time one-way transfer of data between networks. The equipment uses a gigabit optical data link for fully automated transfer, and can also provide one-way email, web mirroring and transfer logging. The company is working on a two-way email system (in reverse from the red to black network) that will require operator vetting.

Bell-LaPadula model. (n.d.) Retrieved on 18 February 2008 from: http://en.wikipedia.org/wiki/Bell-LaPadula_model
This Wikipedia site describes the Bell-LaPadula and Biba Integrity models that fundamentally contribute to the design of Multi-Level Security (MLS) architectures.

Boardman, J., Shuey, D., (April 2004) Combined Enterprise Regional Information Exchange System (CENTRIXS): Supporting Coalition Warfare World-Wide.
Lockheed Martin Information Technologies. Department of the Air Force. Retrieved on 23 January 2008 from:

http://www.au.af.mil/au/awc/awcgate/ccrp/centrixs.pdf
CENTRIXS is currently a network of many coalition networks, configured to suit the information sharing needs of each particular operation and membership. A concept figure in the paper shows a connection between CENTRIXS and CRONOS (Crisis Response over NATO Open Systems), which is another name for the NATO Secret WAN - that is connected to the NATO HQ LAN MINERVA (operating at NATO Secret). The overall expansion of CENTRIXS to meet this and other linkages remains unsatisfied despite articulation of the operational requirement in April 2001. One-way browsing, two-way email/chat/collaboration are based on trusted cross-domain guards (email guards for SIPRNet email, and Radiant Mercury guards for formatted message text data and imagery) between SIPRNet and each CENTRIXS variant (essentially a bilateral relationship between the USA and each member of the particular coalition). This ignores the difficult challenge of trying to interconnect the variants themselves. To achieve the future goal of becoming a single, common, global, multinational data network, a certified Multilevel Security (MLS) solution is desperately needed.

Ciampa, M. (2005). *Security + Guide to Network Security Fundamentals Second Edition*, 317, Thompson Course Technology.
This is a core textbook for Regis University School for Professional Studies MSCT 670.

Coalition Secure management and Operations System (COSMOS) - Technical Interoperability Results. (n.d.) Retrieved on 28 January 2008 from: http://www.cwid.js.mil/public/CWID07FR/htmlfiles/314int.html
The 2007 execution of the annual Coalition Warrior Interoperability Demonstration (CWID) demonstrated the basic functionality of COSMOS - automated, machine-to-machine information exchange of Command and Control (C2) data between coalition members in the international standard format Command and Control Information Exchange Data Model (C2IEDM).

Committee on National Security Systems. (June 2003) *National Policy on the Use of the Advanced Encryption Standard to Protect National Security Systems and National Security Information*. U.S. CNSS Policy No. 15 Sheet No 1.
The National Security Agency (NSA) approved AES to protect classified U.S. traffic, an unprecedented action in the world of high-assurance encryption. Because the algorithm is publicly available, coalition partners can independently implement the algorithm and with a common key, they can securely exchange information.

Common Criteria - An Introduction. (n.d.) Retrieved on 28 January 2008 from: http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf
The Common Criteria represents the efforts of international development to determine criteria for evaluation of IT security that are accepted by the International Standards Organization (ISO) and widely useful within the international community. It builds on work from existing European, US and Canadian criteria (ITSEC, TCSEC and CTCPEC respectively) and resolves differences in their format. Of interest to this paper,

the Common Criteria contains a set of defined Evaluation Assurance Levels (EAL) partly to provide backward compatibility to source criteria, but more importantly to provide consistent general purpose assurance packages that can be used to described standards required for classified and unclassified systems.

Common Security Vulnerabilities in e-commerce Systems. (n.d.) Retrieved on 15 January 2008 from:
http://www.securityfocus.com/infocus/1775
This site describes a number of well known vulnerabilities with web site construction, use and manipulation.

Connors, C. Malloy, M., Masek, E. (December 2006) *Enabling Secure Interoperability Among Federated National Entities: It's a Matter of Trust.* XML 2006 Conference. 3, Retrieved on 22 January 2008 from:
http://2006.xmlconference.org/proceedings/103/presentation.pdf
To date, federated secure information sharing has relied upon pre-arranged information exchange agreements on a bi- or multi-lateral basis that require complex, human-centric and time intensive processes to create or modify. This paper sets out a vision to support information sharing by establishing domain functional areas, and discovery metadata standards that leverage existing information through security filtered published data sets. The concept of Discovery will be an important aspect for advancing meaningful sharing among coalition partners. Generically, Discovery refers to finding and retrieving actionable, decision-quality information "on the- fly" as opposed to such pre-engineered approaches.

Consensus Decision Making at NATO - A fundamental Principle. (n.d.) Retrieved on 26 January 2008 from:
http://www.nato.int/issues/consensus/index.html
This NATO site explains the importance of reaching consensus at NATO HQ, resulting in collective decision making.

COSMOS Aims to Facilitate the Exchange of Data Among Allies. (n.d.) Retrieved on19 February 2008 from:
http://www.cadrc.calpoly.edu/pdf/Currents_Fall_2007.pdf
This site provides comment on the recent success of the COSMOS multinational effort to achieve secure interoperability amongst coalition allies.

Crocker, M. Cross-*Domain Information Sharing in a Tactical Environment*. (March 2007) CrossTalk – The Journal of Defense Software Engineering. Retrieved on 15 November 2007 from:
http://www.stsc.hill.af.mil/crosstalk/2007/03/0703Crocker.html
The author stresses the importance of a net-centric operational environment, and timeliness of complete, trusted information sharing. He criticizes the use of legacy cross-domain solutions such as the certified security guard Radiant Mercury. He says that

security guards work well to constrain the movement of data from one domain to the next (at differing levels) and at protecting the transfer of malware, but do little to mitigate the risks posed by insiders. He cites several technology advancements that could be utilized to better construct security guards (use of the Advanced Encryption Standard (AES) easing the development of common keys to be shared by coalition partners, multiple level security through purpose-built architecture/software/hardware, and the use of metadata security labels and strong search engines).

Cross Domain Solutions. (n.d.) Retrieved on 21 January 2008 from: http://en.wikipedia.org/wiki/Cross_Domain_Solutions
This is a good introduction to the science of developing, assessing and deploying Cross Domain Solutions (CDS) – founded on risk management. Previous decades have focused on enforced Mandatory Access Control (MAC) with rigid and deterministic security. However, the increased volume of data, speed of networks and need for information sharing has led to a shift, favoring user balanced information sharing, where access is now influenced by Discretionary Access Control (DAC). A controversy still exists though where some believe that users are incapable of predicting the full consequences of sharing what they believe is necessary within their own small sphere of influence.

CSI / FBI Computer Crime and Security Survey (2006). Retrieved on 17 March 2007 from: http://www.gocsi.com/
This presents the results of an annual survey to determine computer crime and security in the USA. It is a very reputable source. The most notable point is that although 95% of losses are commonly attributed to insiders, or employees, virus attacks continue to be the source of the greatest financial losses.

Defence Terminology Bank. Retrieved on 29 January 2008 from: http://terminology.mil.ca/term-eng.asp
The Canadian Defence Terminology Bank is a compilation of approved Department of National Defence and Canadian Forces terminology - the authoritative online source for Defence Terminology in Canada.

Diepstraten, M., Parker, R. (April 2003) *NATO Automated Information System Co-operative Zone Technologies.* Journal of Telecommunications and Information Technology, 1-2, Retrieved on 15 November 2007 from: http://www.itl.waw.pl/czasopisma/JTIT/2003/4/37.pdf
This is a fundamental document describing a possible solution (circa 2003) using Cooperative Zones (established per nation-NATO connection) and a trusted network. The cooperative zones provide boundary protection with routing, firewall, IDS and proxy service - but no mention of content checking (presumably part of the trust arrangement). The paper defines the NATO Information Exchange Gateway (IEG) consisting of symmetric cooperative zones that support directory services, email and web services - that has been tested and validated on a NATO test bed. The NATO HQ situation would follow the Case B situation and require both web proxy and reverse proxy based on

access controls. Case C involves Non-Governmental Organizations (NGO) and is envisioned, but more difficult to achieve. The article provides a large number of NATO references that although unclassified - are not publically available.

EAL4 accredited solutions for military, defense and intelligence security. (n.d.) Clearswift. Retrieved on 28 January 2008 from: http://www.clearswift.com/products/specialist/default.aspx
Clearswift is another milspec vendor of cross-domain security solutions, accredited to EAL4 standard. Two products are of direct interest to this paper: Bastion™ (providing assured separation of networks operating at different levels of trust), and DeepSecure™ (providing assured network boundary protection and inspected of encrypted emails). Clearswift claims (with confidence to EAL4) that in a cross-domain solution, an electronic air gap with automated content inspection provides much higher security than a conventional air gap (due to the human involvement in moving the media across the network gap). All critical mail should be content checked, archived and screened automatically for release against sensitivity, policy and originator, validated by digital signature.

Executive Order. (n.d.) Further Amendment to Executive Order 12958, As Amended, Classified National Security Information. Retrieved on 9 January 2008 from: http://www.whitehouse.gov/news/releases/2003/03/20030325-11.html
Although much discussion is found on the Internet relating to this Order, it serves a purpose to define the basic Classification Levels of "Top Secret", "Secret" and "Confidential". These classification levels and their description are important to understand the basis for classified information and how it can fall into different levels.

Global Connections - Coalition Partner Sites. (n.d.) Retrieved on 18 December 2007 from: https://www.cwid.js.mil/public/CW06coalition10May.pdf
Coalition Warrior Interoperability Demonstration (CWID) is an annual event, hosted by the US European Command, with the aim of investigating interoperability issues with coalition partners. From 2006 onwards, CWID was hosted outside the Continental US, and focused on forward deployments and multi-partner coalitions. Many of the participants conducted exercises that focused on net centric operations and multi-national coalition sharing through secure networks. Although this site is not a useful source of the outcomes, or description of the technical issues, CWID is known to be a valuable, annual resource.

Information Exchange Gateway (IEG). (n.d.) Retrieved on 15 November 2007 from: http://194.7.80.153/website/book.asp?menuid=15&vs=0&page=volume2%2Fch02s07.html
This is an extract from the NATO Consultation, Command and Control Agency (NC3A) Technical Architecture site on the Internet. The NC3A is one of 13 NATO agencies. In particular, the NC3A's mission is to support NATO through unbiased scientific support and common funded acquisition of Consultation, Command, Control, Communications,

Intelligence, Surveillance and Reconnaissance (C4ISR) capabilities. In line with the NC3A's vision for an Overarching Architecture, at the strategic level, the IEG concept aims to support the political consultation process and improve planning. The site defines four scenarios where IEGs may be used but falls short of providing a technical description of any.

Integrated Information Assurance - XTS 300 Solution Suite. (n.d.) BAE Systems. Retrieved on 28 January 2008 from: http://www.digitalnet.com/solutions/information_assurance/xts300sol_ste.htm
Like its successor, the XTS-400, the BAE XTS-300 is a multi-level secure computer system, originally developed by BAE Systems, and transitioned from proprietary, mini-computer hardware to COTS, Intel x86 hardware. The XTS-300 completed security evaluation in 1994 at the B3 level and is (or has been) in common use in cross-domain solutions for up to Secret level. The DigitalNet XTS-300 and the STOP operating system are collectively referred to as the Defense Information Infrastructure (DII) High Assurance Guard.

Kriendler, J., (June 2005) *NATO Headquarters Transformation: Getting Ahead of the Power Curve.* Defence Academy of the United Kingdom. Conflict Studies Research Centre. 7-9, Retrieved on 28 January 2008 from: www.da.mod.uk/colleges/csrc/document-listings/special/05(29)-JK.pdf
The author conducted interviews with over 60 high ranking civilian and military officials working at NATO HQ and SHAPE in the latter part of 2004, in an attempt to focus on the non-military aspects of transformation at NATO HQ (institutional and political change). Although there is nothing in this paper concerning the requirement for technology upgrades, there are several useful quotes of how the current procedures for building consensus are not up to the task. There is agreement by nations that the need for 100% consensus will stay, but it's just a question of how to make it work effectively.

Larsen, P.G., *Coalition Command and Control (C2) Interoperability Challenges*. (2007) Retrieved on 15 November 2007 from: http://www.dodccrp.org/events/11th_ICCRTS/html/papers/124.pdf
This is a good introductory paper that sets out the basic challenges confronting military units that conduct coalition operations involving forces from different countries. It introduces the Community of Interest (COI) term and defines levels of interoperability from Level 0 to Level 4. It describes the use of the C2IEDM and MIP gateways – both have an important role to play on the battlefield but are not required at the NATO HQ strategic level. It also introduces the COSMOS project, aimed to solve sharing of information through different networks with appropriate security guards.

Levin, T., Irvine, C., Weissman, C., Nguyen, T., (November 2007) *Analysis of three multilevel security architectures.* Proceedings of the 2007 ACM workshop on Computer security architecture, ACM, 37, Retrieved on 23 January 2008 from: http://delivery.acm.org.dml.regis.edu/10.1145/1320000/1314473/p37-

levin.pdf?key1=1314473&key2=3153311021&coll=ACM&dl=ACM&CFID=51285889&CFTOKEN=77909174
The authors state the persistent requirement for multilevel security architectures, as opposed to the system high approach that is nearly the status quo. They analyze the relative merits of three current MLS architectures: Evaluated Policy architecture based on a security kernel (XTS-400 for example), Multiple Independent Levels of Security (MILS) architecture based on a basic separation kernel, and a new architecture based on Separation Kernel Protection Profile or Least-Privilege architecture. Each architecture was compared with respect to different usability factors. The authors' analysis showed that Least-Privilege and Evaluated Policy architectures provided better assurance, although they admit their results are not all-inclusive. They had no metrics to compare how the architectures might differ in their prevention of covert channels, for example.

Loscocco, P., Smalley, S., Muckelbauer, P., Taylor, R., Turner, J., Farrel, J., (1998) *The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments.* National Security Agency, 1, Retrieved on 21 January 2008 from: http://csrc.nist.gov/nissc/1998/proceedings/paperF1.pdf
The authors build a case for revisiting the ever increasing need for a sound basis to build applications on - a secure operating system. Weakness in design, poor implementation and flawed environmental assumptions will predictably result in vulnerabilities. Although this paper is 10 years old, these comments still ring true.

Lourens, H., (12 July 2007) *Information Briefing on the NLD IGB To The Working Group of National Technical Experts COM and ADP.* Netherlands Defence Materiel Organisation. Retrieved on 13 January 2008 from: http://www.vovklict.nl/site_documentation/diversen/IGB.pdf
The briefing summarizes Netherlands results achieved during Exercise Combined Endeavour 2007, where cooperation with Canada resulted in the design and test of an Interface Gateway Box (IGB) between nations. The approach was to construct and use a TACOMS Post 2000 (agreed NATO Standard) Interoperability Point (IOP). The use of an IOP between nations enabled data exchange between national domains for VOIP, Command and Control Application and messaging services. Future services planned for 2008 testing are HTTP, VTC and Chat. The functionality of the IGB is best described as a service converter from national (proprietary) data formats to generic, standardized formats agreed by the NATO MIP and TACOMS communities.

MacMillan, K., Shimko, S., Sellers, C., Mayer, F., Wilson, A., (2 March 2006) *Lessons Learned Developing Cross-Domain Solutions on SELinux*. Retrieved on 17 January 2008 from: www.tresys.com/files/docs/CDS-SELinux-Symp.pdf
Tresys Technology has been involved in building Cross-Domain solutions using the more powerful and flexible form of Mandatory Access Controls (MAC) known as type enforcement (TE) that is the central security feature of Security Enhanced Linux (SELinux). They believe that TE provides an excellent MAC mechanism for separating information domains and creating processing pipelines.

McNamee, D., Heller, S., Huff, D., (May 2006) *Building Multilevel Secure Web Services-Based Components for the Global Information Grid*. CrossTalk – The Journal of Defense Software Engineering. Retrieved on 15 November 2007 from: http://www.stsc.hill.af.mil/crossTalk/2006/05/0605McNameeHellerHuff.html
US DoD ambitions to create a Global Information Grid (GIG) will be based on web services and standard IP, interchangeable components, and the use of COTS hardware and software - some of which must be built to higher than commercial standards. This article describes the Trusted Services Engine (TSE) (in development) and the Multilevel Document Collaboration Server (DocServer) - the use of both are expected to contribute immensely to a cross-domain data solution in a multi-layer security environment. When tested, the authors demonstrated the possibility for cross-domain collaboration within documents, across different security domains. Common Criteria evaluation and commercialization were predicted for 2007, although an Internet search conducted on 18 February 2008 did not yield any news of accreditation.

Mineweaser, J., *Internet Engineering Task Force (IETF) 66 Meeting Minutes*. (13 July 2006) Montreal. Retrieved on 18 February 2008 from: http://www.ietf.org/proceedings/06jul/minutes/SAMRG.txt
These proceedings document discussion over a number of different topics, of note – comments on the US GIG and black core network. US DoD ambitions to create a Global Information Grid (GIG) by 2020 are based on the utility of web services and standard IP but running over a black or protected core. This requires the encryption of all data at source, based on SSL/TLS – and this remains "a key challenge for network architecture" (Mineweaser, 13 July 2006).

Multi-Domain Security and its Impact on Network Centric Operations. (n.d.), 4, Retrieved on 23 January 2008 from: http://www.c-d-r.net/MDS.doc
This is a difficult to reference, but useful document. Although the c-d-r website is credible, the source of the material is largely unknown. The increase in IT processing speed has not directly resulted in the correct identification of evolving situations, responses and actions required. Further to Multi-Level Security (MLS), this paper introduces the concept of Multi-Domain Security (MDS) and offers risk management approaches. Independent networks are linked together through MLS guards, based on specialized, application layer firewalls - typically based on a trusted operating system (like Trusted Solaris for example). MLS enforces security through Mandatory Access Control (MAC). MLS security guards may check the content of attachments against a dirty word list, word distance vectoring and document similarity comparisons - under the term cross-domain solution. Lockheed Martin's Radiant Mercury product guards multiple networks of various classification levels (10 as at 2004) and sanitizes/downgrades/filters. The term MDS arose out of the requirement to connect networks to portions of the Internet, utilizing Google type search access and weblog sites, normally unavailable for secure networks and presenting increasing levels of frustration

for customers. Most MDS solutions are based on Trusted Solaris. The paper also mentions the utility of Data Diodes, and how they can be used to replace a sneaker network.

NATO Awards Nexor Contract for Provision of High Assurance Mailguards. (n.d.) Retrieved on 24 January 2008 from: http://www.nexor.com/content/view/424/246
Nexor (a United Kingdom (UK) producer and vendor of high-grade security products and services for defense and government) announced their selection by NATO to supply high assurance mailguards for operational use. The Nexor Sentinel is said to meet EAL5 and will be used in the NATO Messaging System project and to provide boundary protection services to NATO operational missions.

NATO New Headquarters. (n.d.) Retrieved on 26 January 2008 from: http://www.nato.int/structur/tenders/newhq3/index.htm
NATO agreed in 1999 to construct a new HQ at Brussels, replacing the temporary structure constructed by the Belgian MOD in 1967 (that was intended to satisfy the requirement for three to five years). The building is still under design, but occupancy is expected for 2012. State of the art technology is expected to be deployed, although this is still in the early stages of evaluating customer requirements.

North Atlantic Treaty Organization - Homepage. (n.d.) Retrieved on 3 February 2008 from: http://www.nato.int/
This is NATO's homepage on the Internet. It contains useful information on the Alliance, its members and way of working. It provides many links to further information on transformation and current developments / news.

North Atlantic Treaty Organization. (2006). *NATO Security Policy and Supporting Directives.* NATO Headquarters, Brussels, Belgium (this policy is not releasable to the public)
This security policy describes high-level policy at NATO fixed and deployed or operational sites. It is supported through a number of security directives that describe policy as it relates to Personnel Security, Physical Security, Security of Information, Industrial Security and two volumes that detail Information Security.

NATO C3 Technical Architecture. Volume 2. Supplement 1: Domain Architectures. Version 7.0. (15 December 2005), 7-8, Retrieved on 16 January 2008 from: http://194.7.80.153/website/book.asp?menuid=15&vs=0&page=vol2%2Dsup1%2Fch01%2Ehtml
This is a portion of the most recent, publically available NATO architecture document. The publication describes NATO information exchange, the use of the Alliance Directory and its relation to national Directory Management Domains – as they apply to classified and unclassified networks. This volume sets out to support information exchange at the Secret system level required to support current operations, training and experimentation. It describes the use of Directory Service Agents (DSA) and how they contribute to the

overall architecture. Directory information exposing names, organizational structure and address information is classified and not found on public systems, such as this one. The document also provides a good primer to the TACOMS Post 2000 Architecture – aimed at enabling tactical wired interoperability amongst coalition environments.

O'Sullivan, R., (May 2005) *Networking Coalitions.* Australian Government Department of Defence. Retrieved on 28 January 2008 from: http://www.defence.gov.au/defencemagazine/editions/20050501/groups/cio.htm The author explains that in the past, cross-domain information movement was entirely governed through the use of standardized military messages. The introduction of Griffin (a collaborative classified network between USA/CAN/GBR/NZL/AUS) and CENTRIXS (USA led and managed) has opened up the possibilities for cross-domain email, web services and chat within the coalition networks. CENTRIXS has different variants, depending on the coalition structure. For example, CENTRIXS configuration for operations in Afghanistan and Iraq are different, and there is limited (email only) connectivity between them.

Parker, R., (14 March 2005) *A NATO Perspective on CENRIX*. 8, Retrieved on 16 November 2007 from: http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/007.pdf The Multinational Information Sharing (MNIS) Program within the USA DoD details that the Combined Enterprise Regional Information Exchange System (CENTRIXS) includes a number of cross-domain security programs associated with the sharing of information with foreign nations and forces, as an integrated solution to supporting the combined warfighting environment. The different variations of CENTRIXS maintains the integrity of USA SIPRNET through distinct network configurations tailored to meet the requirements of each coalition. Information is moved between the USA secret environment (SIPRNET) and the Coalition environment through cross-domain guards and content filters (Radiant Mercury). The author explains the basic construct of the NATO General Communication System (NGCS) and how it is used as a secure circuit and packet-switched pipeline for voice, video and data services - connecting NATO Command Structure, Nations and NATO deployed elements. A key NATO concept is the use of Information Exchange Gateways (IEG) based on a set of cooperative zones at NATO facilities exchanging information using agreed services with member Nations and elements of the NATO command structure. NATO networks are currently in an evolutionary change mode, as they continue to be updated and expanded, with a view to increasing interoperability with Nations. There are currently no interfaces between the NATO Secret WAN and the USA classified networks, although a connection with CENTRIXS is envisaged through a NATO Regional IEG.

Phillips, C., Ting, T., Demurjian, S., (June 2002) *Information sharing and security in dynamic coalitions.* SACMAT '02: Proceedings of the seventh ACM symposium on Access control models and technologies. Retrieved on 21 January 2008 from: http://portal.acm.org.dml.regis.edu/citation.cfm?id=507726&coll=ACM&dl=ACM&CFI

D=50950228&CFTOKEN=74772502
This paper highlights the well documented need to accommodate information sharing on-site (ie, in a tactical environment) within a coalition of different nations, military, civilian and Non-Governmental Organizations (NGO) formed in international operations. In practice, this is much more difficult to achieve than static interoperability at NATO HQ, since the composition of the coalition is dynamic and includes NGOs. The paper defines and uses the terms Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role-based Access Control (RBAC), touching on the potential requirement for time-based access as well.

Prague Summit Declaration. 21-22 November 2002. NATO Press Release. Retrieved on 26 January 2008 from:
http://www.nato.int/docu/pr/2002/p02-127e.htm
The Prague Summit of November 2002 was the first of many summits where NATO declared the importance of transforming to adopt new structures, procedures and technologies to counter the new asymmetric threat of terrorism. This particular Summit, is the basis for modern transformation within NATO, following the dissolution of the USSR.

Press Release – Accreditation of Email Transfer and Data Forwarding Applications Results in Complete Turn-Key Cross Domain Solution. (n.d.) Retrieved on 17 January 2008 from:
www.tenixamerica.com/07_Accreditation_2.html
Tenix America is another producer of a hardware Data Diode, using fiber optic. This article touts full accreditation of Tenix America's 100MB Data Diode. The Diode's Email Transfer Application and Data Forwarding Application were evaluated on their ability to mitigate security threats in three areas of concern: confidentiality, integrity and availability. Tenix offers an Enterprise solution that incorporates: one-way email, one-way file transfer, one-way transfer of IP packets and one-way transfer of clipboard data. The clipboard data feature is especially interesting.

Reed, N., (2004) *Security Guards for the Future Web Final Project Report.* Mitre Center for Integrated Intelligence System. 1-18, Colorado Springs, Colorado.
This report details research during 2003/2004 into three potential areas for future security guards for future web traffic: a Browser-based environment (essentially today's environment), a Web Services environment, and a Semantic Web environment. It provides a good explanation of what constitutes commonly available security guards. It explores the near-term potential with XML guards, although not yet commercially available.

RFC 2828 - *Internet Security Glossary.* (n.d.) Retrieved on 15 January 2008 from:
http://www.faqs.org/rfcs/rfc2828.html
This Glossary provides abbreviations, explanations, and recommendations for the use of information system security terminology. (detailed in 191 pages of definitions and 13 pages of references)

Roberston, G. (2004) *Transforming NATO to Meet the Challenges of the 21st Century.* Transatlantic Transformation: Equipping NATO for the 21st Century, Washington, DC, Center for Transatlantic Relations, 30.
The former Secretary General of NATO made some strong comments on the challenges of transforming NATO.

SecureOffice Trusted Gateway on Linux. (n.d.) Retrieved on 28 January 2008 from: http://www.tcs-sec.com/products/TrustedGatewayLinux.html
Trusted Computer Systems offers a cross-domain solution built on a Linux server platform, the first secure Linux operating system to enter evaluation at EAL4. This builds upon the Trusted Gateway System (TGS), fielded and operational for more than ten years. This solution can be used with Unix clients, or on Windows 2000 or above. It is not limited to any arbitrary combination of networks (could be used as 26:1 with NATO HQ for example), and provides secure, multi-directional data transfer using a graphical, web-based client interface. It has options for dirty word search and two-person review (originator and reviewer) when moving data from a high to lower classification. Users are able to request data movement in any direction, based on their security clearance, site security policies and user access rights.

Shehab, M., Bertino, E., Ghafoor, A., (November 2005) *Secure collaboration in mediator-free environment.* CCS '05**:** Proceedings of the 12th ACM conference on Computer and communications security. ACM. Retrieved on 22 January 2008 from: http://delivery.acm.org.dml.regis.edu/10.1145/1110000/1102130/p58-shehab.pdf?key1=1102130&key2=2786401021&coll=ACM&dl=ACM&CFID=51097838&CFTOKEN=98148372
This article is hardly relevant, but does point out that despite the advances of the Internet (which has made multi-domain collaboration a reality), the lack of interoperation between domain access control policies may give way to security breaches. The authors have promoted a framework where the user's access path is used to provide domains with sufficient information to enable secure access control decisions. They also advocated a path authentication scheme providing increased security to the path as it moves through domains.

Silberglitt, R., AntÃ³n, P., Howell, D., Wong, A. (2006) *The Global Technology Revolution 2020, In-Depth Analyses*. Copyright © 2006 RAND Corporation.
It is useful to extract a few comments from this study that speak to the potential institutional difficulties in implementing new technologies. NATO member nations are on their own recognizance when it comes to implementation. There may be drivers or barriers that come to play, certainly impacting on the Alliance as a whole.

Swamy, N., Hicks, M., Tsang, S., (October 2007) *Verified Enforcement of Security Policies for Cross-Domain Information Flows*. Proceedings of the 2007 Military Communications Conference (MILCOM), Retrieved on 21 January 2008 from:

http://www.cs.umd.edu/~nswamy/papers/cpa-milcom07.pdf
The downside of typical cross domain guards is that content checkers may be too rigid (inhibiting information sharing) in their enforcement of the cross domain security policy. Alternatively, they may be too permissive and not able to realize the larger picture of the information that has moved across the guard. The authors advocate a framework of dynamic association between security labels (using SELinks metadata) and sensitive objects. Much more work has yet to be done to industrialize this concept.

Tenix Data Diode – Absolute Information Protection. (n.d.) Retrieved on 10 February 2008 from:
http://www.tenixamerica.com/products.html
This is the Tenix America site for public information on its Data Diode product. General product requirements and technical specifications are available for the Interactive Link Data Diode, one-way email transfer, one-way data transfer, one-way data and clipboard transfer. The products are accredited for use in government applications.

The Consultation Process - Reaching Consensus. Retrieved on 26 January 2008 from:
http://www.nato.int/issues/consultation/index.html
Continuous informal and formal dialogue is part of the consensus building process at NATO HQ. Consultation and consensus have been a cornerstone of the business process at NATO HQ since the foundation of the Alliance in 1949. These working procedures are still in place.

Thuppal, R., (12 December 2007) *Comd-Net, SIGNET-C and ADM(POL) Information Exchange Gateway*. vs0.72. DIMEI-8. Canadian Department of National Defence.
This unclassified document provides the design specification for the information exchanges between 3 classified networks (all at Secret level) but with different release caveats. Two networks are designated Canadian Eyes Only (CEO), and the third network is designated Secret releasable Canada-United States. The document provides a high-level specification, based on defined web browsing activities (specifying which network can browse openly or specific web data within other sites) and the requirement for content checking of emails and attachments. The firewall design is based on a hardware platform supplied by the Secure Computing Cyberguard TPS appliance. Antivirus and content checking are to be done by the application Alladin eSafe v5.1 running on a DII Guard (based on current accreditation status).

Thuppal, R., (31 October 2007) *Interactive Link - System Design Specification*. vs0.13. DIMEI-8. Canadian Department of National Defence.
This unclassified document provides the design specification for the Interactive Link System - a capability to securely transfer data from a lower classified network to a higher classified network while preventing any possibility of data leakage. It provides the high-level and technical details to which the end system must conform. The Interactive Link Keyboard Switch is most interesting since it allows users to securely access two separate networks from a single workstation, using thin client technology to display the less secure

network in a window on the secure PC. Users can access email, web and public networks without compromising security and removes the purchase and running costs associated with the second PC. One way transfer of emails, files and clipboard data is easily supported. The Interactive Link software installs on the High Network and Low Network Diode Servers to coordinate data transfer. In the document, Tenix Data Diode products are specified, together with EAL7 (Common Criteria) and E6 (ITSEC) accredited servers in order to provide the requisite high level of assurance (the design specification actually serves 3 networks: unclas/secret/TS).

Trusted Solaris 8 Operating Environment. (n.d.) Retrieved on 24 January 2008 from: http://www.sun.com/software/solaris/trustedsolaris/features.xml
This webpage describes Sun's EAL4 evaluated operating system.

Warner, J., Atluri, V., Mukkamala, R., Vaidya, J., (June 2007) *Using semantics for automatic enforcement of access control policies among dynamic coalitions*. SACMAT '07**:** Proceedings of the 12th ACM symposium on Access control models and technologies. ACM. Retrieved on 22 January 2008 from: http://delivery.acm.org.dml.regis.edu/10.1145/1270000/1266877/p235-warner.pdf?key1=1266877&key2=3056401021&coll=ACM&dl=ACM&CFID=51097838&CFTOKEN=98148372
The authors discuss a method to meet information sharing requirements for coalitions (emergency alliances, peace keeping, military, commercial ventures), but focus on the more difficult problem of dynamic coalitions - that may change frequently. Web sharing can be done using traditional access control and authentication tools, but the initial workload of setting this up can become a burden. Additionally, with a coalition, the necessary interactions may be short lived, and can change frequently. Typical access control policies are based on "who", but the authors advocate an abstract definition of "who" in order to accommodate staffing changes within organizations. They propose a first step in automating Role-Based Access Control (RBAC), using semantics associated with the user and the user's role, and attributes found in existing information databases. This is work in progress, and not yet found in commercial applications.

Weaver, R., (2007). *Guide to Network Defense and Countermeasures.* Second Edition, 205, Thomson Course Technology.
This is a core textbook for Regis University School for Professional Studies MSCT 672.

Whitman, M.E and Mattord, H.J., (2005). *Principals of Information Security*. Second Edition, 68-385, Thomson Course Technology.
This is a core textbook for Regis University School for Professional Studies MSCT 670. It surveys the discipline of information security, and provides an introduction to both security management and technical aspects.

XTS-400 - BAE Systems. (n.d.) Retrieved on 21 January 2008 from: http://en.wikipedia.org/wiki/XTS-400

The XTS-400 is a multi-level secure computer system, originally developed by BAE Systems, and supporting Gigabit Ethernet and both IPv4 and IPv6. Its secure trusted operating system (STOP) is the only general purpose operating system to meet the Common Criteria EAL of 5 or above. XTS-400 can host, and be trusted with separate networks - and is typically used in cross-domain solutions, guarding information flow between two or more networks of differing security characteristics - when used with a piece of privileged software.

Zellmer, D., (26 March 2003). *Multi-Level Security: Reality of Myth?* GSEC Practical Requirements v.1.4.b. Retrieved on 23 January 2008 from: http://www.delmar.edu/Courses/ITSC1347/eBooks/Multi-Level_Security(Reality-or-Myth).pdf
The author retains full rights of this document. Although it has been read, it has not been used as a reference.

References

Alberts, D.S., Gartska, J.J., Hayes, R.E., Signori, D.A., (2001). *Understanding Information Age Warfare*. Washington. CCRP Publication Series. DoD Command and Control Research Program, 24-69.

Alberts, D.S., Hayes, R.E. (2005). *Power to the Edge – Command and Control in the Information Age.* Washington. CCRP Publication Series. DoD Command and Control Research Program, 27-57.

Atkinson, S.R., Moffat, J. (2005) *The Agile Organization – From Informal Networks to Complex Effects and Agility*. Washington. CCRP Publication Series. DoD Command and Control Research Program, 89.

A Preferred Solution For High-Security Real-time Electronic Data Transfer Between Networks. (n.d.), 11, Retrieved on 16 January 2008 from: http://www.datadiode.eu/uploads/whitepaper/foxit_ffdd_whitepaper.pdf

Bell-LaPadula model. (n.d.) Retrieved on 18 February 2008 from: http://en.wikipedia.org/wiki/Bell-LaPadula_model

Boardman, J., Shuey, D., (April 2004) Combined Enterprise Regional Information Exchange System (CENTRIXS): Supporting Coalition Warfare World-Wide. Lockheed Martin Information Technologies. Department of the Air Force. Retrieved on 23 January 2008 from: http://www.au.af.mil/au/awc/awcgate/ccrp/centrixs.pdf

Ciampa, M. (2005). *Security + Guide to Network Security Fundamentals Second Edition.* 317, Thompson Course Technology.

Coalition Secure management and Operations System (COSMOS) - Technical Interoperability Results. (n.d.) Retrieved on 28 January 2008 from: http://www.cwid.js.mil/public/CWID07FR/htmlfiles/314int.html

Committee on National Security Systems. (June 2003). *National Policy on the Use of the Advanced Encryption Standard to Protect National Security Systems and National Security Information*. U.S. CNSS Policy No. 15 Sheet No 1.

Common Criteria - An Introduction. (n.d.) Retrieved on 28 January 2008 from: http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf

Common Security Vulnerabilities in e-commerce Systems. Retrieved on 15 January 2008 from: http://www.securityfocus.com/infocus/1775

Connors, C. Malloy, M., Masek, E. (December 2006) *Enabling Secure Interoperability Among Federated National Entities: It's a Matter of Trust*. XML 2006 Conference. 3, Retrieved on 22 January 2008 from: http://2006.xmlconference.org/proceedings/103/presentation.pdf

Consensus Decision Making at NATO - A fundamental Principle. (n.d.) Retrieved on 26 January 2008 from: http://www.nato.int/issues/consensus/index.html

COSMOS Aims to Facilitate the Exchange of Data Among Allies. (n.d.) Retrieved on19 February 2008 from: http://www.cadrc.calpoly.edu/pdf/Currents_Fall_2007.pdf

Crocker, M. Cross-*Domain Information Sharing in a Tactical Environment*. (March 2007) CrossTalk – The Journal of Defense Software Engineering. . Retrieved on 15 November 2007 from: http://www.stsc.hill.af.mil/crosstalk/2007/03/0703Crocker.html

Cross Domain Solutions. (n.d.) Retrieved on 21 January 2008 from: http://en.wikipedia.org/wiki/Cross_Domain_Solutions

CSI / FBI Computer Crime and Security Survey (2006). Retrieved on 17 March 2007 from: http://www.gocsi.com/

Diepstraten, M., Parker, R. (April 2003) *NATO Automated Information System Co-operative Zone Technologies.* Journal of Telecommunications and Information Technology, 1-2, Retrieved on 15 November 2007 from: http://www.itl.waw.pl/czasopisma/JTIT/2003/4/37.pdf

EAL4 accredited solutions for military, defense and intelligence security. (n.d.) Clearswift. Retrieved on 28 January 2008 from: http://www.clearswift.com/products/specialist/default.aspx

Executive Order. (n.d.) Further Amendment to Executive Order 12958, As Amended, Classified National Security Information. Retrieved on 9 January 2008 from: http://www.whitehouse.gov/news/releases/2003/03/20030325-11.html

Global Connections - Coalition Partner Sites. (n.d.) Retrieved on 18 December 2007 from: https://www.cwid.js.mil/public/CW06coalition10May.pdf

Information Exchange Gateway (IEG). (n.d.) Retrieved on 15 November 2007 from: http://194.7.80.153/website/book.asp?menuid=15&vs=0&page=volume2%2Fch02s07.html

Integrated Information Assurance - XTS 300 Solution Suite. (n.d.) BAE Systems. Retrieved on 28 January 2008 from: http://www.digitalnet.com/solutions/information_assurance/xts300sol_ste.htm

Kriendler, J., (June 2005) *NATO Headquarters Transformation: Getting Ahead of the Power Curve.* Defence Academy of the United Kingdom. Conflict Studies Research Centre. 7-9, Retrieved on 28 January 2008 from: www.da.mod.uk/colleges/csrc/document-listings/special/05(29)-JK.pdf

Larsen, P.G., *Coalition Command and Control (C2) Interoperability Challenges*. (2007) Retrieved on 15 November 2007 from: http://www.dodccrp.org/events/11th_ICCRTS/html/papers/124.pdf

Levin, T., Irvine, C., Weissman, C., Nguyen, T., (November 2007) *Analysis of three multilevel security architectures.* Proceedings of the 2007 ACM workshop on Computer security architecture, ACM, 37, Retrieved on 23 January 2008 from: http://delivery.acm.org.dml.regis.edu/10.1145/1320000/1314473/p37-levin.pdf?key1=1314473&key2=3153311021&coll=ACM&dl=ACM&CFID=51285889&CFTOKEN=77909174

Loscocco, P., Smalley, S., Muckelbauer, P., Taylor, R., Turner, J., Farrel, J., (1998) *The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing*

Environments. National Security Agency, 1, Retrieved on 21 January 2008 from: http://csrc.nist.gov/nissc/1998/proceedings/paperF1.pdf

Lourens, H., (12 July 2007) *Information Briefing on the NLD IGB To The Working Group of National Technical Experts COM and ADP.* Netherlands Defence Materiel Organisation. Retrieved on 13 January 2008 from: http://www.vovklict.nl/site_documentation/diversen/IGB.pdf

MacMillan, K., Shimko, S., Sellers, C., Mayer, F., Wilson, A., (2 March 2006). *Lessons Learned Developing Cross-Domain Solutions on SELinux*. Retrieved on 17 January 2008 from: www.tresys.com/files/docs/CDS-SELinux-Symp.pdf

McNamee, D., Heller, S., Huff, D., (May 2006) *Building Multilevel Secure Web Services-Based Components for the Global Information Grid.* CrossTalk – The Journal of Defense Software Engineering. Retrieved on 15 November 2007 from: http://www.stsc.hill.af.mil/crossTalk/2006/05/0605McNameeHellerHuff.html

Mineweaser, J., (13 July 2006) *Internet Engineering Task Force (IETF) 66 Meeting Minutes.* Montreal. Retrieved on 18 February 2008 from: http://www.ietf.org/proceedings/06jul/minutes/SAMRG.txt

Multi-Domain Security and its Impact on Network Centric Operations. (n.d.), 4, Retrieved on 23 January 2008 from: http://www.c-d-r.net/MDS.doc

NATO Awards Nexor Contract for Provision of High Assurance Mailguards. (n.d.) Retrieved on 24 January 2008 from: http://www.nexor.com/content/view/424/246

NATO New Headquarters. (n.d.) Retrieved on 26 January 2008 from: http://www.nato.int/structur/tenders/newhq3/index.htm

North Atlantic Treaty Organization - Homepage. (n.d.) Retrieved on 3 February 2008 from: http://www.nato.int/

North Atlantic Treaty Organization. (2006). *NATO Security Policy and Supporting Directives.* NATO Headquarters, Brussels, Belgium (this policy is not releasable to the public)

NATO C3 Technical Architecture. Volume 2. Supplement 1: Domain Architectures. Version 7.0. (15 December 2005), 7-8, Retrieved on 16 January 2008 from: http://194.7.80.153/website/book.asp?menuid=15&vs=0&page=vol2%2Dsup1%2Fch01%2Ehtml

O'Sullivan, R., (May 2005) *Networking Coalitions.* Australian Government Department of Defence. Retrieved on 28 January 2008 from: http://www.defence.gov.au/defencemagazine/editions/20050501/groups/cio.htm

Parker, R., (14 March 2005) *A NATO Perspective on CENRIX*. 8, Retrieved on 16 November 2007 from: http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/007.pdf

Phillips, C., Ting, T., Demurjian, S., (June 2002) *Information sharing and security in dynamic coalitions.* **SACMAT '02:** Proceedings of the seventh ACM symposium on Access control models and technologies. Retrieved on 21 January 2008 from: http://portal.acm.org.dml.regis.edu/citation.cfm?id=507726&coll=ACM&dl=ACM&CFID=50950228&CFTOKEN=74772502

Prague Summit Declaration. 21-22 November 2002. NATO Press Release. Retrieved on 26 January 2008 from: http://www.nato.int/docu/pr/2002/p02-127e.htm

Press Release – Accreditation of Email Transfer and Data Forwarding Applications Results in Complete Turn-Key Cross Domain Solution. (n.d.) Retrieved on 17 January 2008 from: www.tenixamerica.com/07_Accreditation_2.html

Reed, N., (2004) *Security Guards for the Future Web Final Project Report.* Mitre Center for Integrated Intelligence System. 1-18, Colorado Springs, Colorado.

RFC 2828 - *Internet Security Glossary.* (n.d.) Retrieved on 15 January 2008 from: http://www.faqs.org/rfcs/rfc2828.html

Roberston, G. (2004) *Transforming NATO to Meet the Challenges of the 21st Century.* Transatlantic Transformation: Equipping NATO for the 21st Century, Washington, DC, Center for Transatlantic Relations, 30.

SecureOffice Trusted Gateway on Linux. (n.d.) Retrieved on 28 January 2008 from: http://www.tcs-sec.com/products/TrustedGatewayLinux.html

Shehab, M., Bertino, E., Ghafoor, A., (November 2005) *Secure collaboration in mediator-free environment.* CCS '05**:** Proceedings of the 12th ACM conference on Computer and communications security. ACM. Retrieved on 22 January 2008 from: http://delivery.acm.org.dml.regis.edu/10.1145/1110000/1102130/p58-shehab.pdf?key1=1102130&key2=2786401021&coll=ACM&dl=ACM&CFID=51097838&CFTOKEN=98148372

Silberglitt, R., AntÃ³n, P., Howell, D., Wong, A. (2006) *The Global Technology Revolution 2020, In-Depth Analyses*. Copyright © 2006 RAND Corporation.

Swamy, N., Hicks, M., Tsang, S., (October 2007) *Verified Enforcement of Security Policies for Cross-Domain Information Flows*. Proceedings of the 2007 Military Communications Conference (MILCOM), Retrieved on 21 January 2008 from: http://www.cs.umd.edu/~nswamy/papers/cpa-milcom07.pdf

Tenix Data Diode – Absolute Information Protection. (n.d.) Retrieved on 10 February 2008 from: http://www.tenixamerica.com/products.html

The Consultation Process - Reaching Consensus. (n.d.) Retrieved on 26 January 2008 from: http://www.nato.int/issues/consultation/index.html

Thuppal, R., (12 December 2007) *Comd-Net, SIGNET-C and ADM(POL) Information Exchange Gateway*. vs0.72. DIMEI-8. Canadian Department of National Defence.

Thuppal, R., (31 October 2007) *Interactive Link - System Design Specification*. vs0.13. DIMEI-8. Canadian Department of National Defence.

Trusted Solaris 8 Operating Environment. (n.d.) Retrieved on 24 January 2008 from: http://www.sun.com/software/solaris/trustedsolaris/features.xml

Warner, J., Atluri, V., Mukkamala, R., Vaidya, J., (June 2007) *Using semantics for automatic enforcement of access control policies among dynamic coalitions*. SACMAT '07**:** Proceedings of the 12th ACM symposium on Access control models and technologies. ACM. Retrieved on 22 January 2008 from: http://delivery.acm.org.dml.regis.edu/10.1145/1270000/1266877/p235-

warner.pdf?key1=1266877&key2=3056401021&coll=ACM&dl=ACM&CFID=51097838&CFTOKEN=98148372

Weaver, R., (2007). *Guide to Network Defense and Countermeasures.* Second Edition. 205, Thomson Course Technology.

Whitman, M.E and Mattord, H.J., (2005). *Principals of Information Security*. Second Edition, 68-385, Thomson Course Technology.

XTS-400 - BAE Systems. (n.d.) Retrieved on 21 January 2008 from: http://en.wikipedia.org/wiki/XTS-400

Glossary of Terms and Acronyms

A	Ampere
ACL	Access Control List
AES	Advanced Encryption Standard
AUS	Australia
BICES	Battlefield Information Collection and Exploitation System
BPD	Boundary Protection Device
BPS	Boundary Protection Service
CD	Compact Disc
CDS	Cross Domain Solution
CENTRIXS	Combined Enterprise Regional Information Exchange System
CIO	Chief Information Officer
COSMOS	Coalition Secure Management and Operations System
COTS	Commercial-Off-the-Shelf
C2	Command and Control
CWID	Coalition Warrior Interoperability Demonstration
DAC	Discretionary Access Control
DCID	Director of Central Intelligence Directives
DFAIT	Department of Foreign Affairs, Industry and Trade
DII	Defense Information Infrastructure
DISA	Defense Information System Agency
DMS	Document Management System
DMZ	Demilitarized Zone
DND	Department of National Defence (Canada)
DNS	Domain Name Service
DoD	Department of Defense (USA)
DSA	Directory Service Agent
DVD	Digital Video Disc
EAL	Evaluation Assurance Level
ETA	Email Transfer Application
FBI	Federal Bureau of Investigation
FTP	File Transport Protocol
GBR	Great Britain
GIG	Global Information Grid
GOTS	Government Off-the-Shelf
HQ	Headquarters
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol Over Secure Socket Layer
IDS	Intrusion Detection System
IEG	Information Exchange Gateway
IFOR	Implementation Force

IGB	Interface Gateway Box
IL-DD	Interactive Link Data Diode
IOP	Interoperability Point
IP	Internet Protocol
IPv6	Internet Protocol Version 6
ISO	International Standards Organisation
ISP	Internet Service Provider
IT	Information Technology
JCOP	Joint Common Operational Picture
.jpg	A file compression format (Joint Photographic Compression)
K	Thousand (metric)
KW	kilowatt
LAN	Local Area Network
MAC	Mandatory Access Control
MB	megabyte
MC	Military Committee
MFA	Ministry of Foreign Affairs
MILS	Multiple Independent Levels of Security
MINERVA	not an acronym, but a LAN used at NATO HQ
MLS	Multi-level Security
MMHS	Military Messaging Handling Server
MoD	Ministry of Defence (UK or generic)
MDS	Multi-Domain Security
NAC	North Atlantic Council
NATO	North Atlantic Treaty Organization
NC	NATO Confidential
NCW	Network Centric Warfare
NC3A	NATO Consultation, Command and Control (C3) Agency
NEC	Network Enabled Capability
NEW	Network Enabled Warfare
NGO	Non-Governmental Organizations
NR	NATO Restricted
NS	NATO Secret
NSA	National Security Agency
NLZ	New Zealand
PC	Personal Computer
PKI	Public Key Infrastructure
RBAC	Role-based Access Control
SAGE	Standard Automated Guard Environment
SIPRNet	Secret IP Router Network
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol

SQL	Formerly known as Structured English Query Language (SEQUEL)
SSL/TLS	Secure Sockets Layer / Transport Security Layer
STOP	Secure Trusted Operating System
TGS	Trusted Gateway System
TS	Top Secret
TSE	Trusted Services Engine
UK	United Kingdom
USA	United States of America
USB	Universal Serial Bus
USSR	Union of Soviet Socialists Republic
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Networks
VTC	Video Teleconference
WAN	Wide Area Network