C2 Interoperability

A Force Multiplier for Joint/ Combined Operations and Homeland Security

by
John A. Hamilton, Jr., Ph.D., Auburn University
Pamela A. Sanders, Auburn University
CAPT John Melear, USN, Space and Naval Warfare Systems Command
Mr. George Endicott, DON, Space and Naval Warfare Systems Command

The intensity and frequency of joint and combined operations, including operations other than war (OOTW) as well as the accelerating technological advances in command and control have highlighted C2 interoperability issues. The Command and Control Research Program continues to provide an important intellectual forum for military C2 interoperability problems. This forum has been particularly useful for members of the three service C2 acquisition commands and their major interoperability initiative.

The commanders of the service C2 acquisition centers, Communications and Electronics Command, Fort Monmouth (CECOM), Space and Naval Warfare Systems Command, San Diego (SPAWAR), Electronic Systems Center, Hanscom, AFB (ESC), formed the Joint Command and Control Integration Interoperability Group (JC2I2G). The JC2I2G exists to promote joint interoperability and change processes and structures by initiating "bottom up" change to implement Joint C2 integration and interoperability, and by supporting the unified commands in resolving interoperability issues of service-specific systems. Recognizing the pivotal role the US Joint Forces Command (USJFCOM) as the Joint Force Integrator, the Director, J6 of USJFCOM serves as principal member of the JC2I2G.

The JC2I2G proposed and the Under Secretary of Defense for Acquisition and Technology, Dr. Jacques S. Gansler, approved the establishment of the CINC Interoperability Program Offices (CIPO) at each C2 acquisition center and the establishment of the Joint Forces Program Office (JFPO). After a start-up period that was focused on "proving the concept," the CIPOs achieved sufficient short-term successes that they can now focus on long-term, non-trivial interoperability issues.

The CIPOs now play a major role between the originators of joint requirements and the designers of service C2 systems. The primary purpose of the Joint Forces Program Office is the horizontal integration of the CIPO efforts across the Unified Commands in direct support of US Joint Forces Command. As JFCOM's roles and missions evolve with respect to interoperability, so has JFCOM's interaction

In space of just a little more than two years, the JC2I2G organizations have gained significant insight into interoperability issues and solutions through experimentation, prototyping and results-oriented problem solving. This paper will suggest that the CCRP consider publishing a volume on C2 interoperability codifying the body of knowledge developed by the JC2I2G offices.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2002		**00-00-2002 to 00-00-2002**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
C2 Interoperability. A Force Multiplier for Joint/Combined Operations and Homeland Security	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Space and Naval Warfare Systems Command,53560 Hull Street,San Diego,CA,92152-5001**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**7**	

Interoperability in Command and Control applications is software-driven. This includes software-driven communication protocol stacks, operating systems and data element standards and security modules to give but an incomplete listing. For this reason, we believe it is reasonable to deal with interoperability by using an engineering lifecycle model.

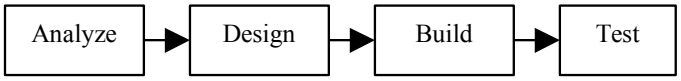


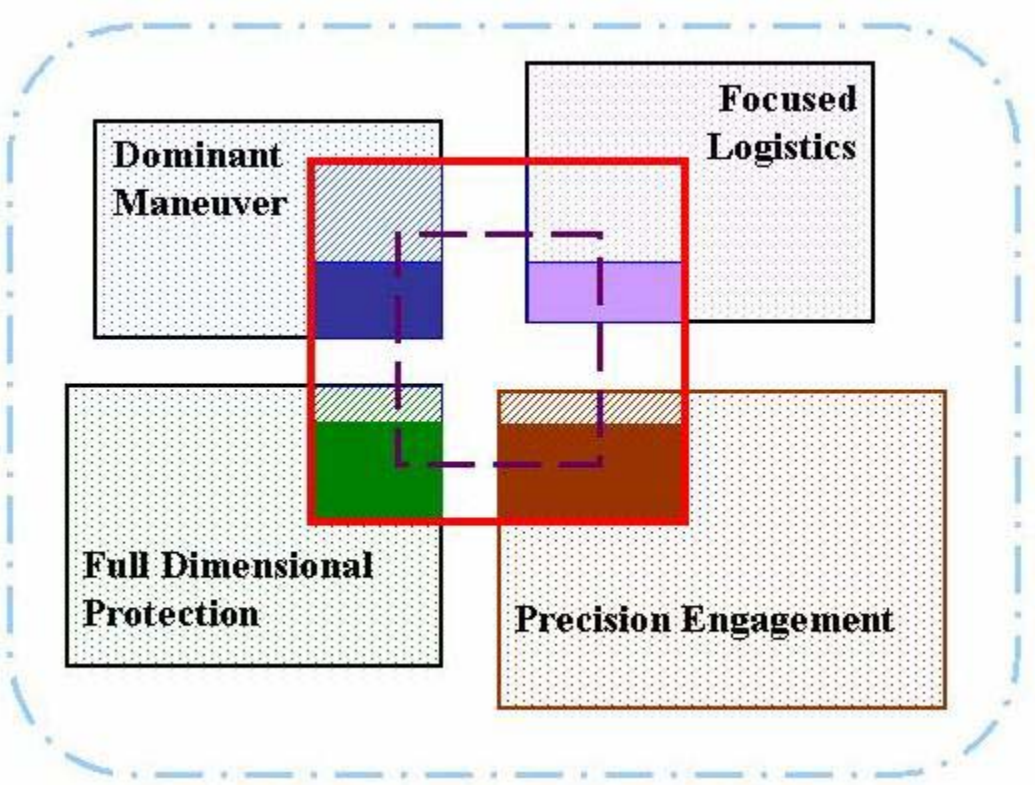
Figure 1. Engineer Thought Process.

In order to use the requirements -> design -> implementation -> test -> maintain software engineering model, it is important to first understand the domain to which this model will be applied (Figure 1).

Figure 2. Interoperability Domain.

This domain was defined during a USD (AT&L) directed study of DoD interoperability tools that continue to proliferate [Rosen and Parenti 2001]. A key insight is the realization that there are two dichotomies that affect this domain. The first dichotomy occurs between service requirements and joint command needs. The second dichotomy occurs between the combat arms/warfare communities/rated communities and the acquisition community as shown in Figure 2 above.

Any engineering approach begins with requirements definition. Interoperability requirements have to stretch across the domains shown in Figure 2. Simulation-based acquisition holds unique potential for interoperability requirements definition. However, successful application of SBA requires a program manager to negotiate his/her way across a disjoint domain as outlined previously. The successful development of a data model as shown in Figure 3, for the Global Information Grid requirements is an example of successful interoperability requirements definition [Hamilton, Murtagh and Deal 1999].



Key

Solid Thick Line: Joint Information Exchange Requirements (JIERs) necessary for interoperability. "MUST Share" Subset.

Thin Striped Section: "Planning" Information within each functional area

Thick Striped Section: "Survival" Information within each functional area

Large Dashed Line: Subset of information which can feasibly be shared between the new system and legacy system(s). "CAN Share" Subset.

Dash/Dot Line: Theoretical Boundary for information which might be shared

Figure 3. Global Information Grid Data Model [Hamilton, Murtagh and Deal 1999].

In Figure 3, the information from each of the four JV2010 functional areas is shown in rectangular boxes of different sizes. Several subsets of information are also identified; these subsets will be discussed in more detail later in this narrative. Note that the diagram is not "drawn to scale." For example, it is not our intent to imply that Precision Engagement will require more information than the other areas; we are just

trying to illustrate that different amounts of information may be required for each area. This same caveat applies to all data subsets represented on the diagram.

Additionally, DoD programmatic requirements limit some of the flexibility program managers have in adjusting to many changing requirements from many different agencies; rapidly advancing technology. Combine this with perennially uncertain funding and program managers face tremendous challenges in just fielding a system, let alone an interoperable system that uses state-of-the-art technology.

There are multiple ill-defined relationships between interoperability and network security. It is clear the computer network defense measures can present challenges to interoperability in terms of national policy, physical system implementation and trusted system relationships. It is unclear whether greater interoperability between national assets makes them more vulnerable to computer network attack. There are significant technical issues associated with communication system interoperability. In military communications, significant non-technical issues relating to national security policy and release authority also come into play.

Once coalition networks are established, the vulnerability of information systems may increase. Internal propagation of a worm with the characteristics of say "Nimbda" or "Code Red" can generate internal broadcast storms behind the network firewalls. This question has profound implications for homeland defense. Requirements play a key role here since interoperability can lead to increased end-point vulnerabilities across the National Information Infrastructure.

From requirements, the next step is design. Architectural methods can be applied to high-level design [Deal, Hamilton and Caudle 97]. Actual C2 architecture implementations will be used to illustrate how architecture, conformant to the DoD C4ISR Architecture Framework can be used to support, joint, combined and homeland defense interoperability. From an interoperability standpoint, homeland defense requires interoperability with non-DoD and non-Federal agencies.

Homeland defense requires interoperability across many existing systems across many different agencies. From a practical standpoint, this is a much harder problem then simply designing a system against a well-defined standard (i.e. TCP/IP); or even designing a system to interoperate within an existing system of systems (i.e. GCCS). Programmatically, DoD is not well organized to support retrofitting interoperability capability into existing systems. From an engineering viewpoint, it is often the case that there exist some parts of one system for which there is no equivalent part in the other system. Tactical Data Links are an excellent example of this problem. Technology advances that render the proposed solution obsolete before it is ever fielded can hamper a technical solution. Worse, the two systems, managed by two different program offices, may be on different upgrade paths with different implementation schedules.

The Joint Forces Program Office efforts in solving interoperability issues between the Army's Maneuver Control System (MCS) and the Marine Corps' Tactical Control

Officer (TCO) systems illustrates all of the issues associated with retrofitting a capability to interoperate within two fielded systems. The logic of having Army and USMC infantry battalions able to digitally exchange information is inarguable. But in fact, that specific requirement has not gone through the CJCSI 3170 requirements generation process. The interoperability requirements both program managers are working on are vague, and in the opinion of some flawed. The undisputed impact of these flawed requirements is a lack of resources to develop a non-trivial direct data exchange capability. It should be noted that amphibious units are required to interoperate with units afloat and then come ashore and interoperate with Army elements as shown in Figure 4.

Figure 4. Army – Marine Corps Interoperability.

The significant progress made by the JFPO, in spite of these obstacles, presents many important lessons learned.

Interoperability in the DoD has to be requirements-driven and this is extremely hard in the current system. CJCSI 3170 is an important step forward, but does not solve many of the fundamental obstacles to interoperability. More challenging is interoperating with non-DoD agencies who are not part of the Joint Staff's requirement generation process. Historically, the US Coast Guard has supported large-scale amphibious landings, but in recent years has operated quite independently from the Defense Department. Most other government agencies are much less prepared to interoperate with military units. Homeland defense must increase the priority given to C2 interoperability within the Defense Department. If DoD C2 systems cannot interoperate among themselves, then interoperation with non-DoD agencies is that much harder.

Conclusions

The CIPO's and the JFPO have been migrating research and activities from the pursuit of "fixing legacy applications and environments" to a "born joint" approach. This is a requirements based approach to interoperability. The majority of so-called "legacy"

interoperability problems will never be solved until replacement systems are brought on-board. As the MCS-TCO interoperability project demonstrates, resolving interoperability issues between two fielded systems is time-consuming and resource intensive. For this reason, interoperability clearly lies in the future, in the requirements that are being developed today. Interoperability is an increasingly important aspect of command and control and worthy of specific emphasis by the CCRP.

References

[Deal, Hamilton and Caudle 97] Deal, J.C., Hamilton, J.A., Jr., Caudle, J., "Unknown Lands and Uncharted Waters, The Army Enterprise Architecture," *3rd International Symposium on Command and Control Research and Technology*, June 17 - 20, 1997, National Defense University, Fort McNair, Washington, D.C., pp 426 - 449.

[Hamilton, Murtagh and Deal 1999] Hamilton, J.A., Jr., Murtagh, J.L., Deal, J.C., "A Basis for Joint Interoperability," 1999 Command & Control Research & Technology Symposium, US Naval War College, 29 June – 1 July

[Rosen and Parenti 2001] Rosen, J. D. and Parenti, J. L., "Aligning Interoperability Tools Within the DoD Battlespace," 2001 DoD Software Technology Conference, Salt Lake City, Utah, 29 April – 3 May 2001.

Authors

John A. "Drew" Hamilton, Jr., Ph.D., is an associate professor of computer science and software engineering at Auburn University. He has a B.A. in Journalism from Texas Tech University, an M.S. in Systems Management from the University of Southern California, an M.S. in Computer Science from Vanderbilt University and a Ph.D. in Computer Science from Texas A&M University. Prior to his retirement from the US Army, he served as the first Director of the Joint Forces Program Office and on the Staff and Faculty of the United States Military Academy. CRC Press publishes his book, *Distributed Simulation,* written with LTC David A. Nash and Dr. U. W. Pooch. email:hamilton@eng.auburn.edu

Pamela A. Sanders is pursuing a Masters in Software Engineering at Auburn University with a research emphasis in interoperability of C4 Systems. She has a B.A. and an M.A. in Psychology from Middle Tennessee State University and Auburn University of Montgomery respectfully. She is an active member of the Auburn Army ROTC program and will be commissioned in the United States Army upon her graduation. email:sandepa@eng.auburn.edu

Captain John Melear, US Navy is the Director of the Space and Naval Warfare Systems Command's Commander-in-Chief Interoperability Program Office (CIPO). Previously he served as the Commanding Officer of the Commander Naval Surface Force, U.S. Pacific Fleet headquarters Naval Reserve unit and the Navy Material Management Support Office Naval Reserve unit. He also served as Executive Officer of two Naval Reserve

units. Captain Melear has a B.S. from the United States Naval Academy, and is pursuing a Masters in Software Engineering at the Naval Postgraduate School. He holds two major naval warfare qualifications as a Surface Warfare Officer and as a Naval Aviator (Radar Intercept Officer). email:melear@spawar.navy.mil

George Endicott is the Deputy Director of the Space and Naval Warfare Systems Command's Commander-in-Chief Interoperability Program Office (CIPO). Previously he served as the Deputy Director of the SPAWAR Architecture Directorate in the Office of the Chief Engineer (code 051). Mr. Endicott has served in a variety of high-level assignments in both OSD and SHAPE. He is a recognized expert in C41 architecture and data interoperability. email:endicotg@spawar.navy.mil