11TH ICCRTS
COALITION COMMAND AND CONTROL IN THE NETWORKED ERA

Coalition Interoperability: a Modeled Approach

C2 Experimentation, Coalition Interoperability

Gerard J. Christman (POC)
Assistant Secretary of Defense for Networks and Information Integration,
Directorate for Contingency Support and Migration Planning
6000 Defense Pentagon, Washington D.C. 20301-6000
gerard.christman.ctr@osd.mil
(703) 697-8195

Mark Postal
NATO Consultation, Command and Control Agency (NC3A)
Oude Waalsdorperweg 61,
2597 AK The Hague
(PO BOX 174 2501 CD)
Netherlands
+31 70 374 3528
mark.postal@nc3a.nato.int

Acknowledgements

The authors would like to acknowledge the Combat and Materiel Developers in the US and NATO chains of command. Special thanks to Paul Ulrich, PM Battle Command, for his advice and counsel on planning events and demonstrations. Dick Lee, Assistant Deputy Under Secretary of Defense, for his advocacy of the C2IEDM model as a means to achieve coalition interoperability. Colonel Stuart Whitehead, Lieutenant Colonel Andre Cota-Robles, and Dave Vincent of the US Army Training and Doctrine Command Program Integration Office for Battle Command for representing the needs of the warfighter and the outreach to the US Army. John Maguire and the SADI team for providing superb support to our effort to evangelize the widespread interoperability with this technology. Thanks to Lieutenant Colonel Guy "Pudge" Townend, Canadian Army, for his direct manner and true professionalism. He always ensured that Allied Command Transformation's role was well represented in this effort. To the NC3A LC2IS Tiger Team, for their efforts to quickly improve the system and undergo spiral development process is a testament to your proficiency and professionalism.

ABSTRACT

In 2004, US Department of Defense officials visited Afghanistan and assessed that the degree of information sharing, particularly in the Command and Control(C2) domain, between the Combined Joint Task Force – 76 and the International Security Assistant Force (ISAF) was less than adequate to meet the minimum military requirement for an expanding ISAF. Upon return, they took the lead to create a proposal that involved the partnership of NATO's Allied Command for Transformation (ACT). The proposal introduces the use of a NATO C2 system based upon the Command and Control Information Exchange Data Model (C2IEDM) to provide a new capability and to create the conditions where national implementations of C2IEDM-compliant systems could be brought to the operation by ISAF nations.

This paper will introduce the Multilateral Interoperability Programme (MIP) and the C2IEDM that results from it. It will discuss the rationale behind the model and its inherent strengths. The paper will also discuss the spiral development process that was undertaken to prepare NATO's Land Command and Control Information Services (LC2IS) for introduction into theater in conjunction with the US Maneuver Control System version 6.4 (MCS v6.4) and the Situational Awareness Data Interchange (SADI)/Global Command and Control System (GCCS).

1. Introduction

The International Security Assistance Force (ISAF) is a NATO-led, UN-mandated operation that consists of troops from 36 nations (ISAF, 2006). ISAF has operations in 14 of 34 afghan provinces. In December 2005, NATO agreed to expand ISAF to 15,000 troops and to operate in 20 provinces (What, 2005).

Combined Joint Task Force-76 (CJTF-76) is a subordinate headquarters of the Combined Forces Command – Afghanistan which is subordinate to US Central Command (USCENTCOM). Operation Enduring Freedom (OEF) is led by USCENTCOM. There are 80 nations that are participating in the coalition that supports this operation (Lawrence, 2005).

In an effort to facilitate communications within the two military operations, ISAF and OEF, NATO and USCENTCOM had to create mission-specific network infrastructures. Specifically, ISAF created a mission Secret network and USCENTCOM created the Combined Enterprise Regional Information Exchange System (CENTRIXS). These networks are not interconnected and data is not exchanged between the two domains.

With two major military organizations conducting operations in Afghanistan, clearly there is a need to keep each other appraised of each others' intentions. However, after visiting the theatre of operations in the fall of 2004, senior DoD officials recognized that

this was not the case and undertook action to analyze the problem and develop proposals to enable information exchange.

Representatives from the Office of the Assistant Secretary of Defense for Networks and Information Integration / Chief Information Officer (OASD NII/CIO) met with representatives of Allied Command Transformation (ACT), Assistant Chief of Staff for Command Control Communications Computers and Intelligence (ACOS C4I) and determined that the solution would be based upon the Command and Control Information Exchange Data Model (C2IEDM). The C2IEDM approach was deemed especially suitable for this application since 25 nations and two major NATO headquarters have accepted the model. Furthermore, NATO is in the process of adopting the model as STANAG 5525. STANAG 5525 is an umbrella agreement with annexes that permit Data Model evolution as revealed by P. Ulrich (personal correspondence, April 28, 2006).

The proposal developed by OASD NII/CIO called for the use of CENTRIXS as the bearer network with a C2IEDM compliant system in the ISAF headquarters and another in CJTF-76. It called for demonstrations outside of Theatre to prove the concept and build confidence with an eventual deployment of the capabilities scheduled in the December 2005 timeframe.

> Our approach to interoperability needs to change as well. Given the rate of advancing technology, we need to move from an approach based upon application standards to one based upon data standards. We need to give users of information the opportunity to use the applications that make sense to them while maintaining the ability to exchange information. (Stenbit, 2005, p. xvi)

2. Background

The Multilateral Interoperability Programme (MIP) is neither a US nor a NATO program but one comprised of member nations that have acceded to the requirements of the baseline data model and information exchange mechanisms developed by working groups of the program and unanimously agreed by the national program managers. Ulrich also provides that while the program can trace its roots back to a series of bilateral initiatives starting as early as1979, the current program was created in April, 1998 with the merger of two existing programs addressing coalition interoperability Corps and below; Canada, France, Germany, Italy, the United Kingdom and the United States of America as the founding members. In October 2001, the Army Tactical Command and Control Information System (ATCCIS) program merged with MIP. ATCCIS was a Supreme Headquarters Allied Powers Europe (SHAPE) sponsored study to investigate achieving interoperability at reduced cost through adoption of common specifications and standards. The merger with ATCCIS resulted in the adoption of the C2IEDM as a foundation product for the MIP specification. Figure 1 illustrates the concept of the data model and information exchange mechanism as the core interface between national C2 systems (Background, 2006).

The authors were informed that in 2005 the MIP merged efforts with the NATO Data Administration Group and produced a Joint Consultation Command & Control Information Exchange Data Model (JC3IEDM) in correspondence with E. Chaum, a member of the XML Working Party of the MIP, regarding the developments with the

model (personal communication, April 27, 2006),. Work continues and the model is still evolving. It will begin its in-service period in 2008.

As of this writing, the program has produced the Command and Control Information Exchange Data Model (C2IEDM) baseline 6.1.5e and, again the JC3IEDM which will be in service in 2008. Now that there is agreement with the model baseline amongst the participating countries in the MIP, it is important to be cognizant of the advantages and disadvantages of using the C2IEDM.

Chaum (2006) states that the C2IEDM data model provides an evolved, shared, common set of semantics and concepts that reduces complexity. E. Chaum later clarified that by beginning with semantic alignment, the architecture and services are less complex and by doing so, one reduces costs of design, development, testing and integration costs (personal communication, April 28 , 2006).

Whitehead (2005) views the model as a mechanism to tear down the "Tower of Babel" that has been created as a result of the various data types and formats from the myriad Battle Command systems acquired over the years. The size and complexity of this informal ontological approach, as Lasschuyt (2003) laments, actually results in a model that is rich in its ability to convey a common understanding to commanders and staffs from 25 nations; clearly not an easy task (Dorion & Boury-Brissset, n.d.).

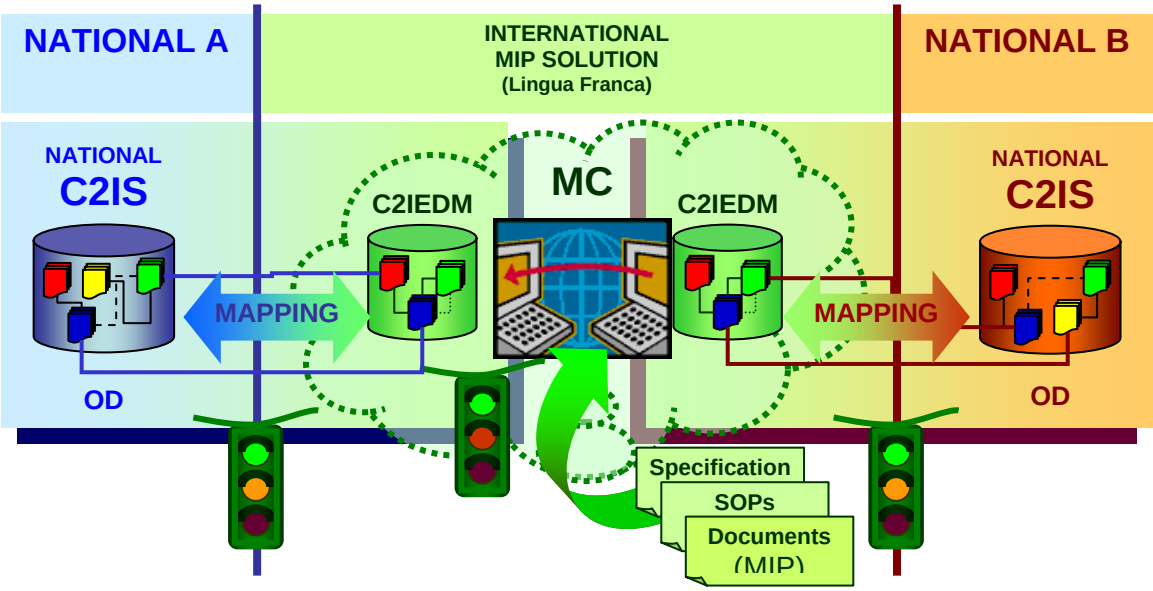

Figure 1 illustrates the operational concept of the information exchange mechanism and the data model between national C2 systems. Used by permission obtained April 24, 2006 via email (Background, n.d.)

Lasschuyt (2003) states that C2IEDM has become too large and complex a model but does not state what this is compared to. Furthermore, he states that the size and

complexity will grow even larger as the model migrates from a land-focused model to a joint one and appears to advocate other strategies.

The real issue is one of sufficiency. The model must be sufficient to meet the warfighters C2 requirements and the ability to form a common understanding of the situation. That is the determinant, not size or complexity.

As it stands today, virtually all MIP-member nations are implementing MIP Block 2 baseline specifications which include the C2IEDM version 6.1.5e. The national implementations have undergone a series of interoperability tests, both operational and systems level, in order to demonstrate that their national systems are ready to be fielded. Given this investment of national treasure and ongoing coalition operations, it is clear that we must set the conditions to leverage these long-envisioned systems to reduce the stovepipes and attain a common understanding of the operation based upon the C2IEDM.

3. Approach

> There is a need for an internationally agreed vision of coalition operations in the information age, shared at least by those countries that are able and willing to lead such operations. This needs to be underpinned by multinational experimentation; otherwise it remains an untested hypothesis. (Blad & Potts, 2004, p.147)

The agreed proposal published in March 2005 called for a spiral approach to develop and demonstrate the capabilities and interoperability of the NATO Land Command and Control Information Services (LC2IS) prototype and the US Maneuver Control System (MCS) version 6.4. Later, the Situational Awareness Data Interoperability (SADI) Data Exchange Server (SDES)/Global Command and Control System (GCCS) system was added to improve compliance with net-centric edicts within the US network domain (Data, 2004).

In order to keep costs down and to minimize the impact on developers, there was widespread agreement that existing planned events should be leveraged wherever possible. Figure 2 illustrates the spirals in the agreed spiral development process undertaken in March 2005 and scheduled to conclude in the November 2006 timeframe. Because much planning had already been undertaken, the US chose Combined Endeavor 2005 as its venue to perform Systems Level Tests and interoperability demonstrations with a number of C2IEDM-compliant systems. For similar reasons, NATO chose the NATO – Coalition Warrior Interoperability Demonstration as it's venue for the first spiral. There were a number of issues discovered during CWID with the prototype. The main issues of concern were the lack of robustness in the prototype implementation and its inability to efficiently manage multiple information sources. As these issues were seen to be more a factor of the timing of the CWID demonstration with respect to the prototype development cycle, they were not determined to be insurmountable.

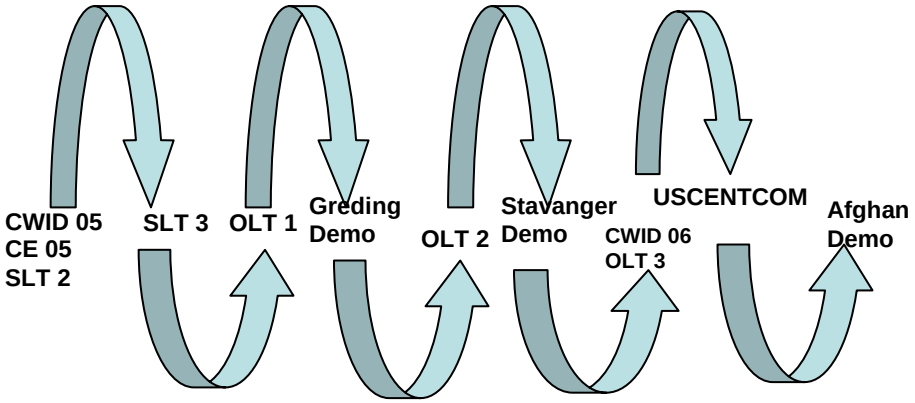

Figure 2. US – NATO Spiral Development Process to deliver an interoperable C2 capability to Afghanistan based upon C2IEDM. The spiral began with the Coalition Warrior Interoperability Demonstration and Combined Endeavor on the left and will culminate in a demonstration of capabilities on Afghanistan.

The group of interested stakeholders is very broad. However, the effort would not have been successful had the core group of stakeholders not coalesced into a cohesive, responsive team consisting of: OASD(NII)/CIO-sponsor; Program Manager Battle Command –US Materiel Developer; TRADOC Program Integration Office for Battle Command- US Combat Developer; ACT – Co-sponsor; NATO Consultation Command and Control Agency (NC3A) – NATO Materiel Developer.

The Systems

Land Command & Control Information Services (LC2IS) Prototype Effective Command & Control (C2) of multinational land forces operations requires fully interoperable C2 tools deployed with all participating national units as well as the NATO command authorities. NATO nations have established the Multilateral Interoperability Programme (MIP) to evolve and manage the information exchange standards and technologies. LC2IS is based on the MIP data model and information exchange techniques (message and data). The prototype has been internally developed by the NC3A.

Maneuver Control System (MCS) V 6.4 is an automated system to develop and share the common tactical picture of the battlespace. It provides corps through battalion level commanders and staff with the ability to swiftly collect, coordinate and act on near real time battlefield information and to graphically visualize the digitized battlefield. Capabilities provided are the Commander's Operational Picture, staff planning, OPLAN/OPORD, Resource Management and Collaborative Planning. Current Battlespace Situational Awareness information is available to all the battlefield functional area systems that comprise the Army Battle Command System (ABCS) system of systems (US, 2005).

P. Ulrich provides that MCS software development is synchronized with the Army Battle Command System and software integration efforts at the Central Technical Support

Facility (CTSF) in Ft. Hood, TX; MCS is being fielded on common hardware with current software version MCS/ABCS 6.4. MIP interface capability has been developed for the current MCS version, i.e., coalition interoperability using the MIP data model (C2IEDM) and agreed information exchange mechanisms (personal communication, April 29, 2006).

Situational Awareness Data Interoperability (SADI) Data Exchange Server (SDES) is a project to define and initiate convergence on a common data exchange approach for situational awareness systems. The project was originally intended to support the objectives of Joint Vision 2020 (JV 2020) and the Global Information Grid (GIG) by facilitating the flow of situational awareness information across the seams between both U.S. and coalition forces. Any system would then have to translate to a single interface standard in order to make its information available to other systems (Chaum, n.d.). The generic concept is illustrated in the figure 3 below.

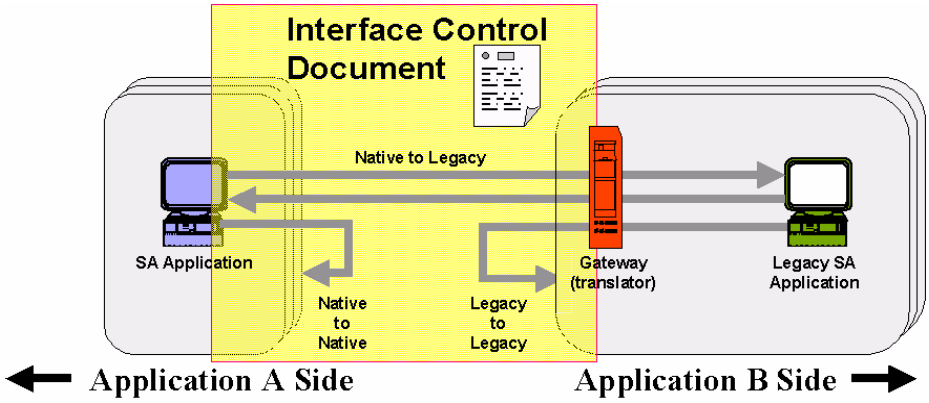

Figure 3 the generic operational concept of the Situational Awareness Data Interoperability project. Used by permission obtained from its author April 26, 2006 via email.

Ulrich also provided that this is a generic description of the original SADI FIOP program which devolved into specific implementation using the MIP interface specifications for coalition interoperability while providing a Net Centric enabled "back-end" to US systems using web services,NCES & the Global Command and Control System – Maritime (GCCS-M) as the end system representing the GCCS Family of Systems (personal communication, April 29, 2006).

NC3A focused its efforts at getting the system ready for testing at the interoperability test facility at Greding, Germany. NC3A formed a Tiger Team and worked to ensure that a core set of capabilities would be ready for testing in the fall of 2005. These core capabilities focus on the management, visualization and sharing of the recognized ground picture. Specifically, efforts were focused on improvements in the user interface to create and manage all the battle-space objects supported by the C2IEDM. The ability to

manage object holdings, associations and affiliations were also enhanced. These capabilities combined with Operational Information Groups (OIGs) (overlays) allowed for the development of complex views of the battle-space.

The LC2IS underwent Systems Level Test 3 and Operational Tests 1 and 2 over the period September 2005 to February 2006 and passed its operational assessments associated with these tests. Similarly, the MCS and SADI/GCCS systems underwent these tests as well and also passed their respective Operational Assessments.

In addition to spirals in the development and testing effort, the three systems underwent two demonstrations for key leaders in NATO and US chains of command that would ultimately decide if the systems were to be permitted into Afghanistan for a field demonstration. Joint Force Command Brunssum (JFCBS) J6 requested a demonstration in Europe so key leaders from JFCBS, the Allied Rapid Reaction Corps (ARRC), USEUCOM, USCENTCOM, USPACOM, the 10th Infantry Division (US), US Army CIO/G6, and the Office of the Secretary of Defense (OSD) could see the readiness of the systems first hand. It was to be the last hurdle before delivering the capability to Afghanistan according to the plan.

The demonstration was conducted at the Wehrtechnischen Dienststelle für Informationstechnologie und Elektronik (WTD 81), Greding, Germany test facility that is home to the Multilateral Interoperability Programme. The demonstration consisted of vignettes developed by the MCS Combat Developer from Fort Leavenworth Kansas. The vignettes benefited greatly from the Combat Developer's real-world experience in Afghanistan. This added realism to the C2 information that was exchanged for demonstration purposes. It lent credibility to this endeavor from an operator's perspective. The vignettes were: ISAF Combat Patrol; CJTF Combat Patrol; Convoy Operations; Downed Aircraft; CJTF Executes Raid; and ISAF Executes Raid. Despite a flawless demonstration and acknowledgments that the systems performed perfectly, JFCBS stated their reservations about conducting demonstrations in an operational theater. Members of the Allied Rapid Reaction Corps (ARRC) staff at the demonstration offered the ISAF IX Mission Rehearsal Training in Stavanger, Norway as a venue to conduct additional demonstrations and to further socialize the LC2IS system with an operational NATO command. In parallel with the Greding event, the NATO Consultation Command and Control (NC3) Board reaffirmed their support for delivering a capability for demonstration in Afghanistan. In addition, the ARRC and NATO Allied Command Transformation (ACT) came to agreement that demonstrations of new technologies would be permitted in Theatre during ISAF IX.

Following the Greding demo, systems returned to Greding in February 2006 for additional Operational Level Testing. These tests are designed to verify that information exchange and reporting can be accomplished between and across multiple levels of command. As such, the tests have more of an operational than technical flavor. Though the systems had participated in earlier Operational Level Testing, adjustments had been made to the underlying data model and business rules that required re-verification of the implementations. Furthermore, the ORBAT is changed for each OLT and thus brings the

opportunity to perform these more extensive tests with different national implementations. All systems passed their Operational Assessments.

The same three systems then went to Camp Ulsnes, NATO Joint Warfare Center, Stavanger, Norway to participate in the ARRC's train-up for ISAF IX and to continue to socialize the concept for an Afghan demonstration of these new capabilities over and above those the ARRC was deploying with. Demonstrations and briefings were conducted for five Flag Officers who were either assigned to the Joint Warfare Center or the ARRC. In addition, roughly 30 field grade officers, four NATO / Defense Staff Civilians, and six Non-Commissioned Officers were given the demonstration using the same vignettes developed for the demonstration in Greding and were permitted as much time to ask questions about architecture, functionality, and capabilities as they wished. The Demonstration team was given special recognition and thanks from the Commanding Officer of the Joint Warfare Center as a result. The systems view architecture for both demonstrations is illustrated in Figure 4.

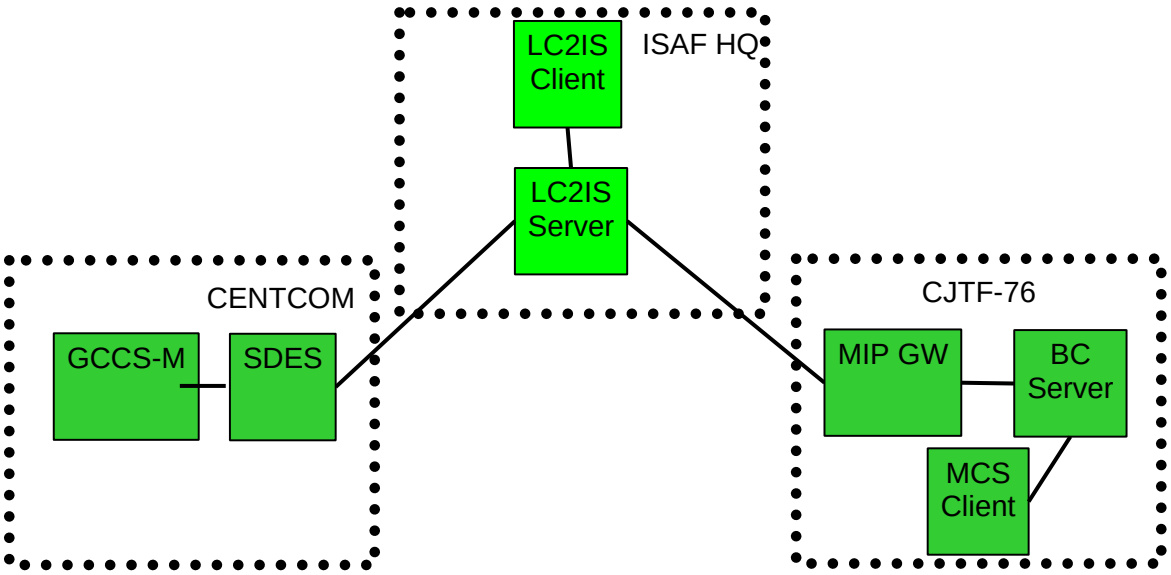

Figure 4. Demonstration Architecture for Greding, Germany and Stavanger, Norway. The dotted boxes are meant to illustrate the various headquarters simulated in the demonstrations.

The so called Stavanger Demo resulted in a commitment from the ARRC to permit a demonstration of the capability in Afghanistan in the November timeframe, and perhaps sooner depending entirely on the operational conditions. This was the desired outcome albeit a bit further to the right on the timeline than we had hoped.

The stakeholders met in Washington and determined that the group should not be idle while waiting for the ARRC to grant permission to conduct the demonstration. It was agreed that the systems could be configured and made operational on the ISAF mission secret network point of presence at USCENTCOM in order to provide a proof of concept in a low threat environment. The results from this effort will also be used to update the ARRC regarding preparedness for the Afghan Demo. Figure 5 provides a narrowly focused illustration of the architecture of the systems to be demonstrated in Afghanistan.

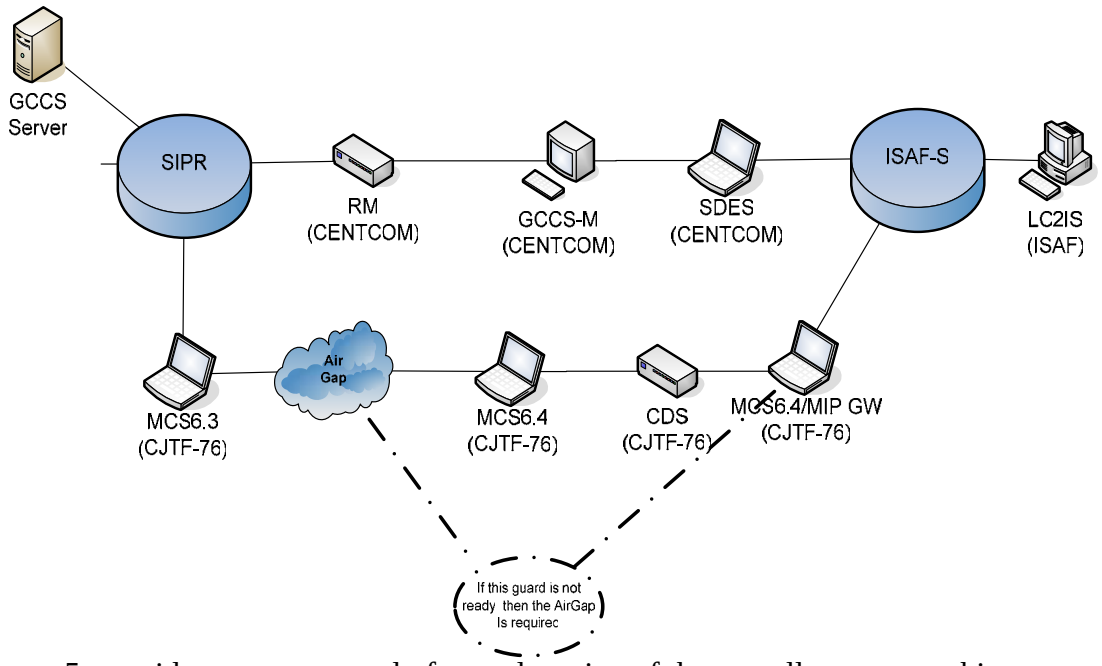

Figure 5. provides a very narrowly focused portion of the overall systems architecture. The intent is to provide the reader with the object relative to this effort. RM is a Guarding solution implemented by USCENTCOM. SDES is the SADI Data Exchange Server.

4. Political Dimension

On the NATO side, definition and implementation of new capabilities is a lengthy process. Allied Command Transformation (ACT) generally conceives of new capability and manages its acquisition while coordinating closely with Allied Command Operations (ACO). The mechanism by which the capability is funded is the NATO Security Investment Program (NSIP). The LC2IS prototype was created to facilitate the collection of user and system requirements for a future Land C2 capability to be funded by NSIP. The Land C2 NSIP project was authorized in 2005 and is currently moving forward toward acquisition and delivery in 2008.

This notion of integrating experimentation into mainstream processes that establish priorities, allocate resources, and shape programs is in keeping with the findings by Alberts (2002). He indicates experimentation will result in requirements that are realistic

and in line with actual needs of the warfighter. “We can expect to see fewer and fewer requirements documents that are not a direct output of experimentation” (Alberts, 2002, p. 105)

Utilization of LC2IS as an operational prototype in ISAF has stirred many emotions and debates within the NATO community. On one hand, the prototype would provide a significant improvement above the currently utilized capability. On the other hand, the LC2IS prototype is seen as operationally un-proven and without full lifecycle support. The later being the byproduct of the two year gap between the definition of the solution in 2006 and the delivery of the solution by industry in 2008. The industrialized solution will have full lifecycle support, but the prototype will not.

The discussion above is important when measuring NATO’s reaction to the proposed delivery of LC2IS prototype as a capability in ISAF. As with all major military programs, the probability of developing and delivering the industrialized version on time and without incident is small. To fill the void, Command and Control Personal Computer (C2PC) has been selected and funded by the Infrastructure Committee. Although filling the capability gap mitigates risk in one area, it can be viewed as causing risk in another. Placing emphasis and funding elsewhere to fill the gap, has the effect of relieving pressure and dampening momentum on fielding the objective system. The LC2IS should not be viewed in isolation. A critical factor in the decision-making process should be the availability of other national implementations for use in an operational environment. Nations have invested their national treasure in the development of their respective C2IEDM- compliant systems and that capital investment should be leveraged. In addition, as NATO is in a leadership role, it must be in the lead with regard to their C2 system. Without leading, an unenviable position results where the command structure has a lesser capability than the nations represented in the operation. Furthermore, without leading, the command structure would lack the capacity to leverage existing, fully developed, national capabilities.

5. Cross-Domain Solutions (CDS)

C2IEDM-based solutions are proposed as a means to improve interoperability in a coalition environment. The MIP Data Exchange Mechanism (MIP-DEM) and C2IEDM provide the means to unambiguously encode and exchange information between two commands. But this does not ensure interoperability. In reality the information providers and consumers reside in different network security domains. The rules and mechanisms for passing information between these domains vary as they are the responsibility of national, coalition and Alliance security personnel. This is an old story that currently does not have a happy ending. Ulrich indicated that a conservative estimate is that the US is years away from realizing an accredited cross-domain solution for use on the national side of the MIP coalition interface (personal communication, April 29, 2006). The development time for a CDS is primarily driven by the requirement for the cross-domain solution to be accredited and implemented in all national, coalition and Alliance security domains; this process alone can easily take 18 – 24 months to complete. In addition, it is also necessary to specify for each domain the information releasability

criteria/policy upon which the CDS will be built. This does not mean that MIP information cannot currently be passed across security domains. It means that cross-domain information exchange is difficult, time consuming as it most like involves physical separation and a man in the loop and more likely to fail than succeed. There is much need for improvement in this area. The US is developing a CDS for implementation with MCS/MIP and is just now entering the validation/accreditation cycle for certification by US officials.

6. Commercialization of MIP products

As C2IEDM is in its ascendancy; private industry is taking notice and is becoming increasingly involved in learning about the MIP, the working groups, and the baseline model. The MIP community creates specifications (MIP-DEM and C2IEDM), not standards. These specifications are reasonably managed and stable. As such, the specifications can, and are, used by commercial companies to provide components useful towards the implementation of MIP compatible systems. These components might include MIP Data Exchange Mechanisms, data access layers, business logic (the middle tier), formatted message parsers and generators, situational awareness visualization components and specialized applications (CIMIC, Logistics, etc.).

If the MIP specifications are viewed as the interface specification for these components, given industry participation, it should be possible to quickly assemble or extend a MIP based system with off the shelf components. Systematic Software Engineering A/S is one such firm that has become a prominent presence in the C2 interoperability marketplace. Their products, SITAWARE and IRIS Replication Manager have been featured in CWID exercises and form the basis of several national implementations. Systematic Software Engineering A/S is directly involved in a number of technical forums responsible for developing the standards that form the baseline C2IEDM 6.1.5e.

7. Summary

In summary, this paper has briefly introduced the MIP and its resulting model, C2IEDM. It has addressed the strengths of using the model as a basis for a command and control system as an alternative to applications standards of the past. The reader has been shown an adaptation of the spiral development method for delivering an operational prototype ahead of schedule and within budget. The notion of incorporating experimentation into the development timeline to inform design and requirements as described by Alberts & Hayes (2005) was also highlighted.

OASD(NII) and ACT were successful in many major areas while working in partnership for this effort.. Firstly in challenging NATO to examine its business processes that are supposed to be responsive to the needs of the warfighter and that are to result in a fielded capability. Secondly, the partners achieved success in developing a capability, albeit in operational prototype form, ahead of schedule, and within budget, that will be leveraged by the NSIP process to provide a fully sustained system. Thirdly, success was found in

increasing awareness of the power of widespread interoperability by leveraging MIP-member nation investments in national implementations of C2IEDM. Fourthly, success was realized by recognizing the strength of leveraging existing exercises, test events, and power to the edge experimentation to be activities for change (Alberts & Hayes, 2005).. Fifth, that SADI/SDES is an effective (albeit limited) exchange / semantic mediation service to connect legacy systems to those based upon C2IEDM as highlighted by E. Chaum (personal communication, April 28, 2006). Lastly, the effort was successful in reaffirming the beneficial aspects of creating a NATO headquarters whose sole focus is transformation and experimentation. This effort required dedicated manpower that would not have been possible without ACT's existence.

8. Future Research

The incorporation of the LC2IS prototype into the ARRC's Mission Rehearsal Training and the subsequent agreement by the ARRC to conduct a demonstration in Afghanistan establishes a model upon which to plan the training of the follow-on force to the ARRC. This would be entirely dependent upon a decision to retain the demonstrated capability in Theater for further experimentation and research. Given a decision to retain the LC2IS prototype, it will be of great interest to see how the C2 systems will be trained at Stavanger or the next appropriate training venue for future ISAF rotations. What are the scenarios that will be trained? To what level will the force structure be represented in the Common Operating Picture (COP)? How will a NATO-derived force tracker be integrated into this COP? Similarly, what is the nature of the relationship between the NATO force tracker and LC2IS? Lastly, it might be useful to examine the techniques that under gird C2IEDM-based systems to determine if they are generalizable to information exchange from one federal Government agency to another or from the Federal Government to consumers on the Internet.

There is an Advanced Concepts Technology Demonstration (ACTD) called Coalition Secure Management and Operations System (COSMOS) (COSMOS, 2006). An objective of this ACTD is to use C2IEDM technology to provide an Application-independent (indigenous) coalition C2 system ("Come as you are"). This effort is co-sponsored by US European Command (USEUCOM) and US Pacific Command (USPACOM). Part of their focus is on coalition operations with Pacific rim nations. It would be interesting to examine if MIP could scale to incorporate more nations and their requirements or if there is a need to develop another group. Location, commuting times, languages, testing venues, exercise participation etc. would have to be examined in detail to determine the advantages and disadvantages, and risks associated with these issues.

In a similar vein, there is an entity called ABCA which consists of US, UK, Canadian, and Australian Armies with New Zealand as an observer (History, n.d.). One of the goals of this body is to achieve interoperability between the forces. Exercise Rainbow Serpent 2006 (EX RS06) is the AS hosted iteration of the biennial ABCA exercises and will be conducted within the Puckapunyal Military Area (PMA) from 01 September – 13 October 2006. The exercise will be conducted under the auspices of the American,

British, Canadian, Australian and New Zealand (ABCA) Armies Program and will involve brigade headquarter and exercise control forces from the United States, the United Kingdom, Canada and Australia in a major multinational Command Post Exercise (CPX). Approximately 1000 participants will be involved including a small contingent of observers from New Zealand. The AS Land Warfare Development Centre (LWDC) has responsibility for the planning and execution support of the exercise as directed by the Deputy Chief of the Army. MIP will play a key role in the exercise with the CAN and USA units exchanging information via the MIP interface as well as potential exchange with the AS MIP prototype; GBR will not have a MIP capability at the exercise

References

Advanced Concepts and Technology Division GE31. (2006, March 22). Retrieved April 28, 2006, from Department of Defense Information Systems Agency Web site: http://www.les.disa.mil/c/extranet/home?e_l_id=32

Alberts, D. S. (2002). Measuring Transformation Progress and Value. In *Information Age Transformation: Getting to a 21st Century Military* (1st Rev. ed., pp. 79-109). Washington DC: Department of Defense Command and Control Research Program . (Original work published 1996)

Alberts, D. S., & Hayes, R. E. (Eds.). (2005). *Power to the Edge: Command Control in the Information Age*. Washington DC: Department of Defense Command and Control Research Program. (Original work published 2003)

Background. (n.d.). *Multilateral Interoperability Programme*. Retrieved April 23, 2006, from http://www.mip-site.org/MIP_Background.htm

Chaum, E. (2006, March). *Multilateral Interoperability Programme (MIP) Community of Interest*. Briefing presented at United States Joint Forces Command, Combatant Command Data Strategy Implementation Workshop, Norfolk, VA.

Chaum, E. (n.d.). A Needed Transformation - and a Role for XML. *World Wide Consortium for the Grid*, Retrieved April 8, 2006, from http://w2cog.org.

Data Sharing in a Net-Centric Department of Defense (Rep. No. DODD 8320.20). (2004, December 2). Washington DC: U.S. Department of Defense. Retrieved April 26, 2006, from DOD Issuances & OSD Administrative Instructions database: http://www.dtic.mil/whs/directives/corres/dir2.html

Dorion, E., & Boury-Brisset, A.-C. (2004, June). *Information Engineering in Support of Multilateral Joint Operational Interoperability*. Paper presented at "Command and Control Research and Technology Symposium: The Power of Information Age Concepts and Technologies, San Diego, CA.

History. (n.d.). ABCA Public Website. Retrieved April 28, 2006, from http://www.abca-armies.org/Default.asp

Lasschuyt, E. (2003, October). *Information Interoperability Domains*. Paper presented at NATO RTO SCI-137 Symposium on Architectures for Network-Centric Operations, Athens, Greece. Retrieved April 3, 2006, from NATO Research & Technology Organization Web site: http://www.rta.nato.int

Lawrence, S. (2005, October 18). *Meeting the challenges presented by our enemy warfighters, terrorists, and hackers.* . Panel Discussion presented at MILCOM 2005, Atlantic City, NJ.

North Atlantic Treaty Organization. (2005, December 8). NATO To Head South. Message posted to http://www.nato.int/docu/update/2005/12-december/e1208a.htm

Potts, D. (Ed.). (2004). Beyond Interoperability: Part 1. In *The Big Issue: Command and Control in the Information Age* (Vol. 45, pp. 139-150). Information Age Transformation Series. Washington DC: Department of Defense Command and Control Research Program. (Original work published 2003)

Stenbit, J. (2005). Foreword. In D. S. Alberts & H. E. Richard (Eds.), *Power to the Edge: Command and Control in the Information Age* (3rd ed., pp. xiii-xvii) [Foreword]. Washington, DC: Department of Defense Command and Control Research Program. (Original work published 2003)

What is ISAF? (2005). In *International Security Assistance Force Afghanistan* (p. 2) [Brochure]. Mons, Belgium: North Atlantic Treaty Organization. Retrieved April 13, 2006, from North Atlantic Treaty Organization Web site: http://www.afnorth.nato.int/ISAF/media/pdf/flyer_isaf.pdf

Whitehead, S. A. (2005, September/October). Battle Command: Toppling the Tower of Babel. *Military Review*, 22-25.