Overcoming Barriers to Information Superiority in Coalition Operations

Dave Biddinger
3325 Buffalo RD
New Windsor, MD 21776
Phone: 410-875-5762
Fax: 301-604-0500
E-mail: dbidd@aol.com

Abstract

The current coalition information systems infrastructure and culture present barriers to the coalition interoperability that is a prerequisite to Information Superiority. One of the first steps toward the realization of Information Superiority is the achievement of interoperability between coalition nation information systems.

A primary commander's challenge is to overcome individual and institutional resistance to change. This is often related to the " not invented here " syndrome that permeates much of the coalition culture. Without a sharing of best practices across the coalition, effort is wasted in duplication and inefficiency.

Based on personal experience and interviews of DoD personnel, the author has selected organizational, acquisition, management, and security barriers for analysis. The author will apply recent experience in both the Armed Forces Staff College *Purple Sunset* exercise series and *Joint Warrior Interoperability Demonstration* (JWID) activities in determining how research and development solutions such as the C4ISR Architecture Framework have addressed the problem.

Cooperation between coalition entities will not come about through radical reorganization nor from the indiscriminate application of technology. Instead, cooperation will come (and in fact, is coming) gradually as the coalition defines C4ISR architectures. The C4ISR framework is divided into operational, technical, and systems processes that will improve the ability meet the globally distributed information superiority needs of the warfighters within the increasingly important context of coalition operations.

1. The Problem

Despite the best efforts of many smart and hard working people, coalition interoperability is still considered broken. Technology is neither the entire problem nor the entire solution. The current coalition information systems infrastructure and coalition culture present barriers to the coalition interoperability that is a prerequisite to Information Superiority. As specified in the Joint Chiefs of Staff (JCS) National Military Strategy, Information Superiority is the capability to collect, process, and disseminate an uninterrupted flow of precise and reliable information, while exploiting or denying an adversary's ability to do the same. One of the first steps toward the realization of Information Superiority is the achievement of interoperability between coalition nation information systems. This is vital for command and control entities.

The current U.S.- led military and intelligence infrastructure was designed to win the Cold War. The Soviet nuclear threat resulted in a myriad of missions that were funded to collect disparate, specific information without the (perceived) need to share this data with other nations. As time passed, a culture of parochialism between nations and even between different entities within a single nation led to a culture of secrecy that still exists. The control of information became more important than the dissemination of intelligence to policy makers.

A lack of well defined " rules of [collaborative] engagement " inhibits coalition interoperability. In a true collaborative, interoperable environment, commanders will share opinions and raw data in informal ways such as via electronic " chat rooms ". Only when the technology is understood and accepted by the commanders and policy changes made will additional barriers such as technology acquisition by coalitions be addressed. In the command and control environment, this issue manifests itself in questions concerning operational authority in U.S. versus coalition organizations.

Finally, the " Interoperability Hammer " is still not realized. Apparently, interoperability cannot simply be mandated or legislated; controlling authorities must appropriate funding according to interoperability guidelines.

2. The Approach and Analysis

Based on personal experience and interviews of DoD personnel, the author has selected organizational, acquisition, cultural, and security barriers for analysis. The author will apply recent experience in both the Armed Forces Staff College *Purple Sunset* exercise series and *Joint Warrior Interoperability Demonstration* (JWID) activities focusing on Australia-Canada-New Zealand-United Kingdom-United States (AUSCANNZUKUS) coalition interoperability in determining how research and development solutions such as the C4ISR Architecture Framework have addressed the problem.

Interoperability is a system attribute (there are efforts underway by *Mitre* and others to establish interoperability as an accepted metric by specifying *Levels of System Interoperability*), not the end goal. However, the solving of interoperability issues is key to attaining the NATO commander goals of:

- Better Battlespace Visualization
- Information Enabled Organisations
- Adaptive Decision Making
- Agile Battle Management
- Increase in Force Effectiveness

3. Analysis of Purple Sunset War Game/ Organizational Issues

The scenario for the War Game is the U.S.-led coalition concern for Tunisia, which is precariously situated between Algeria and Libya. The fictitious U.S. joint command is USMEDCOM. Interoperability issues surfaced in the organizational structure chosen by the students, the

information requested by the students, and the interaction between the J-2 element and the National Intelligent Asset entity.

By establishing the joint targeting boards, the students made effective use of resources. A clearer understanding of the Rules Of Engagement (ROE) – and particularly the escalation and adaptation of ROEs to the battlefield circumstances – may have prevented some confusion and saved some time. It was interesting to note the different viewpoints of the various components; measures designed to minimize the chance of "friendly fire" (anti-fraticide rules) were necessary to " facilitate coordination " according to ground components but unnecessarily " restricted the air " per the aviation components. This is a microcosm of the paradigm differences that exist not only between the nations but also between the components within an individual nation. In the area of information operations, the ROEs are even less defined.

Requests for Information (RFI) that were submitted by the (AFSC students roleplaying as) MEDCOM J-2 to the (students roleplaying as) National Intelligence Assets asked questions of a wide focus regarding the intentions of both Libya and Algeria. As the game progressed, the RFI requested more specific indicators of hostile intentions and expressed their intelligence needs rather than just asking for more resources. Interoperability problems were illustrated by time delays in responding to RFIs. For example, if diplomatic activity (permission to fly over coalition member airspace) was not completed in advance, intelligence vital to the commanders was not provided.

The students were persistent in their demands for intelligence in support of the commanders. Due to War Game infrastructure, they were forced to ask "Control" (the faculty running the game) for the entire range of intelligence questions in the form of RFIs. With the Intelink/ JDISS/ GCCS simulation elements planned for the next release of war gaming software, the students will learn to collaborate with analysts from various nations using coalition tools. The interoperability lessons learned once this new system is in place should include that training prior to the onset of hostilities is crucial. The equally important lesson addressing coalition acquisition will likely be beyond the scope of the exercise.

Often information system procurement contracts are structured such that information cannot be shared legally between procurement agents who would otherwise benefit from synergy. While there are obvious differences between the Services (the Air Force does not typically design and procure ships), there are areas where consolidation makes sense (all Armed Forces require some type of logistics system). In the U.S., PPBS procurement system does not lend itself to interoperability. The coalition agencies suffer from similar stovepiped budget structures that often stifle information sharing, resulting in parallel but uncoordinated efforts to solve the same problems. Collaboration between coalition entities involves a level of trust that is not easily maintained warfighting allies are often economic competitors. Even if one nation develops a system with the intent of sharing its capability, there is no effective coalition mechanism to facilitate sharing its cost. The coalition management must recognize the barriers and move forward together to achieve the goals. The Coalition Wide Area Network (CWAN) development (demonstrated in JWID 1999) is a step in the right direction.

Another management challenge is to overcome individual and institutional resistance to change. This is often related to the " not invented here " syndrome that permeates much of the coalition culture. This is the phenomenon where nations will not accept the practice or process or product that had its roots in a different country. Without a sharing of best practices across the coalition, effort is wasted in duplication and inefficiency.

Clearly the most obvious (and frustrating) barriers to coalition interoperability are antiquated regulations enforced in the name of " security ". Beyond the ridiculous system of " passing clearances " individually in message format when a shared database is an obvious solution, the need for security in designing interoperable systems is paramount to successful coalition collaboration and necessary for management acceptance. The paradox is that security can be viewed as both everyone's and no one's responsibility. The balance between the need to deliver information to the commanders and the need to protect sensitive collection methods must be maintained even in the collaborative coalition Information Assurance (IA) environment envisioned by JV 2010.

Security regulations that currently depend on compliance must yield to risk mitigation requirements based on accountability. In the coalition operations context, Technical Risk Management consists of three entities: IA, operational continuity, and change management.

Security is a recurring theme and a large driver for the types of information systems architectures pursued and designed by the coalition. Because the cost of a loss of information assurance in the coalition is measured in lives, security concerns permeate the coalition design and acquisition efforts. When security is an "add-on" or implemented in a hurry weeks before a product rollout, it generally results in restrictive procedural controls which enhance security slightly and hamper collaboration and interoperability tremendously. Information security must be an integral part of the design effort and issues must be discussed and managed (not avoided) at appropriate decision points in the development lifecycle.

One fallacy is that systems can be made "safe" simply by adding encryption. However, since proper encryption relies on the underlying operating systems which is not trusted to keep the files/data safe , how can this same operating systems be trusted to encrypt safely? A key component of Information Superiority is the protection of communications links from enemy interception. Some experts feel that the United States is actually falling behind in encryption technology and fear that arcane export restrictions may cost jobs and make our critical infrastructure more vulnerable to foreign penetration. The Security and Freedom through Encryption (SAFE) Act seeks to change the export laws in the hope that the U.S. will regain its position on the forefront of this vital technology. Once this position is re-established, consumer privacy advocates and law enforcement agencies (and even the coalition) can negotiate from a position of (technological) strength.

> With today's limited budgets, U.S. forces do not have the luxury of purchasing multiple sets of systems for each level of classification. Furthermore, the number of multinational operations that U.S. tactical forces are involved in has increased dramatically and will continue to increase in the coming years. Thus, finding solutions for this issue is vital. If IA solutions are not in place to enable rapid equipment reuse at different classification

levels, tactical forces will be forced to purchase additional equipment for each system-high level. Of course this will require additional funding.

As an example of multinational reuse of tactical equipment, recent NATO operations in the Balkans demonstrate the trend towards use of multinational forces in tactical operations. U.S. forces frequently report to coalition commanders from other nations. In addition to the usual issues language, standard operating procedures, etc. arising from a multinational chain of command, U.S. forces must protect cryptographic keys and algorithms from falling into the wrong hands, for a coalition partner today may be an adversary tomorrow. To prevent our IA solutions from being used against U.S. forces in the future, security solutions such as tamper proof cryptography, programmable cryptographic chips, and over-the-air key load and zeroize functions should be implemented in future tactical communications equipment.

4. THE RESULTS

Cooperation between coalition entities will not come about through radical reorganization nor from the indiscriminate application of technology. Technology is not a panacea; it must be applied appropriately to ensure interoperability. Instead, cooperation will come (and in fact, is coming) gradually as the coalitions define technical architectures that allow "portability" while filtering out the noise, deception, and ambiguity from data. The coalition must strive to produce " value added

The Intelink communications system is one of the success stories of coalition information sharing. Not surprisingly, one of the primary challenges in the implementation of Intelink at coalition facilities was integration into the security environment. Despite the now widespread acceptance of and dependence on the system for daily work, Intelink became successful due to the rigorous application of electronic publishing standards. The standards allow intelligence professionals to focus on the content of a report (which has abandoned the paper medium in favor of a multimedia presentation format), the fusion of data from disparate sources, and timely delivery (rather than the mundane " how does this look when I print it " issue). As the intelligence consumer, the commander will determine how the information is presented. The Extensible Markup Language (XML), an improvement over the Hyper Text Markup Language (HTML) used on Internet web pages (and of course Intelink) today, allows this freedom of choice. For NATO, the STANAGs will allow coalitions to build upon the success of Intelink.

All upgrades to U.S. DoD information systems are designed using the C4ISR Architecture framework. This is DoD's technical architecture framework used to promote the integration DoD information systems, expand the opportunities for interoperability and enhance DoD's capability to manage information resources across the Department. The C4ISR framework is divided into operational, technical, and systems processes that will improve the ability to execute operations and optimally meet the globally distributed information superiority needs of the warfighters within the increasingly important context of coalition operations.

Even when applying the mechanics of the C4ISR framework, designers must embody the spirit of the mandate. **Simply adhering to the framework in a vacuum from other simultaneous**

design efforts will result in many complaint systems that cannot interoperate! Additionally, the designers must take care not to ignore the " legacy " systems and must provide transition roadmaps so that all stakeholders understand the process. Adversaries will not wait while we rebuild coalition command and control systems from scratch; a balance must be maintained between current systems and future capabilities. One application of this idea is the employment of *STANAG 5066-Data Profiling at High Frequency (HF)*, which specifies waveforms and communications protocols that allow interoperability between the newest systems and legacy equipment.

Another relatively recent development in the area of design and procurement is the establishment of U.S. Department of Defense wide *Joint Mission Areas.* This concept (assuming proper extension to the coalition environment) will help in the interconnecting of separately developed C4ISR compliant systems.

Now that the Cold War has ended, coalition commanders (whether warfighters or peacekeepers) will be successful only with the support of the policymakers and ability of the coalition to embrace new analytical techniques of intelligence fusion through intelligence and collaboration techniques that rely on information system interoperability. This data sharing facilitates not only fused intelligence but also allows for differences of opinion between analysts to be identified such that the command and control elements can make the right decisions quickly.