"Command, Control (C^2) and Coalition Interoperability Post '911': Introducing the Network Centric Infrastructure for Command Control and Intelligence (NICCI)"

by Gary Illingworth

C3I Associates, and AFRL/RRS/IFSE
525 Brooks Road, Rome, New York, 13441-4505
Office: 315-342-1808
Fax: 315-361-5107
illingwg@rl.af.mil

ABSTRACT:

EFFORTS TOWARD INTEROPERABILITY, IN EITHER ITS JOINT UNITED STATES (CONUS) OR COALITION VARIETIES, HAVE EVOLVED SINCE WWII INTO TWO MAIN AREAS OF CONCERN: 'EQUIPMENT STANDARDIZATION AND TRAINING,' AND THE COGNITIVE PSYCHOLOGICAL ISSUES SURROUNDING INTEROPERABILITY AND COMMAND AND CONTROL; PROGRESS HAS BEEN SLOW IN BOTH OF THESE AREAS, HOWEVER.

THIS PAPER ADDRESSES PROBLEMS OF JOINT AND COALITION INTEROPERABILITY AND COMMAND AND CONTROL IN TERMS OF BOTH OF THESE AREAS, AND INTRODUCES TIME CRITICAL TARGETING (TCT) CURRENTLY AS A PRIME DRIVER FOR SEEKING CLOSER COALITION INTEROPERABILITY.

THE ATTACKS OF '911' AGAINST THE UNITED STATES AND THE WAR ON TERRORISM RE-EMPHASIZE THE NEED TO IMPLEMENT GREATER INTEROPERABILITY AMONG JOINT AND COALITION FORCES ACROSS STRATEGIC, NATIONAL, MILITARY, AND POLICE INTELLIGENCE AGENCIES, EMERGENCY RESPONDERS, NON-GOVERNMENT ORGANIZATIONS, AS WELL AS JOINT AND COALITION MILITARY BRANCHES. TO MEET THIS NEED, THE DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA), US NAVY SPACE AND WARFARE SYSTEM (SPAWARS), THE US ARMY RESEARCH LABORATORY, FORT MONMOUTH, NJ, THE USAF RESEARCH LABORATORY, ROME RESEARCH SITE, ROME, NY, AND THE US JOINT FORCES COMMAND ARE DEVELOPING THE "NETWORK CENTRIC INFRASTRUCTURE FOR COMMAND, CONTROL, AND INTELLIGENCE (NICCI)."

United States Joint Interoperability History:

In 1924, the British formed their version of a Joint Chiefs of Staff. Our American version became based upon this British version, coming into being in 1942. That year "an American 'unified high command' was adopted, and, patterned after the British, became informally known as the U.S. Chiefs of Staff." [1] During and after WWII, General Dwight D. Eisenhower became a noted proponent of Joint interoperability, and his legacy in that regard lives on in American military history. At one point after WWII, Eisenhower even advocated one uniform for all the service branches to facilitate standardization (seen across service branches today in the Battle Dress Uniforms (BDU) which are theater specific rather than branch specific). It wasn't until after WWII though, in 1947, that Joint interoperability efforts within the United States achieved any lasting result, culminating in passage of the National Security Act. This Act resulted in the formation of the Joint Chiefs of Staff (JCS), together with the Central Intelligence Agency (CIA), [2] The Department of Defense (DoD), and the United States Air Force (USAF). The Act's passage came only after difficult negotiations between the service

[1] "The Goldwater-Nichols Act Of 1986: Resurgence In Defense Reform And The Legacy Of Eisenhower," (U), by Major Greg H. Parlier, USA, Marine Corps Command and Staff College Marine Corps Combat Development Center, Quantico, Virginia, May, 1989, 111 pages.

[2] (Note: The Act formalized the Central Intelligence Group (CIG), which had been created in 1946 from diverse WWII intelligence agencies such as the OSS (of which television chef Julia Child, for example, had been an operative in Burma during the war) as the CIA.

branches - who thought, among other things, that Joint interoperability spelled doom for naval infantry forces and naval aviation. Even the FBI had to "roll up" its extensive intelligence collection efforts in Latin America that had prospered during the war and surrender its networks to the CIA. As a result of accommodations made to the service branches to get the Act passed, the initial JCS as formed gave more power to the service branch secretaries instead of the Chairman of the Joint Chiefs of Staff (CJCS). The power of the CJCS, thus limited, worked against the cause of Joint interoperability.

Furthermore, a reliance on nuclear ultimatums promulgated throughout the Cold War and known variously under different names [3] up until the 1980s, "provided the United States with the ability to procure 'defense-on-the-cheap.' Consequently, little attention had been paid to non-nuclear strategy since 1945." [4] This state of affairs continued until the passage of Public Law 99-143: "The Department of Defense Reorganization Act of 1986," commonly referred to as the "Goldwater-Nichols Act" which attempted to address Joint interoperability issues.

Coalition Interoperability History:

English speaking allies of the United States - Britain and Canada; formed the original term 'ABC' to represent the three nations in terms of interoperability. In 1947, the ABC armies developed the "Plan to Effect Standardization," the purpose of which was to continue the close cooperation that had developed during WWII between the British and other armies. At the conclusion of the first Basic Standardization Agreement (BSA) in 1964, Australia was added to the list of allies concerned with interoperability issues, and the term 'ABCA' came into use.

In 1948, the Air Standardization Coordinating Committee (ASCC) was formed to focus standardization on issues related to military aviation, or airpower; "the basic purpose and initial members were the same as ABCA, with Australia joining in 1964 and New Zealand in 1965." [5]

During the Cold War, "[f]aced with the threats from the USSR and the Warsaw Pact, the North Atlantic Treaty Organization (NATO), (including three members of ABCA and ASCC) early on established interoperability as a major goal to be pursued." Within NATO, however, nations using English as a second language became part of the interoperability equation. "NATO has pursued the admittedly elusive proper and effective levels of standardization in the areas of doctrine, procedures (tactics), and equipment (logistics and battlefield). Through separate organizations working in different

[3] (Note: Mutually Assured Destruction, or MAD, and 'massive retaliation' were two of these names.)
[4] "The Goldwater-Nichols Act Of 1986: Resurgence In Defense Reform And The Legacy Of Eisenhower," (U), by Major Greg H. Parlier, USA, Marine Corps Command and Staff College Marine Corps Combat Development Center, Quantico, Virginia, May, 1989, 111 pages.
[5] "Australian Defence Force Publication (ADFP) 2 (Operations Series – 'Division of Responsibilities within the Australian Defence Force'), Supplement 1 (International Interoperability Arrangements Handbook)," (U), Canberra, First Edition, 28 June 1995, p 6-1, in "Coalition Interoperability: An International Adventure," (U), *by Major Dean S. Mills*, USAF, Aerospace Power Chronicles, Maxwell AFB, Alabama, http://www.airpower.maxwell.af.mil

areas, [NATO members] have achieved varying degrees and permanence of success, and are currently [i.e. as of 1995] going through a major reorganization of their interoperability efforts…" [6]

"NATO, within its own alliance military structure, established area-aligned bodies to deal with interoperability, all of which used inputs from working groups to produce Standardization Agreements (STANAGs) and Allied Publications (APs). These bodies worked in the area of operations (tactics, procedures, and doctrine), materiel standardization, logistics, and NATO C^3" [7] (Command, Control, and Communications).

In the Pacific, "[t]he Australia, New Zealand, and United States (ANZUS) Treaty has been a cornerstone western alliance in the…region since its inception in 1952. The Treaty did not require development of interoperable military forces, but its impact has largely produced just such an effect. The Australian Prime Minister directed in 1957 that Australia would try to standardize armament and techniques with the United States, as far as was practical. [8] Australia and New Zealand then took up their respective roles in ABCA and the ASCC in the mid-60s."

Cognitive Issues of Coalition Interoperability

Efforts to minimize the effects of differences in equipment and training among English speaking coalitions have, for the most part been centered on traditional order of battle (OB) organizations, or echelons, through standardization in terms of equipment and training. These efforts have not addressed the "cultural differences in cognition and in world view… [which] can seriously impede smooth coordination among allies" [9] in terms of command and control. Various research on coalition or multinational interoperability has shown that "cultural differences can disrupt: situational awareness (SA), decision making, coordination, and communication in multinational coalitions…" through cognitive differences in at least five areas psychologists call 'power distance,' 'dialectical reasoning,' 'counterfactual thinking,' 'risk assessment and uncertainty management,' and 'activity orientation.' The message here is at least clear: "Even if coalition members are provided with the same information, what they see in the information may be very different." [10]

---

[6] "NATO's New Standardization Organization Tackles an Erstwhile Elusive Goal", (U), , *by Maj. Gen. Giovanni Battista Ferrari,* NATO Review, Vol. 43, No 3, May 1995, pp 33-34, , in "Coalition Interoperability: An International Adventure," (U), *by Major Dean S. Mills,* USAF, Aerospace Power Chronicles, Maxwell AFB, Alabama, http://www.airpower.maxwell.af.mil

[7] *Ibid.*

[8] "Australian Defence Force Publication (ADFP) 2 (Operations Series - Division of Responsibilities within the Australian Defence Force), Supplement 1 (International Interoperability Arrangements Handbook)," (U), Canberra, First Edition, 28 June 1995, p 1-1, in "Coalition Interoperability: An International Adventure," (U), *by Major Dean S. Mills,* USAF, Aerospace Power Chronicles, Maxwell AFB, Alabama, http://www.airpower.maxwell.af.mil (Note: The term 'practical' here is synonymous with affordable.)

[9] "Cultural Barriers to Multinational C2 Decision Making," (U), by Helen Altman Klein, Anna Pongonis, and Gary Klein, June, 2000. Presented to the 2000 Command and Control Research and Technology Symposium, Monterey, CA.

[10] *Ibid.*

The Joint and Coalition Interoperability Movement Gains Acceptance.

All interoperability is not of the coalition variety however. Even amongst the branches of the United States military, lessons learned from past operations indicate the need for much greater speed and precision in terms of command, control, and communications. There are many examples: US Navy ships unable to talk to a USAF aircraft flying overhead; during the invasion of Grenada in 1983, in a specific instance a commander had to resort to the use of a commercial long distance payphone from his position in order to call back to Ft. Bragg, NC to request C-130 gunship support for his unit, which was under fire. "In Grenada we did not have interoperability with the Army and the Air Force, even though we had been assured at the outset that we did…uncoordinated use of radio frequencies caused a lack of inter-service communications except through offshore relay stations and prevented radio communications between Marines in the north and Army Rangers in the south." [11]

It was these kinds of instances that lead to the Goldwater-Nichols Act of 1986. "The need of the military to remedy a situation that could cost lives, coupled with the bad publicity at the time, may have contributed to the congressional concerns that led to the [Act's passage] which redefined the relationship between the services and the [Commanders in Chief] CINCs." [12]

The Gulf War of 1990-91

The Act's passage served to focus attention more closely on interoperability issues into the future. "Desert Shield and Desert Storm provided real-world tests of the ability of U.S. forces to operate jointly as codified in the Goldwater-Nichols Act, as well [as] of equipment designed to ensure interoperability." [13]

During the Gulf War of 1990-91, "the difficulties in meshing the forces of 38 nations into anything resembling a smoothly operating military force were enormous." [14] Unclassified lessons learned from the Gulf War indicate that Air Tasking Orders (ATOs) had to be distributed in printed versions (in the case of the US Navy by helicopter from shore stations to the fleet) rather than electronic formats, (a time consuming task, especially on the battlefield), because of differences in software amongst US military branches. [15] "Even though many members of the Coalition were also members of other alliance organizations with interoperability forums, the successes and failures of those efforts were exposed by the light of coalition warfare." Another coalition example:

---

[11] "Interoperability: Is It Achievable?," (U), *by Anthony W. Faughn*, Program on Information Resources Policy Resources. Center for Information Policy Research and Harvard University, September 2001, 53 pages.
[12] *Ibid.*
[13] *Ibid.*
[14] "Coalition Interoperability: An International Adventure," (U), *by Major Dean S. Mills*, USAF, Aerospace Power Chronicles, http://www.airpower.maxwell.af.mil/
[15] "Interoperability: Is It Achievable?," (U*), by Anthony W. Faughn*, Program on Information Resources Policy Resources. Center for Information Policy Research and Harvard University, September 2001, 53 pages.

"Australia decided against sending some of its F-111C aircraft [to the Gulf] after issues of provision of jam-resistant radios, electronic countermeasure pods, and Identification-Friend-or-Foe (IFF) equipment were deemed too expensive or difficult to overcome." [16] "Operation Desert Storm demonstrated that tactical communications are still plagued by incompatibilities and technical limitations. At US Central Command (CENTCOM) corps and wing levels, a significant portion of the war was conducted over commercial telephone lines because of the volume and compatibility limitations of the military communications system. Communications were worse in the field. Particular difficulties arose with the tri-service tactical (TRI-TAC) communications equipment, acquired beginning in the late 1970s and fielded in the 1980s in an effort to guarantee interoperability." Difficulties also arose "stemming from the difference in the planning tools used by the Air Force and the joint community and those used by the Army in setting up the TRI-TAC communications architecture hubs (the circuit and message switches that provided the command and control backbone)." [17]

Within the US Army during the Gulf War, "There was no data conversion and translation between the information received via Joint Tactical Information Distribution System (JTIDS) in the Airborne Warning and Control System (AWACS) for transmission on the Tactical Digital Information Link (TADIL-A) net. Conversely, information received via TADIL-A in the AWACS was not available for conversion to the JTIDS net. Thus, the AWACS could not relay information it received through one system on another system."

Perhaps the most famous example dealing with interoperability during the Gulf War was provided by its Commander in Chief. General Norman Schwarzkopf's testimony before the Senate Select Committee on Intelligence, occurring at the conclusion of the Gulf War, and critical of intelligence occurring during the war, caused leaders to conclude that two separate intelligence 'empires' had arisen – a civilian intelligence culture and a military intelligence culture. Recommendations for fixing the problem included a closer working relationship. [18] Many military intelligence professionals, however, remained distrustful of the civilian intelligence agencies, and so were reluctant to ask them to do anything. An earlier report had concluded "the tactical and national intelligence communities appeared to be excessively isolated from one another, leaving each free to pursue self-sufficiency in their particular realms." [19] The Gulf War proved that demand outstripped supply in terms of bandwidth. [20] This high demand was caused by the field commander's

---

[16] Green, SQNLDR Mark; Owen, WGCDR Rick; and Harwood, SQNLDR John, Force Development (Aerospace) Branch, Australian Defence Headquarters, Canberra, interviewed by author, 9 May 1997, in "Coalition Interoperability: An International Adventure," (U), *by Major Dean S. Mills*, USAF, Aerospace Power Chronicles, http://www.airpower.maxwell.af.mil/

[17] "Interoperability: Is It Achievable?," (U*), by Anthony W. Faughn*, Program on Information Resources Policy Resources. Center for Information Policy Research and Harvard University, September 2001, 53 pages.

[18] "Intelligence Overhaul Urged; Agencies Could be Compelled to Cooperate," (U), *by George Lardner Jr.*, Washington Post, 6 February, 1992, p. A1

[19] "In a Changing World, CIA Organizing to do More with Less," (U)), *by George Lardner Jr.*, Washington Post, 5 July, 1991, p. A9.

[20] "Reshaping National Intelligence for an Age of Information," (U), *by Gregory F. Treverton*, Cambridge University Press, RAND Studies in Policy Analysis, 2001. http://www.cambridge.org (Note: That this shortage of bandwidth was actually caused by field commanders, trying to get another analysis of a

general distrust of the centralized analysis of the imagery – not the imagery itself. Finally, during the Gulf War, Battlefield Damage Assessment (BDA) "was one of the major areas of confusion…" [21]

African Operations of the 1990s

Interoperability problems continued in the post-Gulf War period. "African operations of the 1990s illuminated the difficulty in interoperability among multinational forces. 'Operation Restore Hope' (Somalia, 1991) emphasized the challenges associated with working with other countries and organizations. Equipment considered standard, even basic, in most western armies is simply not present in the inventories of many military contingents from developing countries. The equipment multinationals do bring with them is not likely to be interoperable. [C]rossing over the seams of national control created severe interoperability problems, a situation that occurred whenever one national contingent had to cross over the boundary to reinforce another." [22]

Although operations in Somalia did not involve any interoperability problems on the scale of Grenada or the Gulf War, "[t]he Marine Amphibious Ground Task Force, an organization set up and staffed by the Marine Corps, used obscure word-processing software, while CENTCOM, like most other military users, preferred another, more modern package. At headquarters, a similar difficulty plagued exchanges of electronic mail [e-mail]. At the tactical level, the ATO formats differed for east and west coast ships of the Marine Amphibious Ready Group. The most serious instance reported was that although the Army and Marines used the same single-channel tactical radios, they used different upgrades, resulting in incompatibility severe enough to prevent the Army hospital in Mogadishu from being able to talk to the Navy offshore for the first three weeks of the operation." [23] Three years later, in Rwanda, "the lessons learned identified similar challenges to interoperability in dealing with multinational forces as well as with private volunteer organizations (PVOs) and nongovernmental organizations" (NGOs) [24]

Interoperability and the North Atlantic Treaty Organization (NATO)

In the area of European coalition interoperability, since 1995 the leader has been NATO, who through its NATO Open Systems Working Group (NOSWG), the NATO Common Operating Environment (NCOE), and the NATO Command, Control, and Communications Technical Architecture (NC3TA) is working to provide a five volume series of manuals dealing with procedures designed to be effective in terms of a common

---

centrally provided imagery analysis is an interesting fact in itself. There was NO shortage of bandwidth, then – only panic.)

[21] *Ibid.* (Note: General Norman Schwarzkopf stated that "battlefield damage assessments from national intelligence agencies … were so hedged with qualifying remarks that they created serious confusion for commanders attempting to make wartime decisions.")

[22] "Interoperability: Is It Achievable?," (U*), by Anthony W. Faughn*, Program on Information Resources Policy Resources. Center for Information Policy Research and Harvard University, September 2001, 53 pages.

[23] *Ibid.*

[24] *Ibid.*

operating environment. The NATO Command, Control, and Communications Technical Architecture (NC3TA) "describes an architectural approach that lays the structural foundation necessary to attain interoperability between diverse C3 systems and provides the rationale on why this approach has been proposed for use throughout NATO." [25]

Interoperability Among Non-Governmental Organizations (NGO)

As soon as one leaves the Department of Defense (DoD) however, efforts in the area of interoperability amongst other government agencies, to say nothing of NGOs, almost cease to exist. This resulted in the Public Broadcasting story concerning children in the north mid-western United States who died from a disease because the local health center's only means to deliver incident reports to the Center for Disease Control (CDC) in Atlanta was through the US Post Office. The children's deaths were needless and were caused by the delay in communications.

Interoperability in the Light of the Attacks of '911.'

The events of '911' only serve to further emphasize the need for close coalition interoperability, not only among the military, but among strategic, national, and police intelligence agencies and first responder agencies, both within the United States and abroad. The Quadrennial Defense Review Report issued just weeks after the tragedy of 11 September made it abundantly clear that: "The attack on the United States and the war that has been visited upon us highlights a fundamental condition of our circumstances: we cannot and will not know precisely where and when America's interests will be threatened, when America will come under attack, or when Americans might die as the result of aggression. We can be clear about trends, but uncertain about events. We can identify threats, but cannot know when or where America or its friends will be attacked. We should try mightily to avoid surprise, but we must also learn to expect it. We must constantly strive to get better intelligence, but we must also remember that there will always be gaps in our intelligence. Adapting to surprise - adapting quickly and decisively - must therefore be a condition of planning." [26] The document emphasizes that "the DoD needs to leverage information technology and innovative concepts to develop an interoperable, Joint C^4 ISR architecture and capability that includes a tailorable Joint operational picture."

Not all coalition countries have the financial assets to support standardization however. Therefore, the burden for developing and fielding affordable interoperability methods, systems, and procedures has fallen to the United States. Before the attacks of '911,' efforts along these lines seemed almost optional – there would be time to develop and field interoperability, and efforts toward interoperability within the United States did not immediately require the participation of agencies outside the DoD. Since those terrible attacks however, both Joint and coalition interoperability, particularly among first

[25] "A Foundation for Coalition Interoperability Using NATO's C3 Technical Architecture," (U), *by Dr. Frederick I. Moxley*, Defense Information Systems Agency, *Lucien Simon*, NATO C3 Agency, *and Elbert J. Wells*, U.S. Mission to NATO, 11 pages.
[26] "Quadrennial Defense Review Report," (U), Department of Defense, 30 September 2001.

responder, strategic intelligence, national intelligence, police intelligence, and DoD agencies, has assumed critical importance. Furthermore, speculations that the terrorists may have profited from the attacks on the World Trade Center through the short selling of airline stock just prior to the attacks has pushed the importance information warfare again to the forefront of our attention.

To meet the needs for information management as set out in "Joint Vision (JV) 2020, the United States Air Force "Strategic Plan, Volume 3, Long-Range Planning Guidance Core Competency: Information Superiority" was developed. Future Command, Control, Communications Computers and Intelligence (C^4I) systems should be tailorable across the entire spectrum of operations, and integrated horizontally and vertically across components, functions, and levels of command. The goal of these new systems is to get the right information to the right user at the right time…all information is tailored to each user's needs. [27]

Critical Future Capabilities (CFCs) described by the Aerospace Command, Control, Intelligence, Surveillance, and Reconnaissance Center (AC2ISRC) include: Intelligence, Surveillance and Reconnaissance (ISR) systems; these must have a robust capability to rapidly and accurately disseminate situation awareness information (E-1.5); the capability to disseminate data with the minimum latency necessary to support mission requirements (M-2.3); center/node/platforms will publish their data allowing centers needing the information to subscribe using common software tools (M-3.1); Aerospace Command Centers and common facilities that are rapidly configurable, hardware and software infrastructure (C-7); standardized and interoperable information sets (C-10). [28]

The Joint Battlespace Infosphere (JBI).

To meet Joint networking interoperability needs, beginning in 1999 in conjunction with DARPA, AFRL/RRS began to develop the Joint Battlespace Infosphere (JBI). Considered a system of systems, the current AFRL/IF JBI Program is exploring JBI platform design alternatives through prototyping and analysis; assessing Commercial Off the Shelf (COTS) and Government Off the Shelf (GOTS) technologies and products; researching JBI-unique long term technologies; interfacing legacy systems to JBI prototypes for functional assessment; as well as recommending JBI platform designs and new technology for acquisition. [29]

The JBI has limitations, however. Within the JBI the emphasis is on Joint, rather than coalition operations. Cross cultural aspects such as language and cognitive differences are not addressed within the JBI. Only differences that may exist because of the nature of the service branches, the Army, Navy, Marines, and Air Force are addressed. In many cases, Joint and coalition commanders really want solutions, not just information. This means

[27] "Why NICCI Matters-- An AF-Centric View," (U), *by Lt. Col. Robert E. Marmelstein*, Joint Battlespace Infosphere (JBI) Chief, Joint Programs, Information Directorate, United States Air Force Research Laboratory, Microsoft PowerPoint Presentation, Rome Research Site, 1 March, 2002. Slide 3.
[28] *Ibid.*
[29] *Ibid.* Slide 6.

that commanders want their data to be analyzed before they get it, and they want specific recommendations, or a range of suggested alternatives, with regard to decisions they make. Also, problem solving in a coalition environment will often involve the rapid formation of ad-hoc teams comprised of a force mixture not available in terms of formal Order of Battle (OB). These teams are necessary because of possible limitations or differences with regard to the equipment and forces that may be on hand to accomplish a specific mission in a given region of the world. The ad-hoc team composition will be driven by the nature of the problem and member capabilities and affiliations rather than strictly by the best composition necessary to accomplish the mission. Beyond the information that JBI provides, the flexible, dynamic exchange of additional resources (services, assets, personnel) must be addressed. 'Soft disconnects' (in terms of policy, procedure, and terminology) must be mediated and overcome, taking away valuable time which could be spent specifically on mission planning and execution. To accomplish this, the Network Centric Infrastructure for Command, Control, and Intelligence (NICCI) project is under organization to ensure that needed technological capabilities are accessible to satisfy the needs of the warfighter.

The Network Centric Infrastructure for Command, Control, and Intelligence (NICCI).

Based partly on an earlier study in 1999 by the RAND Corporation, [30] in 2000 DARPA, AFRL/RRS, US Army Research Laboratory, Ft. Monmouth, and US Navy SPAWARS, began development of the Network Centric Infrastructure for Command, Control, and Intelligence (NICCI), which functions somewhat as a client portal-like front end to a systems of systems such as the JBI. To a user, NICCI will mean that with the proper access, the Joint and coalition user will get the information when it is requested, how it is requested, and from wherever it is requested. [31]

Habitats and NICCI

As previously mentioned, a large part of the problem involving coalition interoperability centers around the rapid formation of ad-hoc coalition teams. The challenge is to quickly enable disparate parties to cooperate and interoperate to solve common problems. Each team member should be able to provide information, services, personnel, and assets that bear on the problem. Barriers to rapid team formation include differences in doctrine, [32]

[30] "Habitats: Initial Concepts to Support Military Operations," (U), RAND Corporation, 29 January 2001.
[31] "Why NICCI Matters-- An AF-Centric View," (U), *by Lt. Col. Robert E. Marmelstein*, Joint Battlespace Infosphere (JBI) Chief, Joint Programs, Information Directorate, United States Air Force Research Laboratory, Microsoft PowerPoint Presentation, Rome Research Site, 1 March, 2002. Slide 6.
[32] (Note: in the current war on terrorism for example, in Afghanistan, Taliban strictures concerning women precluded their use by coalition commanders in the visible force mixture; in certain situations this stricture prevented using possibly the best person for the job and instead dictated that an all male force be visibly used. This issue was sidestepped by using female bomber pilots in the air as part of the invisible force, but using an all male force on the ground, where their allied use would have only made Taliban forces fight more fiercely.)

policy; processes; trust; equipment and infrastructure; vocabulary and language. [33] To define and meet these needs, NICCI uses the term "habitat" (the place in which a person or thing is most likely to be found) [34] to describe the conceptual construction of users with common interests to enable rapid and secure exchange of resources (information and services) between Joint Task Force (JTF) and Joint/coalition members. A habitat is a group of people and devices rapidly brought together to perform a task. Habitat technology links its members, helps establish its rules, and supports it with capabilities drawn, in part, from the Global Information Grid (GIG) computing and communications services. A habitat is equivalent to a workgroup -- but one enabled to achieve high performance, adaptive organization, a common context, and functional scalability. [35]

The task of the habitat may be transitory (e.g., to plan and execute a single time critical targeting sortie) or persistent (e.g., to determine targeting within a region for the entire duration of a conflict). Habitats, in a sense, exist already: e.g., a group on a conference call. "What differentiates a habitat from a generic workgroup is the underlying set of services that permit it to be established quickly, adapted for contingencies and exigencies; undergirded with business process rules; garner appropriate support from the Global Information Grid (GIG); and, in general, foster collaboration with a rich set of services and ontologies." [36] In terms of programming code, habitat software is minimal, consisting of small Java-like scripts, thus providing a core set of functions that can be universally reused. "While some coding may be required, it is limited to writing new applications or middleware interfaces to legacy applications that have not yet been included in a habitat." [37] (Once written, obviously, these interfaces may be reused.) "Developers will not be required to create an entire network architecture from the ground up." [38]

Time Critical Targeting and NICCI

Time Critical Targeting (TCT) is a subset of Time Sensitive Targeting (TST). Time Sensitive Targets are those which afford greater destruction to the enemy if attacked at a certain time. An example might be the containment of the enemy within a certain geographic area by systematically attacking the enemy's means of escape, such as a bridge. If the enemy is in the process of escaping, however, and is obviously planning to use a particular bridge as an egress route, that bridge then becomes a time critical target. The bridge must be attacked immediately or the enemy will escape across it.

The prosecution of TCTs frequently involve coalition assets; there may be intelligence about enemy movements provided by police agencies for example, Non-Government

---

[33] "Why NICCI Matters-- An AF-Centric View," (U), *by Lt. Col. Robert E. Marmelstein*, Joint Battlespace Infosphere (JBI) Chief, Joint Programs, Information Directorate, United States Air Force Research Laboratory, Microsoft PowerPoint Presentation, Rome Research Site, 1 March, 2002. Slide 9.
[34] Excerpted from The American Heritage Dictionary of the English Language, Third Edition Copyright © 1992 by Houghton Mifflin Company.
[35] "Habitats: Initial Concepts to Support Military Operations," (U), RAND Corporation, 29 January 2001.
[36] *Ibid.*
[37] *Ibid.*
[38] *Ibid.*

Organizations (NGOs), or even through information provided by Private Volunteer Organizations (PVOs), in other words intelligence provided by other than military sources.

TCTs pop-up, and are therefore frequently not included in the Air Tasking Order (ATO). These targets are acquired through the robust networking of dispersed and often disparate coalition warfighters. The ability to rapidly share this type of information improves general knowledge of the battlespace, situational awareness (SA), facilitates decision making and provides for a collaborative synergy of effort in Joint and coalition operations, thus improving Command and Control. The prosecution of TCTs are an excellent use of NICCI habitats for these reasons.

Templates and NICCI:

NICCI is synergistically robust, and provides: smart information push/pull; intelligent brokering of information; force (JBI), or habitat (NICCI) templates; remote user/platform proxy agents; automatic generation of metadata; determination of information pedigree; security. [39]

The unique features of NICCI allow users to publish information objects utilizing JBI publish and subscribe services. A JBI acts as the repository of heterogeneous information with a standard publish, subscribe and query core services capability for clients. Clients may subscribe by specifying their information requirements using well-formed predicates. Subsequently they will receive newly published information from a JBI. We may consider this to be information that is forward looking in time. The JBI also provides interfaces to a query core service. Clients may specify a well-formed query predicate using these interfaces. The result set will contain information objects that have been archived within the JBI. JBI may be linked to other information sources such as "Broadsword." An example of a NICCI subscription might be: "If the JBI receives any information about new International Maritime Satellite (INMARSAT) usage in country 'x,' send it to me as soon as possible (ASAP)." An example of a NICCI query might be: "what are the INMARSAT usage trends across several remote mountainous regions during the past year.

It is interesting to compare the "Enterprise Evolution" in terms of systems architecture available to DoD users such as the Air Force for example, with those of the business community – those available to users outside of the DoD - terrorists for example - today. USAF efforts to computerize command and control began in the late 1980s with the Computer Assisted Force Management System (CAFMS), and progressed to the Contingency Theater Automated Planning System (CTAPS), then the Theater Battle Management Core System (TBMCS), or where the USAF is today. In the business world, this is referred to as the "Traditional Enterprise Network." Today however, in terms of these systems, the business world leads the DoD using what is termed the

[39] "Why NICCI Matters-- An AF-Centric View," (U), *by Lt. Col. Robert E. Marmelstein*, Joint Battlespace Infosphere (JBI) Chief, Joint Programs, Information Directorate, United States Air Force Research Laboratory, Microsoft PowerPoint Presentation, Rome Research Site, 1 March, 2002. Slide 10.

"Network Enterprise." Efforts in development within the DoD using the "Network Enterprise" model include the Multi Mission Command and Control Platform ($M2C^2$), and Network Centric Warfare (NCW). In the business world, future system architecture is termed "Dynamic Enterprise." The development of NICCI will involve modern "Dynamic Enterprise" systems architectures. [40]

A comparison of three systems now either available or in the process of becoming available to achieve C^2 interoperability problem resolution is given in the table below:

System	Capabilities	Characteristics	Founding Technology
Current 'Enterprise' Systems, e.g. TBMCS, GCCS, GDSS.	Fixed information exchange; position driven; limited brokering.	Static; stove piped (vertical chain of command); service and or platform centric.	Examples include: the network; client server; collaboration.
Joint Battlespace Infosphere (JBI)	Dynamic info exchange; info tailored to user needs; information brokering.	Dynamic; integrated; joint.	E-commerce; info discovery and brokering; 'Fuselets,' force templates.
NICCI	Dynamic resource exchange; process tailored to problem; solution brokering.	Adaptive and or recombinant; seamless; coalition; uses 'Habitats.'	.NET; 'SOAP;' UDDI; JBI; Resource/Process Mediation. [XML]

Both the JBI and NICCI use the term "fuselet" to describe specific pieces of information, or small programs created expressly for a certain individual or agency that publish new information objects by refining or fusing other information objects in a relatively simple way based on the entire knowledge available at that moment in time. A fuselet may or may not contain a specific decision recommendation. Fuselets are made up of simple decision logic which can be expressed in a natural way (e.g. rules). Fuselets are created using scripting languages (e.g. JavaScript) or simple programming tools. An example of a fuselet could be: Each air base (e.g. Ramstein, Aviano, and Taszar) publishes a "base status" object to the JBI. A fuselet subscribes to these info objects and publishes a new aggregate "mission base status" object.

Templates and NICCI: Cognitive Issues

[40] "Why NICCI Matters-- An AF-Centric View," (U), *by Lt. Col. Robert E. Marmelstein*, Joint Battlespace Infosphere (JBI) Chief, Joint Programs, Information Directorate, United States Air Force Research Laboratory, Microsoft PowerPoint Presentation, Rome Research Site, 1 March, 2002. Slide 24.

Habitat or Force "Templates" are developed both in NICCI and the JBI to perform the information handshake between the subscriber, and or the publisher (a combat unit for instance), and the JBI. The Template defines what information the combat unit or habitat requires (an example might be the required accuracy of targeting information), what information the combat unit or habitat can provide (an example might be that the unit is equipped with a weapons pod camera, or that the NYPD squad car has a data terminal), and what are the combat unit's capabilities (an example might be 'munitions').[41]

NICCI will use its "habitat templates" to define its users. Where the JBI manages *how* interchanges occur, NICCI manages who, what, where, when, and why *content* passes or is brokered between users. Additionally however, NICCI will use habitat templates to bridge cognitive differences among its users. Habitats are not specific to a computer terminal or other device, but can consist of telephones, beepers, radio communications, all in addition to networked computer users. President Bush made a case for something like NICCI: "…a program where truckers can report anything that might be suspicious...in Maine. Governor King, working with the local FBI, signed up a lot of lobstermen...If people see anything suspicious, utility workers, [they] ought to report it." [42]

DoD subscribers and publishers commonly exchange information in United States Message Text Format (USMTF) in the form of Intelligence Reports, but these formats aren't applicable or suitable to coalition or non-DoD agencies, thus habitat and force templates have been conceived. These templates will apply cross-culturally throughout the coalition, bringing habitats together.

Human Intelligence (HUMINT) and NICCI: Police and Military Intelligence

The density of soldiers in the battlespace has been diminishing for centuries. Given the precise targeting capabilities today, "massed formations will only become tempting targets." [43] Also, "the distinction between the battlefield and the rest of society has also been eroding for some time." [44] NICCI uses this blurring of distinctions to advantage.

"By custom and law [within the United States], strategic intelligence and law enforcement had been very separate activities until the signing of Executive Order 12333 by President Ronald Reagan, which allows the CIA to 'participate in law enforcement activities to investigate or prevent clandestine intelligence activities of foreign powers or international terrorist or narcotics activity." [45] NICCI encourages information exchange. For strategic intelligence, the goal is policy, but for law enforcement the goal is convictions in court. Strategic intelligence is careful not to reveal its sources, but for law

[41] "Why NICCI Matters-- An AF-Centric View," (U), *by Lt. Col. Robert E. Marmelstein*, Joint Battlespace Infosphere (JBI) Chief, Joint Programs, Information Directorate, United States Air Force Research Laboratory, Microsoft PowerPoint Presentation, Rome Research Site, 1 March, 2002. Slide 15.
[42] http://www.whitehouse.gov/news/releases/2002/04/20020408-4.html
[43] "Reshaping National Intelligence for an Age of Information," (U), by Gregory F. Treverton, RAND Studies in Policy Analysis, Cambridge University Press, 2001, http://www.cambridge.org
[44] *Ibid.*
[45] *Ibid.*

enforcement, the sources eventually become a matter of court record. This means that the role of strategic intelligence agencies is frequently that of "tipping off" law enforcement agencies so that it's source's anonymity can be preserved. The trend is that "pure intelligence…will cede ground to tactical operations, law enforcement in particular. Law enforcement is to HUMINT what support to military operations is to SIGINT and imagery…now that communism is gone." [46] NICCI enables this.

The age of information has multiplied the sources intelligence professionals use, most of which are now not secret but are instead what intelligence professionals call 'Open Source.' "Boiler Plate Cold War American intelligence defined its trade as secrets where *collection* was the supreme task. Future intelligence will be information defined as a high-quality understanding of the world using all sources, where secrets matter much less and where the *selection* is the critical challenge." [47] What the future holds for intelligence is distinctly and vastly different than the intelligence world that went before it. Formerly obsessed with puzzle solving during the Cold War, the critical questions facing intelligence now are mostly diverse and mostly mysteries. For mysteries, information collected secretly may be helpful, but it is [now] seldom critical…"in the past, information was scarce, now it is *overwhelming*." [48] NICCI anticipates this.

The busy policy-maker of tomorrow will rely even MORE on information brokers, and as access to information multiplies, their need for processing it, if not analyses, will go up. As collection becomes easier, selection will become more difficult. "[Policy-makers] will be overwhelmed with information and will be more and more dependent on the people who process it for them," [49] i.e. information brokers. "Intelligence analysts will be only one form of information broker, CNN anchors, journalists, academics, free-lance processors, and Subject Matter Experts (SMEs) will be others. Policy-makers will prefer to have their information 'pulled' for them, rather than 'pushed' upon them. Intelligence used to restrict access to its secrets lest they leak *out*. Now communications needs to be robust so that all the critical information that goes into intelligence estimates can get *in*." [50] NICCI anticipates this need.

Future Command and Control (C^2) environment demand flexible, dynamic systems that enable problem solving in addition to information exchange, and systems that facilitate coalition interoperability. Toward this goal NICCI will provide important capabilities to enable seamless coalition operations, including rapid ad-hoc team formation consisting in theory of any of the possible elements, not just military elements, necessary to accomplish the mission. NICCI will provide intelligent resource brokering and exchange, and will automate the 'need to know' security process (lacking in SIPRNET, the Secure Internet Protocol Router Network), and provide bridging services for policy and or process disconnects. Our future information systems will be constructed rapidly

[46] "Reshaping National Intelligence for an Age of Information," (U), by Gregory F. Treverton, RAND Studies in Policy Analysis, Cambridge University Press, 2001, http://www.cambridge.org
[47] *Ibid.*
[48] *Ibid.*
[49] *Ibid.*
[50] *Ibid.*

and incrementally. This will enable Joint Task Force (JTF) commanders to customize and tune their own information architecture along with their force structure to match any given operational environment, and enable warfighters at all echelons to express and exploit their creativity and innovation to perform their jobs better.

Conclusion:

Problems associated with Command and Control (C2) involve both Joint and coalition interoperability. Joint interoperability among US forces has steadily but slowly developed since WWI, and especially since passing of the Goldwater-Nichols Act in 1986. Joint interoperability mattered during the Cold War, but increasingly since the end of the Cold War, coalitions have been established on an as needed basis to fight current wars and bring combatants to the negotiating table. Problems that exist among coalitions are both equipment and process oriented. In addition, specific problems arise with cognitive differences among coalition partners, especially those involving areas outside of Europe. Furthermore, the need to rapidly form teams of personnel and equipment from very different force mixtures often outside of government to meet the uncertain challenges typical of today's crises determines that these ad hoc teams be capable of both rapid assembly and decisive action. These teams must also be capable of contributing to the command and control, even though most lack the sophisticated computing systems typical in the West.

To fulfill the vast promise that tomorrow holds with respect to interoperability, the Network Infrastructure for Command, Control, and Intelligence (NICCI) is under design to work closely with such modern network architectures as the Joint Battlespace Infosphere (JBI). Although not mutually dependent on each other, a high level of synergy exists between NICCI and the Joint Battlespace Infosphere (JBI); these two programs will improve both Joint and coalition interoperability, and provide the mechanisms to prosecute time critical targets, perhaps the main specific problem in terms of interoperability today.

In terms of Situational Awareness (SA), the benefits NICCI will provide to its habitats is substantial. Missions involving Time Critical Targeting (TCT) for example, will greatly benefit from NICCI's ability to rapidly assemble ad hoc teams composed of police, medical, fire, and disaster relief, as well as traditional military elements, to bear upon targets requiring immediate attention. NICCI's habitat templates will be sensitive to the cognitive differences among coalition partners.

NICCI will provide an expanded Human Intelligence (HUMINT) capability by allowing habitats - clusters of users with common interests and tasks – to subscribe, contribute information, and query information from the Joint Forces Commander (JFC). These habitats can be quickly established whenever and wherever needed, and do not require the investment in terms of computing equipment that prevents many coalition partners from participating. NICCI will also facilitate the exchange of intelligence from today's main intelligence source types, strategic, police, and military.