Using Interoperability as an Effective Enabler of National Power

by

Mr. Jerome Jastrab
Department of the Army

United States Army War College
Class of 2014

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 15-04-2014	2. REPORT TYPE STRATEGY RESEARCH PROJECT	3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE Using Interoperability as an Effective Enabler of National Power	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S) Mr. Jerome Jastrab Department of the Army	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Colonel Dave Dworak Department of Military Strategy, Planning, and Operations	8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 7420

14. ABSTRACT

When conducting alliance or coalition operations, every nation sees interoperability as a desired force multiplier which enables economy of effort. Interoperability is also seen as a means to improve the effectiveness and efficiency of military and interagency operations in pursuit of national interests. However, there is not a common definition and understanding of the word itself, and there are many challenges. Additionally, interoperability occurs at the strategic, operational, and tactical level and covers the technical, doctrinal and human dimensions. Considering this multi-dimensional scope and the temporal nature of gains, a complete and absolute state of interoperability is not achievable. Therefore, in an environment of constrained resources, the Department of Defense must reconsider its approach. This paper recommends Department of Defense adopt an integrated team approach to interoperability and prioritize its efforts and resources on US allies and friendly nations with shared national interests. Subsequently, key staff leads and combatant commanders must play a much greater role in determining interoperability goals and objectives, and optimizing the results for the resources invested.

15. SUBJECT TERMS
Logistics, Multi-National Operations, Building Partner Capacity

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES 41	19a. NAME OF RESPONSIBLE PERSON
a. REPORT UU	b. ABSTRACT UU	c. THIS PAGE UU	UU		19b. TELEPHONE NUMBER *(w/ area code)*

Standard Form 298 (Rev. 8/98), Prescribed by ANSI Std. Z39.18

USAWC STRATEGY RESEARCH PROJECT

Using Interoperability as an Effective Enabler of National Power

by

Mr. Jerome Jastrab
Department of the Army

Colonel Dave Dworak
Department of Military Strategy, Planning, and Operations
Project Adviser

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title: Using Interoperability as an Effective Enabler of National Power

Report Date: 15 April 2014

Page Count: 41

Word Count: 7420

Key Terms: Logistics, Multi-National Operations, Building Partner Capacity

Classification: Unclassified

When conducting alliance or coalition operations, every nation sees interoperability as a desired force multiplier which enables economy of effort. Interoperability is also seen as a means to improve the effectiveness and efficiency of military and interagency operations in pursuit of national interests. However, there is not a common definition and understanding of the word itself, and there are many challenges. Additionally, interoperability occurs at the strategic, operational, and tactical level and covers the technical, doctrinal and human dimensions. Considering this multi-dimensional scope and the temporal nature of gains, a complete and absolute state of interoperability is not achievable. Therefore, in an environment of constrained resources, the Department of Defense must reconsider its approach. This paper recommends Department of Defense adopt an integrated team approach to interoperability and prioritize its efforts and resources on US allies and friendly nations with shared national interests. Subsequently, key staff leads and combatant commanders must play a much greater role in determining interoperability goals and objectives, and optimizing the results for the resources invested.

Using Interoperability as an Effective Enabler of National Power

> It is in the best interest of the United States that its Armed Forces be interoperable with its allies, Coalition partners, multinational organizations, and other friendly nations.

> —Chairmen of the Joint Chiefs of Staff Instruction 2700.01E

The United States (US) Department of Defense (DoD) invests significant energy and resources to obtain interoperability between the national services and with the militaries of our allies. The Department of Defense's current approach is layered, bureaucratic, and primarily stove piped along functional service, agency, or staff lines. Though there have been significant improvements in deliberate efforts to improve the process of designing interoperability into new materiel acquisitions, deficiencies in interoperability are often only exposed when the separate pieces of a multi-disciplined operation are finally assembled together and exercised. In order for Department of Defense to maximize its return on investment in interoperability, it is time for the Department to amend its approach to interoperability. The Department of Defense must exploit the opportunities to reform its approach to interoperability created by the pressures of fiscal constraints. The Department of Defense should follow the examples set in commercial industry and within the Department of Defense acquisition community, and take a standards based integrated team approach to interoperability. [1]

The value of interoperability is ingrained in the human spirit and understood at a very basic level. There is a shared logic among all cultures that when more than one person, or organized groups of people, engage in a common endeavor, the task becomes easier when all parties involved can operate with a common language, common tools, and common methods. This basic logic remains relevant today. In the context of this paper the endeavor is military operations. When conducting military

operations, especially combat operations, one very desirable means of achieving a successful outcome is by employing economy of force. Interoperability is one method of enabling economy of force when different services and nations form alliances or coalitions to conduct joint and/or combined operations.

As recent as February 2013, a North Atlantic Treaty Organization (NATO) publication clearly stated "The key goals have been to acquire new capabilities that can maintain NATO's strategic edge while increasing interoperability amongst its members in order to maximize cooperation and efficiency." [2] Interoperability is highly desirable because it can increase the effectiveness of combat operations and the efficiency of logistics operations by minimizing redundant functional capabilities. Effectiveness in combat operations is primarily achieved through improvements in standardization and commonality in command and control, communications, and procedures. Efficiency in logistics is primarily achieved by standardization and commonality of equipment, supplies and services. Logistics efficiencies manifest themselves in reduced national logistics footprints gained via economies of scale. The increase in effectiveness and efficiency achieved through interoperability both result in resource savings; the amount of time and treasure a nation must invest in order to execute military operations.

The US National Security Strategy places great importance on promoting security through multilateral and multinational cooperation and ensuring strong alliances.[3] In support of these alliances, the US military services routinely execute operations under the auspices of a joint and/or combined command structure, or as part of an ad hoc international coalition. A key enabler to achieving rapid and effective integration of other services and other nations in these types of operations is

interoperability. The enabling components of interoperability are "technical (including hardware, equipment, armaments and systems), procedural (including doctrines and procedures) and human (including terminology and training) dimensions, and complemented by information as a critical transversal element."[4] Nations have historically focused more on the technical side of interoperability. However, during coalition operations in Iraq and Afghanistan over the past ten years, the focus has shifted more to commonality of the human and procedural dimension; focusing in on interoperable information systems, procedures, and training. This shift was primarily due to the nature of coalition operations and the involvement of non-traditional allies.

Prior to delving further into the current issues surrounding interoperability, it is worth a brief review of what military professionals understand when referring to interoperability. Interoperability is a word often spoken, but lacks a common understanding. The old adage of a word having many meanings or a word meaning different things to different people certainly applies.

The information technology community (Department of Defense and commercial) claims the term as one of their own, and defines it as how computers and electric devices communicate with one another.[5] Joint Publication 1, *Doctrine for the Armed Forces of the United States*, also loosely defines and stresses the importance of interoperability, but focuses interoperability efforts on improving joint operations among the US national military services.[6] The North Atlantic Treaty Organization places great importance on interoperability due to its ability to improve the effectiveness and efficiency of inherently problematic multi-national operations. The North Atlantic Treaty Organization emphasizes the joint and multi-national aspect of operations conducted by

the different services from different nations. The Defense Acquisition University defines

interoperability within the context of the greater Department of Defense policy as "the

ability of systems, units, or forces to provide data, information, materiel, and services to,

and accept the same from, other systems, units, or forces; and to use the data,

information, materiel, and services so exchanged to enable them to operate effectively

together."[7] Joint Publication 3-16, *Multinational Operations*, further adds to the

confusion by listing compatibility, interoperability, interchangeability, and commonality

as a subsets to standardization.[8] So not only is there confusion on scope of

interoperability, there is also a lack of clarity from the perspective of scale.

Traditionally, most military professionals think of interoperability occurring

primarily at the tactical and operational level of military operations. However, NATO and

US joint doctrine address the need for interoperability at the tactical, operational, and

strategic levels in order to achieve the objectives associated with each echelon.[9] Sorting

through the nuances of national service doctrine in conjunction with the term as used in

industrial and professional services, it is understandable that not everyone shares a

single definition of interoperability. However, there is a general understanding of the

concept, and most definitions are consistent in theme. They are best surmised by the

simple definition in Joint Publication 3-0: "the ability to operate in synergy in the

execution of assigned tasks."[10]

In April 2000, a report of a French-German-United Kingdom (UK)-US working

group discussed coalition military operations and published a report titled "The Way

Ahead Through *Cooperability*." The report opined the definition of interoperability is

changing as the world around us changes.[11] The current doctrine on mission command

in Department of Defense is based on an idea that military operations are inherently a human endeavor and therefore in a constant state of flux because actions taken by one side are regularly offset by reactions of other side. From this it is logical to conclude that efforts to achieve interoperability are also in a constant state of flux since the supporting technical, procedural, and human dimensions of military operations are also in the same state. Lack of a common definition of the word interoperability implies it is transitory and justifies the commonly held perception that permanence in interoperability is also somehow unattainable or fleeting.

<div style="text-align:center">Interoperability – Measuring Success and the Perception Problem</div>

Lacking a common military and commercial definition of interoperability, it is logical to see why there is a perceived difficulty in defining success when looking at interoperability. When one reviews media forums, interoperability is often seen in the context of exercises or military-to-military activities where the deliberate goal of the activity was to improve interoperability. However, the implication is that the gains are more on a personal level and degrade until the next glowing press release about how the gaps in interoperability were closed yet once again; thus sending the message that the gains are fleeting and non-permanent. Since interoperability efforts are endeavored at three echelons: tactical, operational, and strategic, it allows for the mixed perception of success or failure when reviewing the same event from the different perspectives. Adding to this is the Chairmen of the Joint Chiefs of Staff (CJCS) Instruction which states: "the desired level of interoperability cannot be ascertained within a general statement of policy. The level is dependent on factors unique to each area where international military RSI (Rationalization, Standardization, and Interoperability) is the goal."[12] The conclusion when assessing the success or failure of US interoperability

efforts within the context of this policy is that each contact point for interoperability would be different, with a commensurate difference in a measurement of success. If a common understanding of desired levels of interoperability cannot be ascertained, then it is certainly difficult to measure and to perceive success from any echelon of command.

Why is it difficult for the average person to see the resources invested in interoperability as having a long-term and more permanent type of pay-off? Part of the reason is that state of interoperability is indeed dynamic and constantly changing. Driven by the desire for continuous improvement, militaries across the globe continue to transform themselves by modernizing equipment, changing organizational structure, and adapting doctrine. Even NATO recognizes this reality and has established a permanent organization, the Headquarters Supreme Allied Commander Transformation, to stay abreast and deal with this issue at the alliance level.[13] The life-cycling of personnel through the military, which includes regular duty rotations, results in the constant gain and dispersion of knowledge and experience regarding interoperability. When one considers the multitude of contact points between nations and services from the strategic to tactical levels, degrees of interoperability would consequently experience a regular ebb and flow.

One of the driving forces of change is evolving technologies and the ever accelerating pace of technological developments. The impact of this on the military is what is referred to in the Army War College as a "wicked problem." The pace of technological change in many cases outpaces the military materiel acquisition process. This often drives the services to purchase commercial off the shelf equipment and use

rapid fielding initiatives which bypass many of the steps where interoperability is evaluated and addressed in the acquisition process. Complementing rapid fielding is the requirement to rapidly change doctrine. Accelerated integration of materiel and doctrine into the force creates new seams where interoperability gaps are exposed.

A recent example is the proliferation of robotics used in operations in Iraq and Afghanistan. In response to fleets of rapidly developed and fielded equipment, the US military introduced a new 'Interoperability Profile' for what was labeled Unmanned Ground Vehicles (UGV) in 2011.[14] This interoperability profile applies to all of Department of Defense, but focuses on the US Army and US Marine Corps. The profile covered all the aspects of UGVs from the mechanical platform, communications, payloads, and control – which include software, command and control (C2), and mission planning. From a tactical and operational perspective, it looks like a successful integration of interoperability into a rapidly developing technology and equipment platform. However, from a strategic perspective, it appears interoperability initiatives were an afterthought. The Department of Defense or other federal agencies did not consult and plan with allies and the international robotics industry to address UGV issues such as technical standards, operational employment, doctrine, and procedures. In reality it took two years for the US to address UGV interoperability with allies. In 2013, the U.S. Army (represented by the Tank Automotive Research, Development and Engineering Center and the Maneuver Battle Lab), NATO, Germany, and Turkey conducted UGV interoperability tests at Fort Benning. The intent of tests was to expose gaps between the US and allies equipment. While testing has been going on for three years within the Department of Defense's Robotic Systems Joint Project Office, the

meeting was the first time foreign military representatives participated.[15] In hindsight

was this a success or failure? Depending upon the where, when, and who made the

observation, both are a correct assessment. Prior to the UGV example, the United

States Government Accountability Office published a report in 2005, with similar

findings in regards to Unmanned Aircraft Systems (UAS).[16] However, In this case

interoperability gaps were first exposed at the joint level and then eventually again at

the multinational alliance level. The eventual fix was a Department of Defense

ratification of the NATO Standards Agreement on UAS joint and combined

interoperability. These are just two examples demonstrating the difficulty in defining and

measuring the success or failure of interoperability.

Another interoperability challenge is rapid technological developments that result

in new, or perceived new, domains of military operations. Creation of new domains,

such as cyberspace and space, begins a whole new cycle of exposing gaps and the

need for interoperability across the spectrum of operations. New domains impact the

technical, procedural, and human dimensions of interoperability, and expands

interoperability challenges across a broader spectrum; spilling over to the whole of

government, as well as the commercial sectors. Specific to cyberspace, the inform

parameter (which is a transversal element of the other three dimensions of

interoperability) is predominate, and therefore has a disproportionate impact on

interoperability efforts in the other domains.

> Space and cyber capabilities will be increasingly employed prior to kinetic
> operations and both forces and their command chains will need to be
> prepared for information denied environments. In many nations, space
> and cyber capabilities are not exclusively owned by the armed forces and
> so will also require pan-government efforts and close co-operation with
> industry. Cross-domain operations will require greater interdependence

between the services, improved and robust cross-domain networks providing information down to the most tactical levels, and the adoption of a dual-track approach of disruptive and stealth technologies.[17]

The most exposed seams generally deal with how systems connect and interact with the pre-existing domains. "One of the risks highlighted by the Joint Operational Access Concept was that integrating cross-domain capabilities, particularly across multiple lines of operation, might become too complicated to be practicable or too inefficient."[18]

Another aspect of rapid change that impacts interoperability is the increasing involvement of defense contractors in ongoing military operations. The drive for efficiencies in militaries across the globe and the desire to minimize the number of military personnel in forward theaters adds another dimension which complicates operations. The US government calls on defense contractors to perform an increasingly wider range of services in lieu of military personnel, to include 'use of force' scenarios for protective service personnel. However, the contractual elements of flexibility and specificity and oversight are at odds with each other in every contract. The more detailed the specifications of a contract, the less flexibility there is for the military to adapt contracted services to dynamic operations and environments. Each individual contract expands the spectrum of technical, procedural, and human dimensions of interoperability that US and allied military personnel must integrate into their operations. Recent operations in Iraq and Afghanistan exposed interoperability gaps between military forces and defense contractor personnel supporting military and interagency operations. The most notable being the incidents associated with Blackwater Security Company, traceable to the doctrinal and human dimensions of interoperability. Military contractors "operate under completely independent chains of command…use separate radio frequencies and separate intelligence systems to those of national armed

forces."[19] Add to this situation unique procedures, the use of non-standard equipment and communication platforms, and perhaps different spoken/written languages, and one can quickly see how these factors can exponentially increase interoperability challenges during military operations.

Simplistically, interoperability success at the tactical and operational level is measured in terms of standardization and commonality of the technical, procedural and human dimensions. At the strategic level it is measured by the effectiveness of cooperation among allies at the international level that results in the creation of formal alliances or coalitions to address common political objectives. Interoperability as an enabler is manifested in the production and ratification of standardization agreements among signatory nations. Standardization agreements are meaningless if they become obsolete or lose their relevancy to national interests and policy, or the alliances they serve.

If interoperability qualifies as a wicked problem, then pursuit of interoperability requires iterative solutions just like other wicked problems. In that context, applying effective metrics to measure the success of interoperability initiatives becomes a critical component of the iterative process; a process where absolute interoperability is never achieved. In reality, gaps in interoperability are constantly exposed or re-exposed. Solutions are in a constant state of dynamism, regularly developed, renewed, or sustained. Therefore, the approach to measuring the success of interoperability as outlined in the CJCS Instruction 2700.01E is correct. The Department of Defense and Combatant Commanders can only measure success in a contextual manner. Success is dependent on current national interests and priorities at the strategic level. Success is

also dependent on the current realities of assigned national and foreign interagency and military forces at specific point in time, within the pre-existing geopolitical conditions. Steps to identify and improve interoperability gaps are constant, but measuring success is temporal and contextual.

<div align="center">Current Department of Defense Efforts in Support of Interoperability</div>

The CJCS is tasked with "Advising the Secretary of Defense on interaction between international interoperability efforts and national military force goals, planning, and programs."[20] In response, the CJCS has tasked several agencies and staffs to manage and provide oversight of Department of Defense interoperability efforts. When researching interoperability, one is struck by the sheer volume of organized efforts by nations in pursuit of interoperability, from both the management and program perspective.

Within the Department of Defense, interoperability for the national services is addressed through the Defense Standardization Council chaired by the Under Secretary of Defense for Acquisition, Technology, and Logistics. The Council provides senior management oversight and direction for implementing the DSP and other initiatives related to Department of Defense specifications and standards.[21] Director, Defense Standardization Program Office is responsible for policy and oversight for the Council. The Heads of the Department of Defense components are responsible for materiel standardization throughout the acquisition process.[22]

The Department of Defense addresses Interoperability with allies and friendly nations through a dense network of the Joint Staff, Service Staffs and Commands, and special organizations. The Department of Defense then addresses engagement through two categories: NATO entities and Non-NATO entities. The NATO entities are covered

by the Defense Intelligence Agency, the Joint Staff, the National Geospatial-Intelligence Agency, the Office of the Secretary of Defense, the Department of Defense Explosives Safety Board, and the services. Within the NATO entities there are over 300 working groups, boards, panels, committees, sub-committees, steering groups, conferences, priority areas, and requirements experts teams that these lead staffs and agencies cover for Department of Defense. This summary demonstrates the current bureaucratic and stovepipe approach to interoperability and the possible avenues for redundant efforts due to lack of singular oversight of the main lines of effort.

The Non-NATO agencies are split into four sub-categories: USA American, British, Canadian, Australian, and New Zealand Armies' Program (ABCA) [U.S. Lead Agent: Army]; US Air Force Air and Space Interoperability Council (ASIC) [U.S. Lead Agent: Air Force]; US Navy Australia, Canada, New Zealand, United Kingdom, and U.S. C4 (AUSCANNZUKUS C4) [U.S. Lead Agent: Navy]; and Allied and Multinational Working Groups. Within the Non-NATO entities there are over 50 capability groups, support groups, working groups, boards, committees, councils, and programs that the services, lead staffs and agencies cover for Department of Defense. The figure below visually depicts the relationship with some of the Allied and Multinational Working Groups.

Logos	Fora	Focus	Australia	Canada	New Zealand	United Kingdom	United States	Other
	ASIC: Air & Space Interoperability Council	Aerospace interop.	X	X	X	X	X	
	ABCA: American, British, Canadian & Australian Armies	Army interop.	X	X	X	X	X	
	AUSCANNZUKUS: Australia, Canada, New Zealand, UK, US Naval C4	Naval C4	X	X	X	X	X	
	CCEB: Combined Communications-Electronics Board	C3I	X	X	X	X	X	
	MIC: Multinational Interoperability Council	Military interop.	X	X		X	X	X
	MIP: Multilateral Interoperability Programme	C2I interop.	X	X		X	X	X
	TTCP: The Technical Cooperation Program	Military S&T	X	X	X	X	X	

Figure 1: "The Multifora" Defense Partnership Efforts[23]

To demonstrate the link between national interests and interoperability, the Department of Defense is using the non-NATO entities to reinforce the US policy shift towards Asia, and the US is re-invigorating bi and multi-lateral interoperability efforts with traditional alliance partners. There is a renewed interest from the US to conduct bi-lateral activities with alliance partners in the region, primarily with Japan, Korea, and the Philippines.[24] As recently as September 2013, General Dempsey met with South Korean leaders to talk specifically about interoperability efforts; primarily to counter China's growing influence and to invest in anti-access/area denial strategies.

Subordinate to each agency and service are organizations to cover specific technical and functional areas. For the sake of brevity they are not listed, but one simple

example is the Joint Interoperability Test Center which "conducts testing of national security systems and information technology systems hardware, software and components. Services include developmental, conformance, interoperability, operational and validation testing."[25] Within each technical and functional area there are organizations and staffs Department of Defense-wide responsible for interoperability efforts. This demonstrates the tremendous resource commitment Department of Defense makes in pursuit of interoperability within the national services, with allies, and with friendly nations. Unfortunately, it also connotes the significant bureaucracy required to support all these separate initiatives as well as the inherent inefficiencies associated with this approach.

Commercial industry has responded to overly stove piped structures, where ultimate ownership of process was in question, by developing integrated process teams. Integrated process teams are diverse functional teams that were built to rapidly integrate singularly technical areas in pursuit of a single outcome. The Department of Defense recognized this philosophy, and implemented mandatory use of Integrated Process and Process Development (IPPD) within the acquisition community and supporting defense industrial base.

> IPPD is a management technique normally implemented by Integrated Project Teams…that simultaneously integrates all essential acquisition activities through the use of multidisciplinary teams to optimize the design, manufacturing, business, and supportability processes. IPPD is currently in use in many commercial and government organizations.[26]

In order to best employ the resources available, the Department of Defense should emulate this acquisition best practice into the field of interoperability and move away from stove piped and the primarily staff managed process.

There is little doubt the plethora of Department of Defense staffs and organizations assigned responsibility for interoperability efforts are devoting resources to make progress within their assigned fields. However, these entities operate within the context of their perceived priorities and report to staff chiefs and not to supported commanders. The logical question from this observation is whether the ways and means being employed are achieving the desired ends to ensure the future success of combatant commanders? If not, are combatant commanders not reaching the full potential of the forces available to them in pursuit of the desired ends in the National Security Strategy?

Other countries pursue interoperability with allies and friendly nations in a similar manner to the US. In general, they commit national resources towards pursuing interoperability based on national fears, honor, budgetary realities, and defined national interests. Thematically, interoperability is so pervasive internationally because it is a means to achieve the ends established in national security strategies. Taking Europe as an example, figure 2 below pictorially depicts the structured approach taken by European nations to foster cooperation, standardization, commonality, and interoperability across a wide spectrum of technical fields. Nations engage allies and friendly nations based on national interests directly associated with the function being governed. Nations meet, cooperate, and surrender sovereignty when they believe it is in their best national interest to do so.
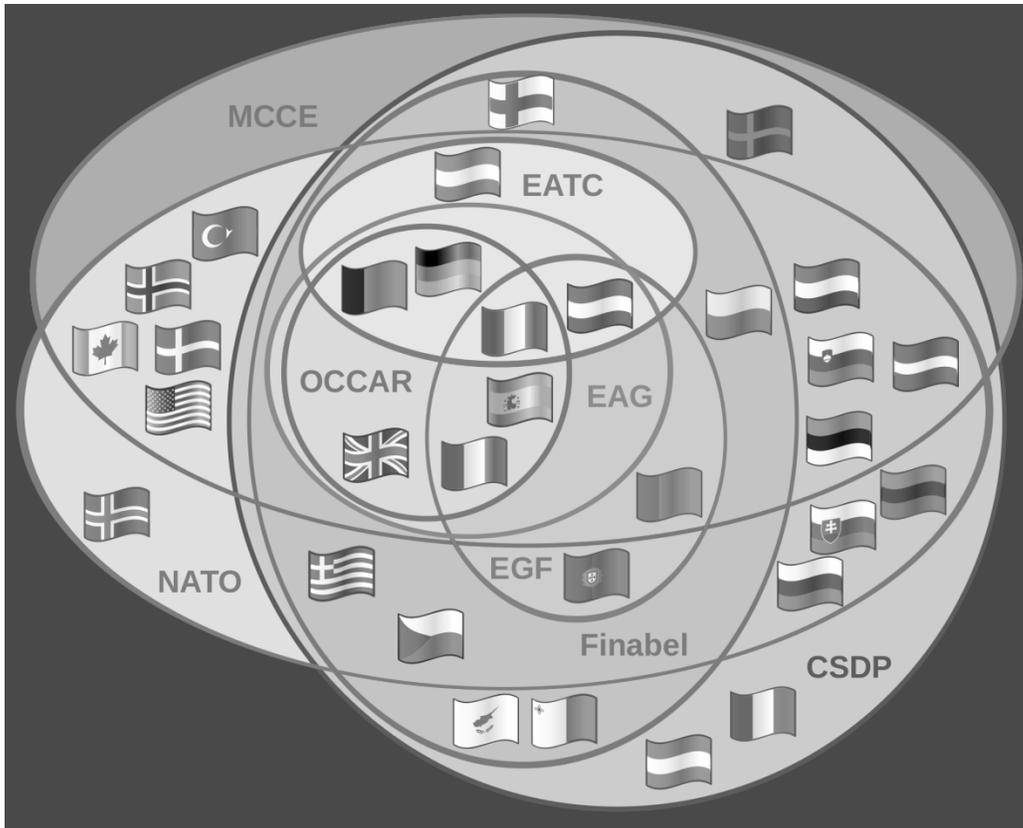
MCCE - Movement Coordination Centre Europe; OCCAR - Organization for Joint Armament Cooperation; EATC - European Air Transport Command; EAG - European Air Group; EGF - European Gendarmerie Force; FINABEL - Interoperability Center of European Armies; CSDP - Common Security and Defense Policy

Figure 2. European Defense Partnerships[27]

Challenges to Attaining Interoperability

There is a perception that despite being highly desirable, interoperability among the US and its allies remains elusive. No doubt, the combat operations in Iraq and Afghanistan over the past 12 years have improved interoperability between participating NATO allies and coalition partners. However, advancing technology and the steady decline in defense spending by allied nations is creating an ever widening gap between the US and its allies. Pierre Claude Nolin stated in a NATO Parliamentary Assembly committee report that "the performance of the European armed forces in NATO or US

led coalition operations, such as in Kosovo, Afghanistan and Iraq, demonstrated clearly the existence of a glaring transatlantic capability gap that has limited the interoperability of multinational forces and the efficiency of coalition war fighting."[28] Is interoperability a victim of the 'NIMBY Syndrome' (Not in My Backyard)? A term used to express "opposition by local citizens to the locating in their neighborhood of a civic project, as a jail, garbage dump, or drug rehabilitation center that, though needed by the larger community, is considered unsightly, dangerous, or likely to lead to decreased property values."[29] Something seen as needed by the US military services and members of an alliance, coalition, or group of like-minded friendly nations, but where the first tier members do not wish to surrender defense industrial capability or share technology to achieve the desired level of interoperability? Achieving interoperability inherently involves sharing intellectual property, technology, and sovereignty in exchange for a beneficial interdependent defense relationship.

Within the context of articulated policy and theory, and established culture and practices within NATO and other organizations, the average person has difficulty understanding why such an organized and deliberate approach to interoperability does not produce more tangible and enduring results. At face value it would appear that there are flawed basic premises, flaws in doctrine, or more likely a lack of commitment to back up the words. An example is the failure of the majority of European NATO members to spend the declared NATO goal of spending 2% of GDP on defense. A realist would argue interoperability is achievable only when it genuinely supports a nation's national interests, or when circumstances force nations to cooperate. So if declarations for increased interoperability are not genuinely followed by committed

actions, it is because it is not in a nation's national interest at that particular point in time.

A review of available military related public sources offers more specific insights. Joint Publication 3-16 *Multinational Operations* states "factors that inhibit interoperability include restricted access to national proprietary defense information; time available; any refusal to cooperate with partners; differences in military organization, security, language, doctrine, and equipment; level of experience; and conflicting personalities.[30] Bernard Thorette states barriers to interoperability are "competing national interests and perspectives, differences in national capabilities and military cultures, and limitations on intelligence sharing."[31] Neatly summarized as fear, honor, and interests.

Reviewing the analytical report published by the Reliability Information Analysis Center on challenges to interoperability in previous US military campaigns, a key point is immediately established. The report emphasizes the importance of addressing interoperability at all echelons: strategic, operational, and tactical.[32]

At the strategic level the main challenge is shifting political objectives which can impact the unity of a coalition, and thereby ultimately the success and legitimacy of a multinational operation. This was seen during the course of the wars in Iraq and Afghanistan as several European nations (Spain, Hungary, Netherlands, Norway, and Portugal) pulled out of the coalition in 2004-2005 as the operation became an occupation; representing a shift in political objectives, where ruling parties became out of synch with the will of their constituencies. The resulting political backlash from voters in Spain ultimately unseated the ruling party. This likely played a role in motivating the other European national governments to withdraw in order to avoid the same fate.

Additional interoperability challenges at the strategic level are the willingness of nations to openly share their national strategic objectives and the plans to achieve these objectives, establishing national policy on information sharing, research and development cooperation, rules of engagement, and limitations on dual-use technologies. Lack of synchronization between nations in a coalition in these areas can have a very detrimental effect on unity of effort and compatibility of forces within the sense of capability and skills. If nations implement policies designed to protect their national defense industry, then this will clearly prohibit or inhibit cooperation with other nations on defense programs or mutual pursuit of weapons systems.[33]

At the operational level, the challenges are more information based, where challenges include intelligence sharing and doctrinal compatibility in regards to command and control procedures, staff planning, and operations oversight. The Reliability Information Analysis Center's *Guide on System Interoperability* consistently found during operations Desert Fox (Iraq), Operation Allied Force (Kosovo), and Iraqi Freedom that there was a lack of interoperability and compatibility between US and coalition partner nation's communications systems, and information and intelligence databases. This lack of interoperability caused problems in maintaining common operating pictures across various functions and inhibited sharing of critical data; complicating command and control and individual staff's ability to assess the environment and plan future operations.[34]

At the tactical level, interoperability challenges manifest themselves in everyday tasks in the materiel and command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) arenas. At this level it is the simple ability of

tactical units to effectively communicate using tactical radio-telephone systems, share intelligence, and execute common tactics, techniques and procedures at the same skill level in support of coalition operations.[35] These issues become even more problematic when conducting joint and air-ground operations which require effective interoperable communications equipment and common doctrine to achieve the desired effects and avoid fratricide.

In sum, interoperability challenges are faced within each of the dimensions of interoperability: technical, procedural, and human; and then again at the echelons of interoperability: strategic, operational, and tactical. Viewed through the prism of a matrix, one can see the challenges to interoperability as a very multi-dimensional problem; one that does not lend itself to resolution through stovepipe assignments of responsibilities.

One last challenge is capturing and institutionalizing interoperability achievements, specifically within the area of knowledge sharing. This area is especially challenging considering the breadth and scope of information and the dynamic state of interoperability knowledge as discussed earlier. The formation and maintenance of such a volume of knowledge is a monumental task. The US, alliance partners, and friendly nations are expending significant intellectual talent and resources to improve interoperability on many levels and through many venues. Beyond personal experience, the knowledge gained is worthless if that information is not documented and available to future leaders for use in future operations. If interoperability gains are not shared and easily available to US military members and the US's closest allies, then the nation has made poor investments.

The North Atlantic Treaty Organization and ABCA make serious attempts to document their information on interoperability and maintain databases in support of these efforts; unfortunately, these databases are not compatible or are stored behind secure firewalls.

> The NATO Standardization Agency (NSA) administers the NATO Standardization Program (NSP), a classified database that prioritizes Alliance standardization requirements as a result of the Force Planning process to achieve interoperability. Force planning aims to promote the availability of national forces and capabilities for the full range of Allied missions. Additionally, NATO terminology is stored and managed by means of the NATO Terminology Database, which contains more than ten thousand definitions of NATO terms, helping to promote common understanding. Standardization Agreements and Allied Publications promulgated by the NSA are essential for the Tactical Evaluation programme of the Supreme Allied Commander Europe (SACEUR). The programme provides SACEUR with a statement describing a unit's capability to execute its assigned mission. Furthermore, NSA-supported standards are needed to certify units that are selected to become part of the NATO Response Force.[36]

The NATO Standardization Program is not a network easily accessed by US military members at the tactical and operational level. The ABCA database is available on the public internet after individual access to the site is requested and granted by the site administrator. However, these two sites are not compatible and are not linked. The information gained through interoperability exercises or experiments not associated with NATO or ABCA is not centrally stored, and locally filed in after action reports, if captured at all.

As outlined, there are many challenges to achieving interoperability with allies and coalition partners. Never-the-less, the legitimacy and effects gained by using the military element of national power through alliance and coalition efforts clearly justifies an investment in, and pursuit of, interoperability with likeminded nations. Additionally, in the current environment of budgetary constraints on militaries worldwide, an investment

in interoperability can produce significant savings by burden sharing among the US and its allies. For example,

> The Network Centric Operations Industry Consortium (NCOIC) pegs the 2010 value of the U.S. aerospace, defense, transportation and security markets at more than $600 billion. It also estimates that 30 percent of this money—about $180 billion per year—is spent to fix systems that cannot interoperate today. In an increasingly constrained budget environment that means $180 billion is spent on systems that cannot enable warfighters and end users to share information seamlessly. If the United States addresses and eliminates interoperability issues, that's a $180 billion windfall that can be shifted away from patches and interoperability fixes and redirected to budget shortfalls or securing increased capabilities for warfighters, peacekeepers, air traffic controllers and other essential end users.[37]

However, as with all things revolving around security and protection of national interests, there must also be an element of caution, so that in pursuit of interoperability strategic advantages in technology and information/intelligence are not lost or sacrificed unnecessarily or without *quid pro quo* benefits.

<div align="center">Recommended Future Approach to Interoperability</div>

The United States' national security apparatus, to include the Department of Defense, clearly does see value in interoperability and its ability to conserve resources and assist in building partner capacity. Significant energy and resources are invested annually in interoperability activities, with European Command and NATO clearly at the forefront. The USA American, British, Canadian, Australian, and New Zealand Armies' Program (ABCA) is refocused and rising as a positive protagonist in the interoperability arena. ABCA is not distinctly aligned with any combatant command, but would most closely fit with Pacific Command. Despite these bright points, the Department of Defense and the Joint Staff's current approach is relatively passive, stove piped, and dominated by a bureaucracy of boards, committees, working groups, and councils. The

results of current efforts are either captured locally, or are compiled and stored in separate, non-compatible databases which are not easily accessed by the organizations which could benefit from the information. Interoperability initiatives currently lack clear objectives, a prioritization process (NATO excepted), and metrics to assess progress and status. In the current resource constrained environment, this approach is not an effective use of national resources and warrants a comprehensive review. The Department of Defense must revisit how to best employ resources in pursuit of interoperability using a business case approach; where return on investment would become the primary metric to determine where and when to employ resources.

Because of its dynamic state, interoperability is inherently an open ended requirement where demands will always exceed available resources. The US first needs to recognize the different echelons employing interoperability, and then take a tiered approach to investing in interoperability efforts. Second, combatant commanders should play a much deeper role in establishing priorities and determining what activities are pursued and with whom they are conducted. The following is a set of recommendations for each echelon of operations:

1. Strategic Level: The focus is on prioritizing resources to ensure interoperability efforts assist in facilitating the desired national political ends, and assigning ownership of interoperability initiatives in order ensure resources are targeted at nations which are in harmony with US national interests. Nations that are willing to actively participate in military alliances or coalitions supporting the US national security and military strategies.

a. Institute an interoperability policy based on the Nixon Doctrine where defense cooperation and interoperability efforts with allies and friendly nations have primacy. This is not to say interested friendly nations would be refused requests to conduct interoperability exercises or experiments with US military forces. Rather the US would use a scaled approach where the most risky (technology sharing) and resource intensive interoperability efforts are conducted with established allies and harmonized friendly nations; while the lowest risk and least resource intensive activities are conducted with lesser harmonized friendly nations on the periphery of US interests.[38]

b. Pursue defense industrial base cooperation and equipment interoperability with US allies and friendly nations taking the layered onion approach – the closer the alignment of national interests and economic interdependence, the deeper the cooperation. Pursue common funding of weapons systems development where dual-use technology levels are low.

c. Transition to an integrated team approach to interoperability, making singular directors or commanders responsible for planning, executing, collecting data, assessing progress/status, and institutionalizing interoperability activities. This approach will develop ownership and tracking mechanisms to assess return on investments, while still retaining CJCS oversight of the Department of Defense's rationalization, standardization, and interoperability efforts. Specifically:

1) Assign the Under Secretary of Defense for Acquisition, Technology, and Logistics responsibility for the technical dimension of interoperability. Specifically within the purview of research and development, all materiel acquisitions, interoperability certifications, standardization agreements, and defense industry cooperation. Expand the Joint Interoperability Testing Center, and make this organization responsible for interoperability certification for all Department of Defense acquisition programs.

2) Assign Combatant Commanders responsibility for the doctrinal and human dimensions of interoperability; responsible for assessing the state of interoperability within their commands, identifying key interoperability gaps, and then prioritizing efforts to close the gaps. This responsibility would include the special operations arena and operational and tactical command and control, intelligence, surveillance, and reconnaissance. Expand the role of the regional Security Cooperation Office from a promotional role to that of a primary staff officer responsible for oversight and reporting of combatant command interoperability programs.

3) Assign Cyber Command responsibility for interoperability efforts in cyber the domain.

4) Assign Strategic Command responsibility for interoperability efforts in space operations, information operations, missile defense, global command and control, intelligence, surveillance, and

reconnaissance, global strike and strategic deterrence, and
combating weapons of mass destruction.

d. Pursue international standards specific to the defense industry sector just
as the International Standards Organization does for commercial industry.
Use the Arms Export Control Act as leverage to influence industry to
cooperate with this initiative, where no cooperation equals no export
allowances. If nations develop organic weapons systems vice partnership
cooperation, focus interoperability efforts on compatibility of input/output
points of contact, versus the complete interoperability of the systems
themselves (interoperability following the 'lowest common denominator'
principle).

e. Move all interoperability databases for the US and its closest allies onto
the developing Global Information Grid as soon as feasible, and assign
responsibility for management and maintenance of this database to the
Defense Security Cooperation Agency.

f. Require the Under Secretary of Defense for Acquisition, Technology, and
Logistics and Combatant Commanders to report annually to the CJCS on
the status of interoperability efforts and results achieved based on return
on investment metrics.

g. The Joint Staff develop a menu for the US military service's contracting
commands dictating rules of engagement, use for force criteria, and
C4ISR equipment standards for defense contractors supporting tactical

operations. Additionally, standardize doctrine and integration procedures for contractors supporting US tactical military units.

Risks and Roadblocks: The primary risk associated with these recommendations is organizational culture and resistance to change; a desire to retain the status quo. The recommended changes may also instigate outright protests from friendly nations who feel slighted by being labeled or considered a lower priority second class nation. Defense contractors may also resort to direct lobbying to congress because they believe it is not in their best interests to adhere to common standards or share technology in the name of improving interoperability. In response, the Department of Defense could enact these measures through an effective change management model, supported by an information operation and public debate in order to onboard internal and external stakeholders. Basing the message on using the fiscally constrained environment as the primary justification for these changes. The message should make clear that if interoperability is made more efficient there will be less waste and the potential to do more with the funds that are available.

2. Operational Level: The focus at the operational level is on shifting primary ownership of interoperability to the combatant commanders. It also involves partial re-missioning of force structure available to the combatant commander in support of interoperability efforts, and expanding the role of the combatant command staff.

a. Assign Combatant Commanders greater responsibility for prioritization and oversight of standardization/interoperability organizations affecting their command. Specifically make European Command responsible for US participation in the NATO Standardization Agency, and Pacific Command responsible for US participation in the ABCA.

b. Direct geographic combatant commanders to incorporate interoperability events in the mil-to-mil program using funds available through the Traditional Combatant Commander's Activities account.

c. Direct combatant commanders to include a separate entry, specific to interoperability, in the Intermediate Military Objectives document; supported by lines of activity, as a means to establish goals, track progress, and request resources.

d. Use exercises employing Regionally Aligned Forces (RAF) to find and resolve gaps in interoperability with key partners in the region. Employ supporting standardization/interoperability organizations to develop and document solutions with key regional partners. Integrate RAFs into Coalition Warrior Interoperability Demonstrations. Where applicable, also incorporate interoperability into the US Army National Guard State Partnership Program activities in order to leverage existing and funded opportunities.

e. In conjunction with the acquisition community, place a priority on employing and testing the concept of "open architecture" as an all-encompassing approach to interoperability of C4ISR platforms. Open

architecture allows computers and digital systems to accept/translate

output from other systems, while using firewalls to screen content.

f. Champion standardization of supply chain management among allies and

friendly nations within the combatant command. These efforts facilitate

economy of force, and reduce competition for critical logistics

infrastructure during operations. Specific to NATO, an efficient supply

chain also reinforces efforts to have US and NATO allies look at logistics

as a collective responsibility vice a national responsibility.[39]

Risks and Roadblocks: As at the strategic level, there is risk associated with

resistance to change, and a desire to retain the status quo. However, the

primary risk/roadblock is likely pushback from the combatant commanders

who may feel they do not have the staff resources to implement many of the

recommendations and the increased emphasis on interoperability. Lack of

manpower is a valid concern, and the US military services should review if

manpower in the staffs losing levels of responsibility can be shifted to the

combatant commands in order to assume the additional responsibilities.

Never-the-less, many of the recommendations include capitalizing off of

existing events and unit resources to achieve the desired ends.

3. Tactical Level: No change; continue current efforts. Tactical level units will

remain the human interface/point of contact with allies and friendly nations to

build trust, identify gaps in interoperability, and develop techniques and

procedures that foster interoperability. However, tactical units must focus on

ensuring knowledge gains are documented and provided to the combatant

command staff for further dissemination and entry into global databases.

Conclusion

General Dempsey recently commented that the interoperability of US Forces and

South Korean military was second only to NATO, but he also commented 'there is

always room for improvement'.[40] This comment demonstrates succinctly the issue of

interoperability – the work is never done, and it is a complex multidimensional issue

which has a tremendous breadth and depth of application. However, the lack of a

common understanding of the term and the complexity of the scope often cause

sometimes unjustified perceptions that progress is fleeting. Often a defense program or

interoperability event is viewed as both a success and failure depending upon the point

of observation.

Interoperability is an extension of the political relationships between nations and

their national interests. In order to ensure the resources expended towards

interoperability are achieving the political ends and serving the national interests our

national leaders have defined, the Department of Defense must transform its approach.

The Department must take an integrated team approach to interoperability in order to

achieve the best results with the limited resources available. The future approach must

also empower combatant commanders to play a much larger role in prioritizing and

directing interoperability initiatives within the doctrinal and human dimensions of

interoperability.

Lastly, instead of being all things to all services and all free industrialized nations,

the Department of Defense needs to prioritize it efforts on the US military services' joint

operations, and with key allies where the US has strong established alliances in place.

The same applies to the materiel and communication fields, where interoperability

efforts should focus on establishing minimum baselines for commonality of equipment

and basic platforms, standardized point to point connections between systems, and an

open architecture for sharing data. Through these initiatives the US and allied nations

can overcome interoperability challenges by better defining the scope of interoperability,

better defining objectives and metrics, and ensuring the best use of existing resources

to counter the dynamics of ongoing military transformation and succeed in alliance and

coalition operations which support US national interests.

Endnotes

[1] Office of the Under Secretary of Defense (Acquisition and Technology), *DoD Integrated Product and Process Development Handbook* (Washington, DC: U.S. Department of Defense, August 1998), 2.

[2] Jason Wiseman, "NATO Interoperability and New Capabilities," *Atlantic Voices* 3, no. 2 (February 2013).

[3] Barack Obama, *National Security Strategy* (Washington, DC: U.S. Department of Defense, May 2010), 31, 41.

[4] NATO Topics Web Page, http://www.nato.int/cps/en/natolive/topics_84112.htm (accessed December 30, 2013).

[5] "Interoperability was coined by the information technology (IT) world in an attempt to define an ideal way for computers and other electronic devices to relate to each other." https://www.ncoic.org/technology/what_is_interoperability/ (accessed November 15, 2013).

[6] U.S. Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States*, Joint Publication 1 (Washington, DC: U.S. Joint Chiefs of Staff, March 25, 2013), II-13.

[7] U.S. Department of Defense, Defense Acquisition University, *Glossary of Defense Acquisition Acronyms & Terms*, 15th ed. (Fort Belvoir, VA: Defense Acquisition University, December 2012).

[8] U.S. Joint Chiefs of Staff, *Multinational Operations*, Joint Publication 3-16 (Washington, DC: U.S. Joint Chiefs of Staff, July 16, 2013), I-7.

[9] North Atlantic Treaty Organization Interoperability Topics Web Page, http://www.nato.int/cps/en/natolive/topics_84112.htm (accessed December 30, 2013). Also see U.S. Joint Chiefs of Staff, Joint Publication 1, II-13.

10 U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010 (As Amended Through 15 November 2013)), 136.

11 U.S.-CREST web site, at http://www.uscrest.org/CMO.ht,

12 Chairmen of the Joint Chiefs of Staff Instruction (CJCSI) 2700.01E, *International Military Agreements For Rationalization, Standardization, And Interoperability (RSI) Between The United States, Its Allies, And Other Friendly Nations* (Washington, DC: U.S. Joint Chiefs of Staff, January 18, 2012), A-1.

13 North Atlantic Treaty Organization web page, http://www.nato.int/cps/en/natolive/topics_52092.htm (accessed February 21, 2014).

14 Robotic Systems, Joint Project Office, *UGV Interoperability Profile (IOP) Capabilities Plan For Version 0* (Warren, MI: U.S. Army TARDEC, March 11, 2011).

15 Tadjdeh Yasmin, "Army Seeks Robots That Are Interoperable with Allies," *National Defense Magazine O*nline, September, 2013, http://www.nationaldefensemagazine.org/archive/2013/September/Pages/ArmySeeksRobotsThatAreInteroperableWithAllies.aspx (accessed January 17, 2014).

16 United States Government Accountability Office, *Unmanned Aircraft Systems DOD Needs to More Effectively Promote Interoperability and Improve Performance Assessments* (Washington, DC: US Government Printing Office, 2005), 22.

17 Elizabeth Quintana, Joanne Mackowski, and Adam Smith, *Cross-Domain Operations and Interoperability*, Occasional Paper (London: Royal United Services Institute, July 2012), 11.

18 Ibid., 12.

19 Ian Wing Lieutenant Colonel, "Private Military Companies and Military Operations," Land Warfare Studies Centre, Working paper 138 (October 2010): 35.

20 CJCSI 2700.01E, International Military Agreements For RSI, B-2.

21 Under Secretary of Defense for Acquisition, Technology, and Logistics, *Defense Standardization Program,* Department of Defense Instruction 4120.24 (Washington, DC: U.S. Department of Defense, July 13, 2011)*.*

22 Ibid.

23 The Technical Cooperation Program (TTCP), *A Beginner's Guide to The Technical Cooperation Program TTCP '101'*, DOC - SEC - 01 - 2007, September 30, 2007, 6.

24 Richard L. Armitage, Joseph S. Nye, "The U.S.-Japan Alliance Anchoring Stability In Asia," A Report of the Center for Strategic and International Studies (CSIS) Japan Chair, August 2012, 9, 11.

[25] Defense Information Systems Agency (DISA) web page, http://www.disa.mil/About/OurOrganization-Structure/JITC (accessed January 15, 2014).

[26] IT Economics Corporation web page, "Integrated Project Teams," http://iteconcorp.com/IPT.html (accessed February 23, 2014).

[27] Military Doctrine Center for European Armies – Finabel, "About," http://www.finabel.org/about (accessed December 23, 2014).

[28] Pierre Claude Nolin, *Interoperability: The Need for Transatlantic Harmonisation*, (Brussels, Belgium: NATO Parliamentary Assembly, Committee Report 177 STC 06 E, 2006), I.1.

[29] Dictionary.com, "Nimby," http://dictionary.reference.com/browse/nimby (accessed February 22, 2014).

[30] U.S. Joint Chiefs of Staff, Joint Publication 3-16, I-9.

[31] Bernard Thorette, "The Need for Enhanced Interoperability," *Army* 56, no. 6 (June 2006): 34-36, 38, 40.

[32] Reliability Information Analysis Center, *System Interoperability: The RIAC Guide* (Utica, NY: Reliability Information Analysis Center, 2008), 4.

[33] Jean-Paul Darnis, et al., "Lessons learned From European Defence Equipment programs," Occasional Paper, no. 69, (October 2007): 3.

[34] Reliability Information Analysis Center, *System Interoperability,* 11-14.

[35] Ibid., 4.

[36] North Atlantic Treaty Organization web page, http://www.nato.int/cps/en/natolive/topics_69269.ht (accessed February 24, 2014).

[37] Tip Slater, "Framework Needed for NetworkI," *Defense Systems Online,* June 23, 2011, http://defensesystems.com/Articles/2011/06/08/NCOIC-View-Version-3.aspx (accessed February 22, 2014).

[38] The Official Homepage of the US Army, http://www.army.mil/article/3867/Nixon_Doctrine_and_Vietnamization/ (accessed March 6, 2014).

[39] Olivind Baekken, "Multinationality and Cooperation in Logistics," NATO's Nations and Partners for Peace, 2000.

[40] Jim Garamone, "U.S., South Korean Military Leaders Hold Talks in Seoul," *American Forces Press Service,* http://www.defense.gov/news/newsarticle.aspx?id=120878 (accessed December 31, 2013.