Information as Power

INFORMATION AS POWER

An Anthology of Selected United States Army War College Student Papers

Volume Two

Editors:

Jeffrey L. Groh, David J. Smith,
Cynthia E. Ayers, William O. Waddell

Information as Power

An Anthology of Selected United States Army War College Student Papers

Volume Two

Executive Agent for the Anthology:
United States Army War College

The views contained in this publication are those expressed by the authors and do not necessarily reflect the official policy or position of the United States Army War College, the Department of Defense, or any other Department or Agency within the U.S. Government. This publication is cleared for public release; distribution is unlimited.

This publication is available on line at http://www.carlisle.army.mil/usacsl/Studies.asp.

Cover photograph by Staff Sgt. DeNoris A. Mickle, USAF. Used by permission.

U.S. ARMY WAR COLLEGE
CARLISLE BARRACKS, PENNSYLVANIA 17013

Contents

Preface *vii*

Section 1
Information Effects in the Cognitive Dimension

Introduction 1
Professor Dennis M. Murphy

Information Operations Roadmap: One Right Turn and We're There 5
Colonel Brian J. McKiernan

Public Diplomacy: Key Enabler of America's National Security Strategy 25
Lieutenant Colonel Russell H. Smith

Strategic Communication: A Department of Defense Approach 43
Lieutenant Colonel Bart E. Stovicek

Winning the War of Perceptions: A Regional Approach to Implementing Interagency Strategic Communications 61
Colonel Matthew P. Beevers

Section 2
Information Effects in the Physical Domain

Introduction 79
Dr. Jeffrey L. Groh

Always On: Achilles Heel of the Networked Force? 85
Lieutenant Colonel Michael T. Barry

Countering State-Sponsored Cyber Attacks: Who Should Lead? 105
Mr. Levon (Rick) Anderson

Network Operations: The Role of the Geographic Commands 123
Lieutenant Colonel Peter J. Beim

Winning the Peace: Building a Strategic Level Lessons Learned Program 145
Mr. Daniel L.A. French

Notes 169

Preface

The Information in Warfare Working Group (I2WG) of the U.S. Army War College (USAWC) is pleased to present this anthology of selected student work from Academic Year 2007 representing examples of well-written and in-depth analyses on the vital subject of Information as Power. This is the second volume of an effort that began in 2006. The I2WG coordinates and recommends the design, development and integration of content and courses related to the information element of power into the curriculum to prepare students for senior leadership positions. This publication is an important component of that effort.

Interestingly, one needs to go back to the Reagan administration to find the most succinct and pointed mention of information as an element of power in formal government documents.[1] Subsequent national security documents allude to different aspects of information but without a specific strategy or definition. Still, it is generally accepted in the United States government today that information is an element of national power along with diplomatic, military and economic power…and that information is woven through the other elements since their activities will have an informational impact.[2] Given this dearth of official documentation, Drs. Dan Kuehl and Bob Nielson proffered the following definition of the information element: "use of information content and technology as strategic instruments to shape fundamental political, economic, military and cultural forces on a long-term basis to affect the global behavior of governments, supra-governmental organizations, and societies to support national security."[3] Information as power is wielded in a complex environment consisting of the physical, information, and cognitive dimensions.

Increasingly, however, the United States finds itself falling behind in its ability to wield the information element of power. And, while it certainly is a military "superpower" one has to question whether the U.S. maintains that same status with regard to information. The current information environment has leveled the playing field for not only nation states, but non-state actors, multinational corporations and

even individuals to affect strategic outcomes with minimal information infrastructure and little capital expenditure. Anyone with a camera cell phone and personal digital device with internet capability understands this. Insurgent use of information as an asymmetric strategic means has been extremely effective in the current theaters of Iraq and Afghanistan leading Richard Holbrooke to famously muse: "How can a man in a cave out-communicate the world's leading communications society?"[4]

On the other hand, the U.S. military has increasingly leveraged advances in information infrastructure and technology to gain advantages on the modern battlefield. One example from Operation Iraqi Freedom is the significant increase in situational awareness from network centric operations that enabled the military to swiftly defeat Iraqi forces in major combat operations.[5]

Clearly, managing the "message," while controlling the necessary technological "means," represents critical challenges in today's information environment. We hope that this anthology will serve not only to showcase the efforts of the College but to inform the broader body of knowledge as the Nation struggles to operate effectively within this environment and to counter an adversary who so effectively exploits it.

This publication was made possible through the outstanding efforts of several people outside of the editors and authors. The editors wish to extend their special thanks to Harry Phillips for his tireless, professional efforts in compiling and reviewing the manuscript for the anthology. Also, thanks to Gretchen Smith for the cover design, and, as always, thanks to layout editor Ritchie Dion.

Professor Dennis M. Murphy
Chair, Information in Warfare Working Group
United States Army War College

Section One

Information Effects in the Cognitive Dimension

Introduction

Dennis M. Murphy
Professor of Information in Warfare
Center for Strategic Leadership
U.S. Army War College

This section focuses on "information effects" that include those words, images and actions that ultimately influence perceptions and attitudes leading to a change in behavior. Rafal Rohozinski rightly notes that "if IO (information operations) is meant to accomplish a planned intent, then the concept of 'information effects' compels a broader analytical lens that includes the unintended consequences of both IO and kinetic actions." In short, the messages soldiers send, both through informational means and other actions, will in some way influence the receivers: adversary, friendly, and neutral; foreign and domestic. This section considers strategic communication as a way to achieve these information effects. Public Diplomacy, military Information Operations and Public Affairs are considered primary capabilities (means) of strategic communication in nascent Department of Defense literature. The papers in this section grapple with some of the issues inherent in these capabilities and the ability of the United States to use them effectively to achieve strategic objectives.

Colonel Brian J. McKiernan, earned the Armed Forces Communications-Electronics Association Writing Award for his paper "Information Operations Roadmap: One Right Turn and We're There." This work opens this section with an assessment of the Information Operations Roadmap by examining non-military applications of information technology in the Information Age, reviewing current doctrine and considering information operations during recent United States military operations. His study provides recommended adjustments to the Information Operations Roadmap based on this analysis.

Lieutenant Colonel Russell H. Smith examines the effectiveness of American public diplomacy and the implications of its success or failure on the 2006 National Security Strategy of the United States.

His paper examines public diplomacy as an enabler of foreign policy, considers public diplomacy as a strategy of engagement, and assesses the effectiveness of America's public diplomacy strategy.

Lieutenant Colonel Bart E. Stovicek argues in his paper that effective Department of Defense support to Strategic Communication can only be achieved by developing a Strategic Communication culture within the Department, and that existing capabilities must be strengthened in order to ensure strategic competitiveness and effective U.S. Government Strategic Communication during the next century.

Colonel Matthew P. Beevers highlights the current challenges, offers options, and outlines a case in point for coordinating and synchronizing the various elements of interagency external communications on a regional level while underscoring the inherent benefits of bringing the actions of those entities into alignment to advance U.S. interests abroad. Beevers uses the communications coordination group established in Afghanistan in 2003 as an example of how this concept can work.

Well-written and insightful, these papers serve to provide the military with the necessary tools to fight the long term struggle which is the Global War on Terrorism and ultimately counter the ideological support for terrorism.

Information Operations Roadmap: One Right Turn and We're There

Colonel Brian J. McKiernan
United States Army

During Donald Rumsfeld's tenure as Secretary of Defense, the Department of Defense (DoD) initiated one of the most comprehensive transformations in the history of the United States military. "The *2001 Quadrennial Defense Review* identified information operations (IO) as one of six critical operational goals that focus transformation efforts within DoD."[1] In October 2003, as a guide for achieving this goal, the DoD published the Information Operations Roadmap. Since its publication, the IO Roadmap has played a significant role in shaping how DoD, the Services and Combatant Commands organize, train, equip, plan and execute information operations. However, based on analysis of non-military applications of information technology (IT), a review of current information operations doctrine, and observations from recent military operations, it appears some adjustments to the roadmap are necessary.

The Case for Transformation

"The Administration argues that new technologies make defense transformation possible and that new threats to U.S. security make defense transformation necessary."[2] Among the new technologies profoundly impacting military operations are those in the area of IT. The Congressional Research Service report on Defense transformation says:

> *[t]he Administration's vision for defense transformation calls for shifting the U.S. military away from a reliance on massed forces, sheer quantity of firepower, military services operating in isolation from one another, and attrition-style warfare, and toward a greater reliance on joint (i.e., integrated multi-service) operations, [network centric warfare] NCW, effects-based operations (EBO), speed and agility, and precision application of fire power. Some transformation advocates characterize these*

> *changes as shifting from an industrial-age approach to war to an information-age approach.*[3]

Presumably, with a transformed military that is "better informed," more agile, and equipped with precision weapons and capabilities, an exponential increase in speed of action more than compensates for the corresponding decrease in mass. This supposes that "…a fundamental law of Newtonian physics applies also to military maneuver: one can achieve overwhelming force by substituting velocity for mass."[4] This increase in velocity relies on the U.S. military's ability to achieve information superiority over its adversaries, which Joint Publication 3-13, *Information Operations*, defines as "… an operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting the enemy's ability to do the same."[5] In large measure, the success of U.S. military transformation rests on the belief that a transformed military can gain and maintain information superiority over its adversaries.

Is the Information Age Really Upon Us?

With so much of the U.S. military transformation resting on the ability to gain and maintain a significant advantage through the application of new technologies, particularly information technologies, it is important to determine if this underlying assumption has merit. In their book, *War and Anti-War, Survival at the Dawn of the 21st Century*, renowned futurists, Alvin and Heidi Toffler assert that "throughout history the way men and women make war has reflected the way they work."[6] The Tofflers' model for the evolution of societies uses the analogy of "waves" to describe the major shifts in civilizations throughout history. Their model includes three waves with the first being the Agrarian Age. They maintain that the Second Wave, known as the Industrial Age, is currently giving way to the Third Wave, or the Information Age.

The Tofflers' also observe that societies from each wave exist simultaneously in today's world, and those reflecting the qualities of the later waves tend to dominate societies from earlier waves. This, along with the Toffler's assertion that the manner in which societies build wealth influences how they make war, means the United States should

enjoy distinct advantages over most nations based on its integration of information and information technology in both disciplines. Accepting the Tofflers' views, it seems the Administration's rationale for transformation of the military is on solid ground.

Creating Wealth the "Wal-Mart Way"

The Tofflers explain one of the main distinctions between Second Wave and Third Wave economies this way.

> *While land, labor, raw materials, and capital were the main "factors of production" in the Second Wave economy of the past, knowledge – broadly defined here to include data, information, images, symbols, culture, ideology, and values – is the central resource of the Third Wave economy.*[7]

Considering the Tofflers' view that the way man wages war largely reflects how he creates wealth, an examination of the largest retail company in the world should reveal some useful insights into how the United States might alter how it wages war in the Information Age.

Thomas Friedman's discussion of Wal-Mart's "supply-chaining" in his book, *The World is Flat: A Brief History of the Twenty-First Century*, details how this small variety store chain became the world's largest retailer through the aggressive and innovative use of IT to gain an "information advantage" over its competitors. "By investing early and heavily in cutting-edge technology to identify and track sales on the individual item level, the Bentonville Ark[ansas]-based retail giant made its IT infrastructure a key competitive advantage that has been studied and copied by companies around the world."[8]

Can a Third Wave Military Gain Similar Advantages?

According to the Tofflers, "…a revolution is occurring that places knowledge, in various forms, at the core of military power. In both production and destruction, knowledge reduces the requirement for other inputs."[9] An examination of the DoD transformation confirms the general trend toward "reduced input" based on increased "knowledge." The most obvious and sweeping reduction is found in the U.S. Army. Army transformation replaces the large World War II-style Division with the smaller, more agile Brigade Combat Team (BCT) as the basic

warfighting organizational element. According to the Operational and Organizational Plan, the Future Combat System (FCS)-equipped BCT

> *…has the wherewithal to develop the situation before, during, and after contact, affording leaders and Soldiers unprecedented situational dominance with revolutionary competencies and capabilities. The BCT operates within a new tactical paradigm based upon the Quality of Firsts—the Ability to See First, Understand First, Act First, and Finish Decisively.*[10]

Similarly, Army transformation increases emphasis on Special Operations Forces, which will grow by 14,000 personnel and add four battalions to Army Special Forces. The programmed growth in Special Forces is another example of the trend away from mass, attrition-style warfare of the Industrial Age toward reliance on "reduced inputs" in the Information Age.

Similar trends are noticeable in other Services as well. The development of improved sensors, precision guided munitions, and low-observable technology enabled the U.S. Air Force to significantly reduce the number of aircraft and the number of munitions required to destroy tactical and strategic targets. All three of these technological advances provide advantages based on dramatically improved employment of information. Improved sensors provide unprecedented *fidelity of information* concerning the target; precision guided munitions enable unprecedented accuracy by *providing information* directly to the ordnance thereby allowing it to adjust its course; and low-observable technology provides enhanced protection by *denying information* to the enemy about the location of aircraft.

This migration from large inputs to reduced inputs is not merely a matter of new technologies improving the effectiveness of existing weapons and systems. The real driver is technological advances that dramatically increase the quantity and quality of available *information*, help transform this information into *knowledge*, and through network centric operations rapidly share it vertically and horizontally across the force. In his book, *The Principles of War for the Information Age*, military theorist, Robert Leonhard points out that "[c]urrent military doctrine

is 'estimate-based.'"[11] That is to say, "[w]e are fundamentally ignorant of the enemy's whereabouts and intentions, and so we *estimate* the future."[12] During planning, staff officers prepare operations estimates, intelligence estimates, logistics estimates, personnel estimates, and various other estimates to inform the commander of the location and status of friendly and enemy forces. During execution, staffs use situation reports to update these estimates. With the proliferation of tactical internet, satellite communications, global positioning systems, and other technologies, the timeliness and fidelity of information concerning enemy and friendly forces has improved dramatically. When a military force with such capabilities is "networked" to the degree of Wal-Mart's business model, warfare approaches a point where Clausewitz's "fog of war" begins to dissipate. In this environment, militaries move away from estimate-based operations toward knowledge-based operations.

Based on its technological superiority, the U.S. military enjoys a significant advantage over most adversaries that choose to fight symmetrically. However, as the Toffler's observe, societies from all three "waves" exist simultaneously. Therefore, the U.S. military must be prepared to face adversaries that choose to fight asymmetrically. In his book, *Three Cups of Tea*: *One Man's Mission to Fight Terrorism and Build Nations…One School at a Time*, Greg Mortenson, the Director of the Central Asia Institute, described an encounter with suspected Taliban operatives equipped with high-powered binoculars and a satellite phone on an international flight from Afghanistan.

> *Down there in the dark…was the most technologically sophisticated navy strike force in the world, launching fighters and cruise missiles into Afghanistan. I didn't have much sympathy for the Taliban, and I didn't have any for Al Qaeda, but I had to admit that what they were doing was brilliant. Without satellites, without an air force, with even their primitive radar knocked out, they were ingenious enough to use plain old commercial flights to keep track of the Fifth Fleet's positions. I realized that if we were counting on our military technology alone to win the war on terror, we had a lot to learn.*[13]

Even Agrarian Age societies can access and employ Information Age technologies such as cellular phones, computers, and the internet,

further complicating the task of dealing with opponents that fight asymmetrically.

Another major challenge is gaining an "…understanding of the enemy's intentions, his motivation to fight, and the strength of his will—factors that matter most in war."[14] Determining enemy intent relies heavily on non-technological means like human intelligence (HUMINT) and detailed knowledge of foreign cultures. Achieving information superiority in this environment requires a wide range of capabilities some technological and some not. The IO Roadmap addresses this requirement by emphasizing the need to enhance IO capabilities across the U.S. military.

Key Aspects of the Information Operations Roadmap

Reviewing some key elements of the IO Roadmap establishes an understanding of how the DoD envisions the U.S. military's transition from Industrial Age estimate-based operations to Information Age knowledge-based operations. The IO Roadmap participants believed there were three areas important to making IO a core military capability. First, DoD is building a network-centric force and those networks will increasingly become an operational center of gravity that must be protected.[15] Second, DoD must improve its ability to conduct psychological operations (PSYOP).[16] Third, DoD must improve network and electromagnetic attack capability.[17] The participants also believed that if DoD aggressively implements the recommendations in the Roadmap it will benefit the Department and particularly the Combatant Commanders by providing a common understanding and approach to IO, delegating more authority for IO execution to the Combatant Commanders, creating a trained and educated IO career force, providing a centralized IO planning, integration, and analysis capability in U.S. Strategic Command (USSTRATCOM), and enhancing specific IO capabilities like PSYOP, network protection, electronic and network attack, and improved command and control.[18]

Developing a Common Understanding of Information Operations

Perhaps the most important role of the Roadmap is the establishment of a single, authoritative definition and framework for IO. This is

immensely important as it forms the basis for the development of doctrine, organization, training, material, leadership and education, personnel and facilities (DOTMLPF) to support IO as a core military capability. The Roadmap recommended, and DoD later established in DOD Directive O-3600.01, the following definition of information operations.

> *The integrated employment of the core capabilities of Electronic Warfare, Computer Network Operations, Psychological Operations, Military Deception and Operations Security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making while protecting our own.*[19]

As defined, the purpose of IO is to affect *adversary* decisionmaking in some manner while protecting one's own.

The Roadmap also provides a basic framework for the concept of IO. This framework establishes three broad functions of IO; disrupting the adversary's unity of command while preserving one's own, protecting one's own plans while misdirecting the adversary's, and controlling the adversary's communications and networks while protecting one's own. The framework further describes IO in terms of five core capabilities; electronic warfare (EW), psychological operations (PSYOP), operational security (OPSEC), military deception (MILDEC), and computer network operations (CNO). Finally, the Roadmap identifies supporting capabilities such as; physical security, information assurance, and counterintelligence, and related activities such as; public affairs and civil military operations, that must be closely coordinated with and integrated to achieve effective information operations. The U.S. military has several years of experience in both conventional and asymmetric conflicts since adopting this definition and framework and it appears they might benefit from further refinement.

Enhancing IO Capabilities

In light of the U.S. military's increased reliance on computer networks, the IO Roadmap places appropriate emphasis on the enhancement of CNO capabilities. Additionally, the proliferation of computers and computer networks means that both conventional

militaries and asymmetric opponents, such as insurgents and terrorists, may use both public and private computer networks to support their operations. In this environment, the U.S. military's ability to achieve information superiority over adversaries relies heavily on its ability to protect its networks through computer network defense (CND) and also to attack an adversaries computer networks through computer network attack (CNA).

Electronic Warfare (EW), another IO core capability, is essential to achieving information superiority in the contemporary operating environment. The Roadmap states that EW remains too focused on defensive activities such as electronic protection (EP) and suppression of enemy air defenses (SEAD). DoD's vision for EW is to develop a more robust offensive EW capability that will "…deny adversary situational awareness, disrupt command and control, and develop targeting solutions to defeat weapons while protecting [one's own] against the same."[20] This enhanced capability will be critical across the entire range of military operations from stability, security, transition, and reconstruction (SSTR) operations, to counterinsurgency, and major combat operations.

The Roadmap also recommends that DoD enhance and refocus PSYOP capability. This recommendation was based on the assessment that PSYOP forces lacked the ability to rapidly develop and disseminate high quality products targeted at diverse audiences, sufficient numbers of fully qualified and equipped personnel with diverse linguistic capability, and the ability to disseminate PSYOP products in denied areas. Recent experience in Operation Iraqi Freedom confirms that these capabilities are some of the most important for effective IO. DoD's goal is to create " [a] PSYOP force ready to conduct sophisticated target-audience analysis and modify behavior with multi-media PSYOP campaigns featuring commercial-quality products that can be rapidly disseminated throughout the Combatant Commander's area of operations."[21]

Trained and Ready IO Career Force

A major challenge in moving IO from concept to capability is the development of a trained career force. The Roadmap participants

assessed that the five core capabilities were not well understood across the Services. Further complicating matters, each Service tended to train their specialists based on Service-specific requirements each emphasizing elements that had the most impact in their particular medium. Developing a trained and educated IO career force is also difficult because of the growing complexity and rapid technological changes in specialty areas such as EW, PSYOP, and CNO.

The solution described in the Roadmap includes the development of a core cadre of professionals capable of planning and executing fully integrated IO. This cadre will consist of IO planners that come from the mainstream of each Service and IO specialists who are functional experts in one or more of the core IO capabilities; EW, CNO, or PSYOP. IO planners would serve in assignments that alternate between their basic branch and IO planning positions. Similarly, IO specialists would serve in assignments that alternate between their specialty areas and general IO planning positions.

Developing a robust training and education program for IO is another critical requirement for creating a trained and ready IO career field. The Roadmap asserts that programs of instruction for joint IO planners and specialists must be standardized. The Roadmap also emphasizes the need to develop a greater appreciation for IO in the general military population. This would be accomplished by standardizing the IO curriculum at intermediate level education (ILE) for majors, and at senior service college (SSC) for lieutenant colonels and colonels. The Roadmap also calls for DoD to coordinate across the Service schools to integrate IO training into early military education as well.

These concepts and recommendations made in the IO Roadmap establish a solid foundation for the process of moving IO from idea to operational capability. The U.S. military transformation is well underway, and developing IO as a core military capability continues to gain momentum. There seems to be little debate whether or not the U.S. military should pursue IO as a core capability. However, there is still much debate among the Services, in the classrooms at Service colleges, and at military training centers about how best to plan and integrate IO into military operations. An examination of IO in some

recent military operations provides some insight into U.S. military successes and challenges and leads to some recommended adjustments to the IO Roadmap.

Information Superiority in Recent Military Operations

"Information Warfare" in Operation Desert Storm

The term information operations had not been coined when the United States led a coalition in the 1991 war to eject Iraqi forces from Kuwait. Even so, coalition forces under command of General Norman Schwarzkopf, developed a campaign plan that foreshadowed current information operations doctrinal concepts. Key components of the strategy to defeat the Iraqi forces in Kuwait and restore Kuwaiti sovereignty relied on integrating four of the five core capabilities of today's IO; OPSEC, MILDEC, PSYOP, and EW.

Coalition success relied on OPSEC of the grandest scale. Essential to a successful flanking attack, the coalition surreptitiously moved the entire XVIIIth Airborne Corps from the vicinity of Dhahran, Saudi Arabia, to tactical assembly areas hundreds of miles to the west just prior to initiating ground combat operations. Another key element of Schwarzkopf's operational design were deception operations aimed at tying Iraqi forces to the defense of areas not essential to coalition success. Schwarzkopf positioned the 82nd Airborne Division near major airfields and retained the 4th and 5th Marine Expeditionary Brigades (MEB) afloat in the Persian Gulf to convince the Iraqi leadership there was a threat of both an airborne operation and an amphibious assault. Coalition forces also employed large scale PSYOP coupled with B-52 strikes on frontline units to undermine the will of individual soldiers and whole units to fight. Disruption of enemy command, control, communications, intelligence, surveillance, and reconnaissance (C4ISR) was also essential to gaining an informational advantage over the enemy. Upon gaining air superiority, coalition Air Forces, relying heavily on EW capabilities, systematically attacked key command and control (C2) nodes and infrastructure to degrade Iraqi leaders' ability to "see" what was in front of their forces; make decisions about the orientation of their forces; and command and control of the withdrawal of those forces once the decision was made to quit Kuwait.

Using improved intelligence, surveillance, and reconnaissance (ISR) capabilities like the Joint Surveillance Target Attack and Radar System (JSTARS), space-based systems, precision guided weapons, and low-observable technology, coalition forces attacked throughout the depth of the Theater of Operations to isolate, and then defeat the Iraqi forces in Kuwait and Southern Iraq. Coalition forces attained their military objectives and created the conditions required for terminating major combat after thirty-seven days of air combat operations and only one hundred hours of ground combat. This remarkable victory was achieved at a much smaller cost in manpower and material than experts predicted largely due to the coalition's ability to "blind" the enemy while maintaining its own ability to see the enemy and the environment. However, even though coalition forces enjoyed information superiority and used it to great advantage, the U.S. military had not yet parted with the Industrial Age approach of massive forces using "attrition-style warfare."

Information Operations in Operation Iraqi Freedom

As the prospect of a new war against Iraq grew throughout the early months of 2003, many "military analysts" were astonished that the United States was prepared to initiate war with Iraq, and "regime removal" was its military objective. More surprising was the prospect of achieving this much broader objective with only a fraction of the forces used to eject Iraqi forces from Kuwait in 1991. Many wondered if the degradation of Iraqi military capability through a decade of sanctions was sufficient to make such a ratio feasible. Actually, a combination of the degradation of Iraqi military strength, coupled with the U.S military's improved ability to gain information superiority based on advances in information technology, made this plausible.

The Coalition's advantages in sensors, precision guided weapons, and improved command and control systems like tactical internet, global positioning systems, and satellite communications, provided unprecedented information superiority over the adversary in a conventional fight. Increased certainty about the location, disposition, and status of both one's own forces as well as the enemy's gave commanders greater confidence in directing the actions of their forces and resulted in a dramatic increase in the tempo of operations. With

only 183,000 ground forces at the outset of Operation Iraqi Freedom (OIF), a fraction of the forces available at the start of Desert Storm, the Coalition penetrated two hundred and fifty miles into enemy territory. In less than three weeks, a bold Coalition offensive reached the enemy capital, toppled the regime, and achieved the initial military objectives of the campaign. As Leonhard predicted, "knowledge-based" operations dramatically changed the way the U.S. military waged war and resulted in a significant increase in the tempo of operations. Similarly, the Toffler's predicted "reduction of inputs to destruction" in warfare was realized in OIF.

However, with the Iraqi military defeated and Saddam removed from power, the operational environment changed dramatically. The center of gravity in this new environment shifted from Saddam and his regime to the country's population. The Coalition's considerable advantages in major combat operations seemed to carry less significance in this new conflict where a stubborn insurgency had taken root. In this conflict, the range of activities Coalition forces engage in, and the manner in which they apply military resources, changed drastically. The nature of the information required to accomplish its tasks differs from the information required to conduct operations against a conventional military force. Still, gathering that information and gaining information superiority over the adversary remain central to success. However, this superiority rests not on the ability to "see enemy formations" over the next ridge but to understand where, when, and how the adversary will attempt to influence the population to support their cause rather than that of the Iraqi government and the Coalition.

One U.S. Brigade Commander responsible for an area of operations in Central Baghdad at the outset of SSTR operations noted, "… I quickly discovered that IO was going to be one of the two most vital tools (along with human intelligence) I would need to be successful in a counterinsurgency (COIN) campaign."[22] However, upon examination of this commander's information operations, it is clear the primary focus of the brigade's information operations was on influencing the behavior of the neutral population rather than adversary decisionmaking. This commander describes his concept for IO in the following way:

> *Our overall target audience was clearly the silent majority. However, to reach them and to ensure that our messages and themes would resonate with them, we determined that we needed to use mainly Iraqi proxies to convey our messages. We therefore, identified five groups of Iraqis that had significant influence among the population: local imams and priests, local and district council members, staff and faculty from the universities, Arab and international media and local sheiks and tribal leaders.*[23]

Consistent with the preponderance of tactical commanders and many operational commanders in OIF, this commander views PSYOP, civil military operations, and public affairs as the central efforts of IO in COIN and SSTR operations. This highlights an inconsistency between the current definition of IO and how most commanders view it. The current definition *does not include operations intended to influence the behavior or decisionmaking of foreign neutral or friendly populations*.

Furthermore, both the current definition and the framework described in the IO Roadmap cause many to view IO as separate operations which must be synchronized and coordinated with the overall operations. In an effort to provide some theoretical underpinnings for IO, Colonel William Darley, the V Corps Public Affairs Officer during Operation Iraqi Freedom, wrote an article entitled *Clausewitz's Theory of War and Information Operations*. In it, he describes the relationship between IO and kinetic operations this way.

> *IO and kinetic operations are inseparably linked, like strands of a DNA molecule in a gene, and in the same way have a dominant/recessive relationship (for example, one exercising dominance over the other depending on where the conflict falls on the continuum relative to the polar extremes).*[24]

While this is a step in the right direction, it might be further improved by viewing IO as an integral part of all operations both kinetic and non-kinetic. Colonel Darley maintains that information operations are dominant at the lower end of a continuum of violence in "The Universe of Political Conflict" while "kinetic operations" are more dominant at the higher end of this spectrum. This is a common conclusion many make because they tend to equate IO core capabilities

and supporting activities like PSYOP and civil military operations, which have become euphemistically known as "non-kinetic" operations, with IO as a whole.

The contrast between the two I Marine Expeditionary Force (I-MEF) operations in 2004 to gain control of Fallujah, a key insurgent stronghold, provides important lessons about dominating the information environment and integrating IO into operations. The first operation, Operation Vigilant Resolve, ended almost before it began when "U.S. forces unilaterally halted combat operations after a few days due to lack of support from the Interim Iraqi Government and international pressures amid media focus on unsubstantiated enemy reports of collateral damage and excessive force."[25] According to LTG Metz, Commander of Multinational Corps Iraq (MNC-I),

> *…the operation failed because operations in the information domain were not integrated into the battle plan….Steps to prepare the information battlefield, including engaging numerous and varied Iraqi leaders, removing enemy information centers, and rapidly disseminating information from the battlefield to worldwide media were not woven into the plan.*[26]

I-MEF had all of the required resources to dominate the enemy tactically and would certainly have succeeded if they had not been forced to unilaterally cease operations. Unfortunately, they failed to properly consider the information environment and the potential impacts that failing to dominate that portion of the operational environment would have on their operations.

The outcome of I-MEF's second operation, Operation Al-Fajr, in November 2004, was significantly different. "A key task for the MNC-I planners was to ensure that the information defeat of Vigilant Resolve was not repeated in Operation Al-Fajr."[27] The success of the operation relied on OPSEC and MILDEC to conceal the build-up of forces north of Fallujah; effective PSYOP to encourage noncombatants to leave the city and insurgents to surrender; and electronic warfare to control the enemy's communication. Other keys to the success of the operation were the early seizure of Fallujah Hospital, the insurgent's propaganda facility, and a deliberate plan for forces to document

evidence of insurgent atrocities and quickly share the information with international media outlets. All of these actions were essential in the Coalition's effort to control the information environment and ultimately to accomplish its military objective of seizing control of Fallujah from the insurgents. Operation Al-Fajr was not really a case of IO tightly woven into the operational plan. It was more a case of planners developing a comprehensive understanding of the operational environment, particularly the informational realm, and developing a plan to effectively employ *all* available capabilities to dominate the adversary across every part of the operational environment—informational included.

This review of IO in recent military operations confirms that the U.S. military continues to progress toward making IO a core military capability. This progress actually builds on initial successes in Desert Storm even before the current concept for IO was established by the IO Roadmap. Observations from Desert Storm and OIF also demonstrate that the U.S. military has and continues to improve its significant advantage in information superiority when fighting symmetric wars against conventional militaries. Observations from later stages of OIF suggest that more effort is required to achieve the same advantages when fighting asymmetric warfare during counterinsurgency or SSTR operations.

Recommended Adjustments to the Information Operations Roadmap

The IO Roadmap is a good guide for expanding the U.S. military's IO capability as a critical goal of transformation. The Roadmap places appropriate emphasis on developing a common understanding of IO across the military, enhancing key IO capabilities, and developing a trained IO career force. However, the process could be improved by making some adjustments to the Roadmap.

Developing a Common Understanding of IO

Based on observations of recent United States military operations it appears that the definition and framework require further refinement. The DoD should consider refining the definition that was

promulgated by DoD Instruction O-3600.01. The review of recent operations indicates that most of the information operations executed in COIN and SSTR are largely focused on neutral-party behavior and decisionmaking. The current definition of IO is too narrowly focused on *adversary decisionmaking* and doesn't address operations and activities that most commanders, in practice, view as critical to success in COIN and SSTR operations—influencing and affecting foreign population behavior.

The analysis of the two Fallujah operations suggests another potential improvement to the definition and the framework for IO. Currently, the term IO is used to describe the employment of several disparate capabilities (core and supporting) and related activities. The rationale for this, according to the IO Roadmap, is that "[l]ike all core competencies, information operations can not be successfully executed without diverse supporting capabilities."[28] Rather than focusing the definition on the capabilities and activities associated with IO, it may be more useful to define IO in terms of the information environment.

Joint Publication 1-02 defines the information environment as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information."[29] This might lead to an alternate definition for IO such as:

> *Operations conducted in the information environment to affect foreign populations, and adversary behavior and decisionmaking processes while protecting friendly decisionmaking.*

This definition, while much broader, focuses on the medium in which IO take place and the purpose of those operations, rather than a set of capabilities that may be employed. This change would cause commanders and staffs to view IO more as a fundamental of operational design and the information environment as a dimension of the operational environment that must be analyzed and understood in the same way as other components of the operational environment such as the political, social, economic and military systems.

This approach is consistent with the model described by LTG Metz when he highlighted the differences between the first and second battles for Fallujah in 2004. Additionally, for the United States military to

gain an advantage over its competitors similar to Wal-Mart's advantage over its competitors, it should view information in much the same way that Wal-Mart does, as the central resource in the business. "Any military—like any company or corporation—has to perform at least four key functions with respect to knowledge. It must acquire, process, distribute, and protect information, while selectively denying or distributing it to its adversaries or allies."[30]

Wal-Mart leveraged the latest innovations in information technology to reengineer their business process across every element of the organization, including marketing, sales and distribution. Fundamentally, the business units perform the same functions but in a vastly different manner, a manner that streamlines virtually every aspect of the company's core processes and functions. Similarly, using the IO Roadmap as the guide, DoD should focus the *entire* organization on information as fundamental to operations. This requires a revision of the roles, responsibilities and capabilities of the existing functional elements of the force so they best accomplish the four functions with respect to knowledge—acquire, process, distribute, and protect information.

Trained Career Force

Next to establishing a common understanding of IO, the Roadmap's second most significant contribution is building and maintaining a trained and educated IO career force. While on the surface it seems that an Information Age military has a distinct advantage over military or paramilitary forces of a first or second wave society, the differences between the Operation Vigilant Resolve and Operation Al Fajr indicate the importance of appropriate emphasis on the information component of warfare when designing and executing military operations on today's battlefield. The United States military must build a core cadre of personnel that are knowledgeable and experienced in planning and conducting integrated operations that fully consider the informational element of the operational environment and maximize the contributions of all the available resources and capabilities.

The Roadmap lays out a logical approach to this problem but DoD may need to adjust its emphasis on different aspects of this plan.

First, DoD should place the greatest emphasis on training the general military population on the analysis of the information environment and the implications for each functional element of the force. The program of instruction for every level of professional military education must include appropriate instruction on information as a fundamental of operations and how it pertains to that particular military occupational specialty. Second, the Services must enhance the proficiency and capability of what are currently called IO specialists like EW, CNA, CND, PSYOP, and other technical specialists. Third, the services should train *all* of their planners to be experts in planning operations which take all aspects of the information environment in to consideration. Integrating information operations should not be viewed as a "mystical task" whose secrets can only be carried out by an "IO wizard." Every commander, chief of operations, and chief of plans at every level must be completely conversant and adept at integrating information operations into the plans and operations.

This is somewhat different from the current approach of establishing a separate career force of IO personnel that are responsible for planning and integrating IO into operations. The U.S military must not allow IO to become a "sideshow" rather than an essential part of the "main event." This will likely happen if Combatant Commanders and Joint Force Commanders maintain the approach of integrating the information component into operations by first separating out something that is fundamental to operations and crosses every functional element of warfighting. This separation of an integral element of operations is accentuated when the services create a separate career force with functional responsibility for integrating a core capability into operations.

Improve PSYOP Capability

While it seems the U.S. military is far down the path in gaining a sustainable technical advantage over its adversaries which results in information superiority in conventional warfare, it does not appear the same is true for COIN and SSTR operations. The IO Roadmap identifies the requirement to improve the PSYOP capability in the U.S. military. Recent experience in OIF indicates that PSYOP are extremely important in COIN and SSTR operations thus confirming

this requirement. This capability is not well understood by the general military population. There is also a pervasive perception across the conventional force that IO is nothing more than the coordinated application of PSYOP, CMO, and PA. DoD should develop a program to educate the force on the proper integration of PSYOP into operations and clarify its role. All military planners, not just a special subset called IO planners, must understand the organization, capability, and principles of employment of PSYOP forces

Conclusion

Overall, the IO Roadmap serves a very important purpose throughout DoD. The Roadmap provides a forcing function for leaders in every Service to move the process of transformation forward with respect to warfare in the Information Age. It correctly recognizes the increased advantage a military force gains over the adversary through the ability to "see first," "decide first," "act first," and "act more effectively." This advantage is equally important throughout the entire range of military operations from SSTR to major combat operations. The difference lies in the kind of information required, the methods and capabilities used to collect that information, and methods and capabilities used to affect decisionmaking and behavior.

The Roadmap forces the Services to move beyond concepts and experimentation to developing policy, doctrine, tactics, techniques, and procedures for integrating information and advances in information technology into military operations. There remains a wide range of opinions and understandings of what constitute information operations and how they should be integrated into operations. DoD should continue its emphasis on information superiority and the establishment of common understanding of IO across the DoD if the United States is to remain peerless in its ability to project and successfully employ the military as an element of national power far into the 21st Century. However, it should consider some adjustments to the Roadmap in order for the United States military to successfully integrate the information component in operations and garner a significant and lasting advantage over its potential adversaries.

Public Diplomacy: Key Enabler of America's National Security Strategy

Lieutenant Colonel Russell H. Smith
United States Marine Corps

The 2006 National Security Strategy (NSS) of the United States of America charts a path for leadership for America.[1] A key aspect of leadership is the ability to influence others to subordinate their own interests in favor of the interests of a collective entity or a nobler set of ideals. The two foundational pillars of the 2006 NSS—promote freedom, justice, and democracy, and lead a growing community of democracies in the quest to solve the complex problems of today's world—require the United States (U.S.) to align with other countries around the globe in pursuit of common policy objectives. However, virulent anti-Americanism and a growing resentment of U.S. foreign policy is eroding America's influence around the world. Even the leaders of some traditional American allies have found it convenient and politically advantageous to disparage America.[2]

The terrorist attacks of September 11, 2001 clearly demonstrated to the U.S. that anti-American sentiment abroad can have real and disastrous consequences at home as well as overseas. Public opinion surveys by the Pew Research Center have exhaustively documented the precipitous decline in favorable views and trust of the United States across large swathes of the globe.[3] The problem of growing anti-Americanism is especially acute in the Middle East and among predominantly Muslim populations. Gallup polls in December 2001 and January 2002—only months after the 9/11 terrorist attacks, and arguably a period when international public opinion was overwhelmingly supportive of the United States—highlight the depth and breadth of the animus. By an average of two to one, poll respondents in nine Muslim countries reported an unfavorable view of the United States.[4] Other polls in the summer of 2002, May 2003, and March 2004 reported similar results and according to Pew, foreign publics' opinions of America appear to be steadily declining.[5] Failure to reverse this trend of widespread

anti-Americanism will undermine America's ability to achieve critical foreign policy and national security objectives and portends failure for successful implementation of America's National Security Strategy.

Public diplomacy seeks to promote the national interest of the United States through understanding, informing and influencing foreign audiences in order to influence the behavior of foreign governments.[6] Ongoing debate on U.S. public diplomacy convincingly argues that current efforts are ineffective and in need of significant overhaul. This paper examines U.S. public diplomacy and the implications of its success or failure on the 2006 NSS. The examination includes a discussion of public diplomacy as an enabler of foreign policy; a look at public diplomacy as a strategy of engagement; an assessment of the effectiveness of America's public diplomacy strategy; and implications of ineffective public diplomacy for the success of the 2006 National Security Strategy.

Foreign Policy Enabler

> *Throughout the world, the public face of the United States generates strong opinions, positive and negative. These public attitudes directly affect our ability to achieve our foreign policy…*[7]

In the years since the 9/11 attacks, it has become clear the United States is involved in a generational and global struggle of ideas—a struggle that pits the power of hate against the power of hope.[8] Initially after the 2001 attacks, people around the world expressed shock and support for the U.S. government. As time passed, international support for U.S. policy objectives dwindled while negative attitudes about America increased and became more intense. The launching of the Iraq War in March 2003 resulted in a sharp downturn of foreign opinions of the United States—not only in the Arab and Muslim world, but even among America's closest allies.[9]

The strategic environment today is radically different than it was prior to 9/11. The United States currently faces a war on terrorism, intensified conflict within Islamic factions, and insurgency in Iraq. Global transparency, driven by new media and low cost technologies,

shape the new strategic landscape.[10] Worldwide anger and discontent are directed at America's tarnished credibility and the way it pursues its goals. America's image problem, many suggest, is linked to perceptions of the United States as arrogant, hypocritical, and self-indulgent.[11] Research conducted by Business for Diplomatic Action[12] suggests that additional causes of anti-Americanism are: a feeling of exclusion from the globalization movement led by U.S. business expansion, resentment regarding popular U.S. culture, and negative views of the behavior of individual Americans.[13]

The challenges America faces in the Global War on Terrorism (GWOT) are great and the 2006 NSS is clearly an ambitious strategy designed to address these challenges. Success in the GWOT will require sustained cooperation between the U.S. and other nations, but America's image needs a makeover if this cooperation is to be achieved.[14] The two foundational pillars of the 2006 NSS require the United States to align with other countries in the pursuit of common policy objectives. The NSS lists nine essential tasks America must undertake to successfully face the security challenges of the 21st century:

- Champion aspirations for human dignity
- Strengthen alliances to defeat global terrorism and work to prevent attacks against us and our friends
- Work with others to defuse regional conflicts
- Prevent our enemies from threatening us, our allies, and our friends with weapons of mass destruction (WMD)
- Ignite a new era of global economic growth through free markets and free trade
- Expand the circle of development by opening societies and building the infrastructure of democracy
- Develop agendas for cooperative action with other main centers of global power
- Transform America's security institutions to meet the challenges and opportunities of the 21st century
- Engage the opportunities and confront the challenges of globalization[15]

In analyzing these tasks it is clear that their achievement will depend largely on United States engagement with foreign governments and their constituencies. Cooperation, a mutually shared vision, and the implementation of a coordinated plan of action between the United States and allies around the world are required if the 2006 NSS is to succeed. The alarming trend of widespread anti-Americanism and resentment of U.S. foreign policies are growing obstacles to cooperation, coordination, and a shared vision between the United States and other nations. If not reversed, these obstacles portend failure for key aspects of the NSS.

Public diplomacy helps shape global perceptions of U.S. policies and objectives. It is a key component of foreign policy that the United States has actively employed since the early 20th century to promote its interests abroad. The overarching goal is to increase understanding of American values, policies, and initiatives and to counter anti-American sentiment and misinformation about the United States around the world.[16] If used effectively, American public diplomacy can help influence foreign governments and other international actors to support America's foreign policy and national security objectives.

Effective public diplomacy enables U.S. foreign policy because it both informs foreign audiences and promotes dialogue between America and other nations. Credible information helps dispel myths and misperceptions about America's motives and intentions. Dialogue begets the understanding, cooperation, and coordination between nations that is necessary to solve the complex challenges of the 21st century. Public diplomacy has enormous, untapped potential to positively influence the world's opinion of America's policies, objectives, culture and people. Unfortunately, ineffective or inadequate public diplomacy can undermine American foreign policy and hamstring successful implementation of the tenets of the 2006 NSS.

Strategy of Engagement

While public diplomacy has received widespread attention since the 9/11 terrorist attacks, it is not a new concept. The U.S. government first officially acknowledged its use of public diplomacy activities during World War I when President Woodrow Wilson created the Committee

on Public Information (the Creel Committee) to convince the citizenry in foreign countries of the nobility of American foreign policy goals.[17] In its early years, public diplomacy was called "propaganda." Much of what was disseminated during World War I and the inter-war years in an effort to "whip up domestic support" for foreign policy and counter foreign propaganda aimed at the United States was heavy handed and lacking in credibility.[18]

Modern public diplomacy has evolved dynamically since then, and goes far beyond the concept of how elected and appointed government officials communicate, argue, and influence policies publicly. Today, it is a concept whereby governments conduct international relations through communications media and by dealing with a wide range of nongovernmental entities for the purpose of influencing the politics and actions of other governments.[19]

Public diplomacy can perhaps be easily understood by contrasting its fundamental characteristics with that of traditional diplomacy. While both types of diplomacy attempt to influence the behavior and policies of governments, traditional diplomacy is often opaque, and generally confined to government-to-government interaction. Public diplomacy is transparent, in many cases widely disseminated, and principally aimed at foreign publics instead of their governments.[20]

During the 20th century, public diplomacy played a central role in the battles against fascism and communism. In his famous "Campaign of Truth" speech in 1950, President Harry Truman declared that the Cold War was a war of ideas, "a struggle, above all else, for the minds of men." Winning the hearts and minds of people living under communist regimes was deemed essential to achieving victory in this war of ideas, and President Truman's speech launched an aggressive public diplomacy campaign designed to undermine communist ideologies by exposing them to western ideas and values.[21]

The modern concept of public diplomacy was first developed at Tufts University's Fletcher School of Law and Diplomacy during the Cold War. Dean Edmund A. Gullion is credited with coining the term when the Edward R. Murrow Center of Public Diplomacy was

established in1965.[22] At that time, the Murrow Center's institutional brochure stated that:

> *Public diplomacy…deals with the influence of public attitudes on formation and execution of foreign policies. It encompasses dimensions of international relations beyond traditional diplomacy; the cultivation by governments of public opinion in other countries; the interaction of private groups and interests in one country with those of another; the reporting of foreign affairs and its impact on policy; communication between those whose job is communication, as between diplomats and foreign correspondents; and the processes of inter-cultural communications. Central to public diplomacy is the transnational flow of information and ideas.*[23]

The U.S. Department of State defines public diplomacy as "government sponsored programs intended to inform or influence public opinion in other countries."[24] However, this definition falls short of explaining the why of public diplomacy, which is to influence foreign policy decisions of other nations in support of U.S. foreign policy. Public diplomacy informs, for the purpose of persuading, foreign governments and publics.[25] Public diplomacy acknowledges that foreign public opinion plays a role in creating foreign policy and therefore seeks to influence these publics.[26] Former U.S. Public Affairs Officer, Hans Tuch, author of *Communicating with the World*, spoke to one aspect of the objective of public diplomacy when he defined it as, "official government efforts to shape the communications environment overseas in which American foreign policy is played out, in order to reduce the degree to which misperceptions and misunderstandings complicate relations between the U.S. and other nations."[27]

Joseph Nye, former Dean of Harvard's Kennedy School of Government, brought the definition of public diplomacy into the 21st century when he described it as "a policy expression of soft power." In his book *Soft Power*, Nye defines his work's title as the power of getting others to want the outcomes you want. Instead of resorting to threats or physical force, soft power rests on the ability to seduce people into creating certain outcomes.[28] In American politics, public diplomacy is some times mistakenly viewed as a "soft tool" of national power to be used only in times of international crisis in a kind of perception

management role. However, effective public diplomacy is not about achieving the short term goals of a particular administration, or solely for strategic crisis management, but instead takes a longer view of opening constructive dialogues between nations in order to shape the geopolitical environment.

Elements of modern public diplomacy include cultural diplomacy, corporate public diplomacy, international broadcasting, and utilization of foreign print media.[29] Public diplomacy involves not only shaping the message(s) that a country wishes to present abroad, but also analyzing and understanding the ways that the message(s) may be interpreted by diverse societies. It necessitates developing the tools of listening and conversation as well as the tools of persuasion.[30]

The U.S. government clearly recognizes that achieving its foreign policy objectives in the 21st century will increasingly rely on its ability to successfully shape the perceptions and attitudes of foreign publics. American public diplomacy is a strategy of engagement that enables foreign publics to make informed judgments about America's policies, its society, and the relationship of both to their own interests.[31]

Assessing American Public Diplomacy

American public diplomacy and the 2006 NSS must complement each other for both to succeed. Public diplomacy must effectively shape an international environment that facilitates achievement of U.S. foreign policy goals and enables its national security strategy. America's pursuit of its foreign policy goals and how it executes the tenets of the 2006 NSS must reflect and reinforce what its public diplomacy is telling the world about America. This is the essence of the relationship between public diplomacy and the NSS.

Admittedly, public diplomacy has limitations and is not the panacea for all of America's image problems. However, if employed effectively, public diplomacy has enormous potential to enable America's foreign policy and its NSS. But is America's public diplomacy effectively enabling U.S. foreign policy and shaping a geopolitical environment that will support implementation of the new NSS? In an attempt to

answer this question, this paper assesses America's public diplomacy strategy using the criteria of feasibility, acceptability and suitability.

Feasibility examines whether a strategy can be accomplished with available resources. In this 21st century global struggle of ideas, the United States must understand what it will take to convince the world to follow American leadership, and it must possess the resources to get the job done. In recent years, public diplomacy has gained a new urgency and has become the "holy grail" of American foreign policy.

Searching for a silver bullet for the dilemma of America's waning power and influence, the Bush Administration thought it found one in stepped-up public diplomacy. The premise behind this conclusion was simple enough. As Charlotte Beers, the State Department's first Under Secretary for Public Diplomacy and Public Affairs, put it in November 2001—in many countries America's message is often "distorted," "one-dimensional," or "simply not heard." If only the rest of the world enjoyed unfettered access to accurate information and independent media, they would understand the U.S. does not seek an empire, that the "war on terror" is in every civilized nation's interest, and that American values are universal. If only the United States clearly articulated its message then surely the rest of the world would jump on the American bandwagon.[32] Based on this assumption, increases in funding for public diplomacy activities[33] and quick fixes such as a State Department-coordinated series of Madison Avenue-like "brand USA" marketing campaigns[34] have been tried. Unfortunately, the solutions to America's image problem do not lay in short term manipulative public relations; and these initiatives have thus far produced no real change in foreign public opinions of America's actions and intentions on the world stage.[35]

It appears the current Administration has yet to understand that improved marketing of our message will not result in significantly reduced levels of anti-Americanism. Other countries are not buying what the U.S. is currently selling, no matter how slick or sophisticated the sales pitch. It's not the packaging that others dislike, it is the product.[36] Enduring results will depend on a fundamental transformation of the message the U.S. communicates, the consistency of that message, and

a sustained long term approach at the level of ideas, cultures, and values.[37]

In an address to the 2005 Forum on the Future of Public Diplomacy, Karen Hughes, U.S. Department of State (DoS) Under Secretary for Public Diplomacy and Public Affairs, unveiled America's current strategy for U.S. public diplomacy efforts. Key components of this strategy are:

- Offer people throughout the world a positive vision of hope and opportunity that is rooted in America's belief in freedom, justice, opportunity and respect for all.
- Isolate and marginalize the violent extremists; confront their ideology of tyranny and hate. Undermine their efforts to portray the west as in conflict with Islam by empowering mainstream voices and demonstrating respect for Muslim cultures and contributions.
- Foster a sense of common interests and common values between Americans and people of different countries, cultures and faiths throughout the world.[38]

While supposedly a "new" strategic framework to underpin and guide U.S. public diplomacy, it appears that this strategy is based on the same premise that has guided U.S. public diplomacy efforts since 9/11—the world hates us, because they don't understand us.[39] However, available evidence indicates that this new public diplomacy strategy has been relatively ineffective thus far at reversing the virulent anti-Americanism that is spreading across the globe. Sadly, it appears the problem is not that the world misunderstands America, but rather that America may not truly understand the rest of the world.

Arguably the primary resource necessary to prevail in the global war of ideas is influence. America must be able to persuade others that its policies, objectives, perspectives and values are worthy of emulation; that the American way is indeed in the best interests of the world. However, there is widespread agreement that America's image abroad needs burnishing and that America's power to persuade is in a state of crisis.[40]

In his introduction to the 2006 NSS, President George W. Bush addresses the historic dichotomy of American foreign policy that once again faces the United States: the choice between isolationism or world leadership. He equates the path of isolationism to a path of fear and looks to history to show that every time America's leaders have chosen the path of isolationism the Nation's security challenges have only increased. The path of leadership is equated to a path of confidence and one that is declared to be consistent with the great tradition of American foreign policy. In walking the path of leadership, the United States will seek to shape the world; to influence events for the better. The path of leadership rests in part on strong alliances, friendships, and international institutions that enable America to promote freedom, prosperity, and peace in common purpose with like-minded nations.[41]

In closing, the 2006 NSS states, "the challenges America faces are great, yet we have enormous power and influence to address those challenges. The times require an ambitious national security strategy.... Our national security strategy is idealistic about goals, and realistic about means."[42] The premise of this statement is that the United States has both the power and the influence necessary to implement its NSS. If this premise is flawed, then America must reassess whether or not its current strategy of public diplomacy is feasible. The 2006 NSS is an ambitious strategy, and boldly declares that America views itself as a leader among the nations of the world. Current trends would argue that maybe America is not the leader she once was, and as a result, her influence has diminished.

Acceptability determines whether the strategy is worth the cost and whether it is politically supportable. Is the Administration requesting, and is the Congress providing resources for public diplomacy commensurate with the magnitude of the problem?

In 1980, the U.S. government spent $518 million on public diplomacy activities, and funding increased each successive year for most of the following decade. With the fall of the Soviet Union in 1989, and perhaps because of complacency with the U.S. position in the world, some in American government and academia circles began to view public diplomacy as a relic of history. In the years between 1989 and the events of 9/11 both Congress and the various administrations

downplayed the importance of funding public diplomacy activities. Public diplomacy often was viewed as less important than political and military functions and was seen by some legislators as a pot of money that could be tapped for funding other government activities deemed more important or more popular with constituents. While actual funding increased during this time, and levels in Fiscal Year (FY) 2000, FY2001, and FY2002 were higher than in 1980 ($770 million, $712 million and $747 million respectively), in constant dollars, funding during these three years dropped below FY1980 levels.[43] In 1999, the United States Information Agency (USIA), America's primary public diplomacy agency, was folded into the U.S. Department of State as part of an effort to reorganize the foreign policy agencies (largely for budget savings purposes.)[44]

The President's FY2007 budget request of $1.6 billion set the record for U.S. government public diplomacy expenditures. While an impressive figure, in constant dollars FY2007 U.S. Government expenditures for public diplomacy are less than FY1994 expenditures and equal to what was spent on public diplomacy activities during FY1987. Since the terrorist attacks of 9/11, new funding designated for public diplomacy (posted to the State Department's Diplomatic and Consular Programs account) has been added through both regular and supplemental appropriations. Supplemental funding has become a standard practice for public diplomacy activities. Between FY2002 and FY2006, public diplomacy activities have received about $245 million in emergency supplemental appropriations.[45]

Despite the recent increase in funding, critics point to what they view as meager levels for public diplomacy as compared to military and other expenses. Since 2002, the Council on Foreign Relations has consistently recommended that funding for public diplomacy should be increased to "significantly higher levels" to be more in line with its role as a vital component of U.S. foreign policy.[46] Some assert that as the world gets smaller due to information technology, being vigilant about foreign population's attitudes of America is as important and less costly, perhaps, than a buildup of military strength.[47] However, if present funding levels are any indication, Congress and the Administration do not concur with this assertion.

A longstanding public debate as to whether or not public diplomacy is simply cleverly packaged propaganda (and therefore morally suspect) is another aspect of public diplomacy's acceptability. Propaganda is defined as "the spreading of ideas, information, or rumor for the purpose of helping or injuring an institution, a cause, or a person."[48] In 1955, Oren Stephens, author of *Facts to a Candid World: America's Overseas Information Program*, called such programs (now known as public diplomacy) "propaganda" and referred to the U.S. Declaration of Independence as being "first and foremost a propaganda tract."[49] During his 1963 testimony to a House of Representatives subcommittee, the highly respected and internationally recognized broadcasting personality and then USIA Director, Edward R. Murrow referred to his agency's activities as propaganda.[50] Stephens and Murrow were in no way disparaging America's overseas information activities when they referred to them as propaganda over forty years ago. However, in today's culture, propaganda connotes falsehood, and public diplomacy practitioners bristle at the use of this word as a descriptor of their activities. At a 2002 forum on "Press Coverage and the War on Terrorism," co-sponsored by the Brookings Institution and Harvard University, Former Ambassador Christopher Ross articulated this perception when he said, "When I hear the word propaganda I imagine a much more manipulative kind of process than I would like to think public diplomacy is."[51]

Arguably, America's experiences with the disinformation campaigns of Germany and Japan in World War II, and worldwide communism during the Cold War, created a mindset in the American psyche that propaganda is dishonorable and underhanded, and not the "American way." Americans seem reluctant to put a lot of effort and resources into their public diplomacy. This reluctance may in part be attributable to a deep-seated resistance in the American psyche to "propagandizing" and a fundamental belief that truth will always win out in the end.

Suitability assesses whether the strategy can reasonably accomplish its objectives, while considering resources, effects, and the timeline for implementing the strategy. The apparent mismatch of resources and priorities for American public diplomacy has already been discussed, and the conclusion here is the same. The resources being applied to

U.S. public diplomacy activities are not sufficient to ensure it effectively accomplishes its objectives.

The United States is involved in a generational and global struggle about ideas. The 2006 NSS details America's strategy to achieve victory in this struggle and states that it will be "the work of generations."[52] A transformational public diplomacy strategy will only succeed if it is resourced properly and is persistent. This strategy will take at least a decade to have a significant impact. In the United States, election cycles and episodic commitment have shaped public diplomacy for more than half a century.[53] Can the current public diplomacy strategy reasonably accomplish it objectives? Only if America changes the paradigm of how it resources and implements this strategy and then sustains the effort over the years and decades that it requires.

Implications of Ineffective Public Diplomacy

If effective public diplomacy is a key component of U.S. foreign policy and vital to the success of its NSS, then it follows that ineffective public diplomacy can undermine America's ability to achieve its foreign policy and national security objectives. The National Defense Strategy (NDS) supports the NSS by establishing the following overarching objectives to guide Department of Defense (DoD) security activities and provide direction for the National Military Strategy (NMS):[54]

- Secure the United States from direct attack and counterattack, at a safe distance, by those who seek to harm the country
- Secure strategic access to key regions, lines of communications and the "global commons"[55] of international waters, airspace, space and cyberspace
- Strengthen alliances and partnerships by helping other nations increase their ability to defend themselves and protect common security interests
- Establish security conditions favorable to the United States and its partners while working to expand the community of like-minded nations[56]

From these strategic objectives flow the missions of America's armed forces. In this final section we will consider some implications that ineffective public diplomacy may have on the ability of the U.S. military to accomplish its mission.

With the fall of the Berlin Wall in 1989 and the demise of the Union of Soviet Socialist Republics (USSR) in the 1990's, the United States of America stood alone as the only nation that had worldwide interests coupled with the capability to project decisive military power anywhere throughout the globe. Since World War II, America has maintained forward based and forward deployed military forces in countries and oceans around the world. The presence of these forces have strengthened alliances, reassured allies, deterred potential foes, promoted stability, and projected an aura that the United States was everywhere. America's ability to project military power at the time and place of its choosing translated to influence—the ability to produce an effect on the world scene without apparent exertion of force or direct exercise of authority.[57] Today, America is clearly the dominant power on the planet and its ability to project military might anywhere on the globe is unrivaled. From this one might logically infer that U.S. influence around the world is dominant and unassailable. Unfortunately, despite the fact that America remains the world's preeminent economic and military power, the deterioration of its reputation and credibility abroad is resulting in a decline of America's worldwide influence.

So what does increased anti-American sentiment and the resultant loss of American influence mean to America's armed forces' ability to accomplish the objectives set forth for it in the NDS and NMS? What are the future capabilities of the U.S. military to deploy and forward base around the world? The answers to these questions are not encouraging and foreshadow a hobbling of the mighty American war horse. The primary effect of America's penchant for unilateralism, perceived U.S. led globalization, and prevalence of U.S. supported state authorities unresponsive to their populations, is a growing international loathing of the United States.[58] Second and third-order effects of this negative trend are increased foreign public support for terrorism directed at Americans, adverse impact on the cost and effectiveness of U.S. military operations, and a weakening of the United States' ability

to align with other nations in pursuit of common policy objectives. These effects negatively impact the U.S. military's ability to accomplish its global missions of defense, deterrence, and fostering stability. Using the context of the four overarching defense objectives set forth in the 2005 NDS this paper explores some of these effects.

Secure the United States from direct attack. The enemy America faces today is a complex network of ideologically driven extremists. Their objectives are to terrorize America's citizens, undermine its partnerships with other nations, and erode its global influence.[59] Victory on foreign battlefields alone will not suffice to defeat this foe. In order to secure the U.S. homeland from direct attack the NDS states that, "we will give top priority to dissuading, deterring, and defeating those who seek to harm the United States directly, especially extremist enemies with weapons of mass destruction."[60] Achieving this objective requires a broad international effort to deny terrorist networks the sanctuaries and resources they need to operate and survive.[61] Ongoing military operations around the world to find, fix, and destroy the enemy are the main thrust of this effort. As an enabler, public diplomacy's objective is to remove obstacles to cooperation and coordination between nations so there is unity of purpose and a shared vision in this generational struggle to eradicate the global threat. Increasingly sophisticated use of the Internet and media is enabling extremists to coordinate and execute their operations with minimal risk to themselves or their organizations.[62] American public diplomacy must effectively employ these same tools to discredit terrorists by promoting truthful and peaceful messages.[63] However, with America's influence and credibility declining, the world may increasingly reject its message, and other nations may be increasingly united against American policies and interests in the future rather than united in support of them. Unless this trend is arrested, America may have difficulty in achieving the international unity of effort necessary to "counter, at a safe distance, those who seek to harm [America]."[64]

Secure strategic access and retain global freedom of action. The U.S. military can not defend America's security interests in areas of the globe it can not reach. While its global strike[65] capabilities are impressive, America's armed forces need strategic access to key regions, lines of

communication, and the global commons to enable these capabilities and set conditions for follow-on decisive operations. Agility gives U.S. commanders the ability to contend with the principal characteristic of today's security environment—uncertainty. Agility is the ability to rapidly deploy, employ, sustain and redeploy capabilities in geographically separated and environmentally diverse regions. Agility ensures the U.S. military can act swiftly and decisively to protect American interests abroad.[66] Strategic access is the key to agility—access to air bases and sea ports in foreign countries, the ability to pre-position strategic assets, overflight rights, and permission to transit territorial seas. America's ability to project military power at the time and to the place of its choosing hinges on strategic access. Experiences during the Iraq War provide telling examples of how U.S. strategic access was tied to America's relationships with not only Iraq's neighbors, but long-standing allies far removed from the theater of operations. From Turkey's refusal to allow U.S. combat forces to attack Iraq from their country, to current restrictions against launching combat aircraft from U.S. airbases on foreign soil, it is readily apparent that the U.S. military is dependent on America's relations with the governments and peoples of the world for its global freedom of action.

Strengthen alliances and partnerships. The NDS declares that international partnerships and alliances are a principal source of America's military strength. Mutual alliances between like-minded nations provide far greater collective security than any one nation can achieve on its own.[67] DoD's Security Cooperation Program is one of America's principal vehicles for strengthening alliances and partnerships. This program encourages partners and allies to increase their military capability and willingness to operate as part of international coalitions. Security cooperation spurs the military transformation of key allies through the development of a common security assessment and joint, combined training and education; combined concept development and experimentation; information sharing; and combined command and control. One of America's most effective tools in prosecuting the GWOT is training indigenous forces.[68] The growing trend of anti-Americanism and resentment of U.S. policies may undermine America's relations with its partners and allies to the point where they will deem it politically expedient to curtail their participation in DoD's Security

Cooperation Program. Indeed DoD obliquely recognizes this in its NDS when it states, "our capacity to address global security challenges alone will be insufficient; some allies and partners will decide not to act with us; our leading position in world affairs will continue to breed unease, a degree of resentment, and resistance."[69]

Establish favorable security conditions. America "will create conditions conducive to a favorable international system by honoring our security commitments and working with others to bring about a common appreciation of threats; the steps required to protect against these threats; and a broad, secure, and lasting peace." These objectives will be accomplished by assuring America's allies of our commitment to their physical defense, by dissuading potential allies, by deterring aggression, and countering coercion.[70] Effective public diplomacy will be critical to the success of these actions. The United States must credibly communicate to the world its commitment to international partners, and consistently demonstrate the will to resolve conflicts decisively on terms favorable to itself and its allies. Ineffective public diplomacy can undermine American credibility abroad, allow misconceptions of America's military capabilities and national resolve, and inadvertently communicate to friends and allies that America's commitment is wavering. In today's interconnected world, John Donne's Renaissance Era concept, "no man is an island,"[71] rings more true every day. To achieve this objective, the U.S. military will increasingly rely on collaboration with like-minded nations to bring about a common appreciation of threats; protection against these threats; and a broad, secure, lasting peace.[72] Ineffective public diplomacy undermines America's ability to assure, dissuade, deter and coerce, and threatens the establishment of security conditions necessary for a favorable international environment.

America's national security interests increasingly require that other nations around the world share a common view of the solutions to the challenges and uncertainties of the 21st century. America's public diplomacy must effectively counter the growing trend of world-wide anti-Americanism. Failure to do so will negatively impact America's ability to implement key tenets of its national security strategy. While improved public diplomacy alone will not arrest the decline in

America's image and influence abroad, failure to dramatically improve what America is telling the rest of the world will increasingly hamstring the ability of the United States Armed Forces to defend America's vital interests at home and abroad.

Strategic Communication: A Department of Defense Approach

Lieutenant Colonel Bart E. Stovicek
United States Army Reserve

> *Policies matter. Mistakes dismay our friends and provide enemies with unintentional assistance….Strategic communication is a vital component of U.S. national security. It is in crisis, and it must be transformed with a strength of purpose that matches our commitment to diplomacy, defense, intelligence, law enforcement, and homeland security.*[1]

In its 2004 report on Strategic Communication (SC), the Defense Science Board (DSB) highlights this accurate yet pessimistic view of the state of United States Government (USG) SC. Under the heading "Strategic Communication," the 2006 Quadrennial Defense Review (QDR), serving as a roadmap to change within the Department of Defense (DoD), stated the requirement to, "integrate communications efforts horizontally across the enterprise to link information and communication issues with broader policies, plans, and actions."[2] Most recently, in September of 2006, the DoD published the Strategic Communication Roadmap (hereinafter called the Roadmap) to ensure that the objectives identified in the QDR are achieved. While the Roadmap does not constitute policy in the strictest sense, it serves as the guiding force to SC policy being developed within DoD by providing a plan of action and milestones. Curiously, however, the first task identified in the Roadmap is to establish a new SC organization to facilitate horizontal integrated communication efforts. Such a move presupposes that there is not already a mechanism established to serve this purpose. Thus, the Roadmap adds an additional vertical layer of coordination to achieve horizontal integration, and focuses on only a few "primary supporting capabilities," rather than the integration of all capabilities in support of USG SC objectives. Pursuit of this policy will further degrade the unity of effort necessary to integrate *all* DoD capabilities toward achieving USG SC goals and will continue to

marginalize the effectiveness of supporting communication capabilities by creating redundant communication architecture within DoD.

The fundamental problem lies in the lack of a USG SC strategy and the absence of a precise definition of SC. As a result, there is an unclear understanding of the department's supporting role in USG SC that has yielded a flawed approach to the problem within DoD. Effective SC is indeed a vital component of U.S. national security and in the QDR the DoD has properly articulated its vision of the department's role in supporting the integration of its military capabilities in support of USG SC efforts. However, the Roadmap poorly interprets the QDR SC imperative and fails to properly implement proper strategic controls to ensure unity of effort is maintained in DoD support to USG SC. These failures degrade the competitive position of the U.S. in the international information environment. This essay will show why an effective USG SC strategy is necessary and will seek to define DoD support to SC. Further, this essay will show that effective DoD support to SC can only be achieved by developing an SC culture within DoD and that existing capabilities must be strengthened in order to ensure strategic competitiveness and effective USG SC during the next century.

Strategic Communication: If America Does Not Explain Itself, the Extremists Will Do It for Us

The USG has no SC strategy to serve as the foundation for integration of all USG efforts to effectively communicate its policies to the world. As a result, in the world at large and especially in the Muslim and Arab world today, the USG is challenged to explain itself: to explain why the U.S. is in Iraq and Afghanistan; why the U.S. is not in Darfur or Iran; why Israel is such an indispensable ally; why the USG supports governments that suppress, sometimes brutally, the very freedoms it professes to represent, and so on. The USG, through its agencies and departments, implements policies and engages audiences across the globe. Its policies and actions speak for themselves, but its ability to meet the challenge of explanation through mutually supporting actions and messages from all elements of the USG interagency has been, and continues to be, inadequate.

Across the globe people view Americans with varying levels of confidence and/or skepticism regarding their belief that America is a beacon of freedom and tolerance. Arguably, a vast majority of the global population has only indirect experience with the U.S. and its agents. Invariably, their beliefs are shaped by their own personal experience; by influence from key communicators within their societies; and within the context of their own social, economic, and political environment. Nowhere is this felt more acutely than in the Arab and Muslim world. As the U.S. seeks to marginalize extremists, success in this endeavor is determined primarily by its policies.[3] Adversaries of the United States understand their own populations better than the U.S. does. They understand how to communicate with them better than the U.S. does, and they understand the deep seated resentments and historical animosities toward the U.S. that motivate their audiences to accept and in some cases act on their own version of the truth. America's adversaries leverage this advantage to portray U.S. policies, both historical and contemporary, in a negative light.

The U.S. message of freedom and tolerance, though powerful, is not powerful enough alone to overcome this advantage. Ambassador Karen Hughes, the current Under Secretary of State for Public Diplomacy and Public Affairs, believes that "given a fair hearing and a free choice, people will choose freedom over tyranny and tolerance over extremism every time."[4] This statement is a great sound-bite, but it must be carefully considered to grasp the full impact of its meaning. Freedom and tolerance are the messages, but a fair hearing and free choice are the ultimate conditions to be established in order for the message to be heard, believed, and ideally, acted upon. Establishing these conditions locally, regionally, nationally, and internationally involves so much more than just words. It demands a synchronized and coordinated effort of mutually supporting actions and messages by all elements of the USG.

There continues to be a need for a national communication strategy that provides objectives and guidance for both regional and transnational issues and a mechanism to coordinate all interagency informational efforts at the national level.[5] The effort to accomplish this is underway within the Department of State (DoS) under the leadership of

Ambassador Hughes. Since September 11, 2001, DoS has expanded its public diplomacy efforts globally; and echoing the belief of Secretary of State Rice in the "integration of public diplomacy, of message, of communications and policy"[6] Ambassador Hughes developed a strategic framework to focus DoS PD efforts.[7] This framework, however, is specific to the DoS. As the lead for the Policy Coordination Committee on Public Diplomacy and Strategic Communications, Ambassador Hughes is responsible for ensuring that *all* agencies are working together in this effort. Hence, interagency coordination continues to be insufficient. The Government Accountability Office in its May 2006 report on public diplomacy comments on this chronic inadequacy stating: "since 2003, we have reported on the lack of strategic elements to guide U.S. public diplomacy efforts. Despite several attempts, the United States still lacks an interagency public diplomacy strategy."[8]

Defining DoD Support to Strategic Communication

Despite the absence of a unifying U.S. national SC strategy, DoD included SC as a specific area of study in its 2005 QDR. The QDR did not provide a specific definition of SC in its final report but acknowledged that SC is a government-wide responsibility and made the following finding:

> *The Department must instill communication assessments and processes into its culture, developing programs, plans, policy, information and themes to support Combatant Commanders that reflect the U.S. Government's overall strategic objectives.*[9]

Stating the DoD SC imperative in this way provides an adequate point of departure for the development of SC policy within DoD because it describes the necessary link between DoD communication efforts and USG overall strategic objectives. Absent a definition, however, this statement may lead one to believe that DoD "communication assessments and processes" are SC, when, in fact, they are capabilities necessary to successfully support USG SC.

If SC is not precisely understood, DoD and the interagency are doomed to wrestle with its implementation. The Roadmap defines SC as a USG process:

> *Focused United States Government processes and efforts to understand and engage key audiences to create, strengthen, or preserve conditions favorable to advance national interests and objectives through the use of coordinated information, themes, plans, programs and actions synchronized with other elements of national power.*[10]

Jeffrey Jones, the former Director for Strategic Communications and Information on the National Security Council defined it as "the synchronized coordination of statecraft, public affairs, public diplomacy, military information operations, and other activities, reinforced by political, economic, military and other actions, to advance U.S. foreign policy objectives."[11] In an effort to establish a common reference for members of the Interagency Strategic Communication Fusion Team in a presentation on SC and psychological operations (PSYOP) a simple definition was provided: "the directed transmission of USG 'intent' through a supporting architecture to an audience for a reason that supports U.S. goals or objectives."[12]

These efforts to define SC offer clarity, but highlight the difficulty in providing a single unifying definition. The absence of an official national SC definition, like the absence of a strategy, convolutes USG efforts to develop SC policy. In the end, the Roadmap definition serves very well as DoD attempts to develop its role in support of it. Common to all definitions is the representation of SC as a USG process. The use of USG to describe SC throughout this essay are redundant with this distinction in mind. All SC in this context are USG activities. The contributions made by the various USG departments and agencies (including DoD) are not, by themselves, SC. Rather, SC is the synchronized and integrated coordination (see Jeff Jones' definition above) of these contributions in order to achieve the broader USG strategic communication objectives. The distinction is very simple. DoD, DoS and other USG departments and agencies support SC by conducting various communication activities such as Public Diplomacy, Public Affairs (PA), or PSYOP. Additionally, other activities are conducted, such as deployment of a carrier group, funding of a new weapons system, or Theater Security Cooperation. Like the specific communication activities, these actions are conducted to achieve a specific aim within the department or agency conducting

them, but when viewed as a part of all USG activities, in support of national objectives, they also support SC.

SC can be compared to a wristwatch. The purpose or overall objective of the watch is to provide accurate time. Interagency communication activities are analogous to the hands on the watch. These are the specific activities conducted to translate the action within the watch into symbols that represent accurate time to the owner (audience) of the watch. The gears and springs and screws within the movement of the watch are all of the other activities that must be conducted in order to provide accurate time. The purpose of the movement is to maintain the steady motion of the hands; a more limited objective than providing accurate time. As individual components, the gears and hands are not a wristwatch, and their action in isolation does not provide accurate time. However, when all components of the watch are operating together in a synchronized and coordinated fashion for the purpose of providing accurate time, they are a wristwatch. Activities conducted by USG departments and agencies, when performed in isolation are not SC and serve limited objectives, but when coordinated and synchronized with integrated communication activities in support of broader national objectives, are SC.

Proper development of SC policy demands an understanding of this precise distinction between USG SC and the various capabilities and actions necessary to support it. The DoD SC imperative above calls for the strengthening and improved integration of DoD communication capabilities within the existing DoD culture, and framework for planning and execution. The Roadmap, however, in attempting to provide implementing guidance has redefined the imperative to "strengthening *Strategic Communication processes.*" This focus on a SC process within DoD, rather than existing capabilities and processes, has tremendous impact on the outcome. By attempting to create a new "Strategic Communication" process where none previously existed within DoD, the writers of the Roadmap are creating a redundant mechanism for integration.

At first glance, this appears reasonable; if we are not effectively supporting SC, then greater oversight must be established. But an inadequate USG SC effort does not necessarily equate to a requirement

to reinvent DoD communication processes. In its September 2004 report on Strategic Communication, the DSB makes a strong case for implementing a new vision for SC, but nowhere in the document does the board explicitly state that DoD communication processes, are inadequate. Rather, the DSB recommends an increased emphasis on existing capabilities, processes and activities that support SC. However, the Roadmap gives notice of intent to create a new process by stating: "To this end, OSD and the Joint Staff will develop a staff process that integrates and supports Strategic Communication initiatives."[13]

Responsibility for coordination of interagency activities in support of SC rests with the Policy Coordination Committee (PCC) on Public Diplomacy and Strategic Communications led by the Under Secretary of State for Public Diplomacy and Public Affairs.[14] There is an inherent responsibility for each USG agency to integrate and synchronize internally. Within DoD, responsibility for integration of communication activities with policies, plans, and operations rests with Combatant Commanders. The weak link is effective integration into the overall USG effort. Within DoD, responsibility for integration with the interagency resides with the Office of the Secretary of Defense (OSD) and the Joint Staff.

Implementing the QDR Vision For SC

"Clearly, if you are going to do well over time, you have to have some ability—yourself or in combination with others—to come up with a vision…and then follow it up with believable and implementable action plans"[15] The 2006 QDR identifies SC as an area of particular emphasis for DoD and provides the guiding vision to strengthen its support of efforts led by the DoS for integration of SC across the federal government. The Roadmap serves as the guide or action plan for implementing this vision. Overall the Roadmap provides an effective and coherent plan for improving DoD support to SC except for one flaw; it's imperative to establish SC architecture within the department.[16]

"Shaping the choices of countries at strategic crossroads" is one of four priority areas for examination the QDR identifies in order to effectively operationalize the U.S. National Security Strategy. To

this end, the examination recognized that "security cooperation and engagement activities…to increase understanding, strengthen allies and partners, and accurately communicate U.S. objectives and intent" require new authorities and an improved interagency process.[17] This statement is supported by findings of the DSB Task Force on Strategic Communication. Of the seven recommendations presented by this task force to transform SC, only two are specific to DoD. Indeed, the first three recommendations are: to provide much needed Presidential guidance; develop an SC structure within the NSC with representation from key governmental departments and agencies, and with increased directive authority; and to create a "Center for Strategic Communication to support the NSC and the departments and organizations represented on its Strategic Communication Committee."[18]

The QDR implicitly and properly ties effective DoD support to SC to an equally effective interagency process. The QDR does not specify how the SC linkage between the interagency and DoD is to be made, but it does recognize the need to transform from a single departmental approach on strategic issues to an interagency approach and offers several recommendations to strengthen the process. Further, DoD understands that although the lead agency for USG SC is the DoS, the same integrated approach to communication activities is necessary within the department to effectively support SC, and DoD communication capabilities must be properly organized and resourced to ensure adequate support to SC efforts. The QDR specifies two key tasks to achieve these aims:

1. Ensure DoD activities, plans, and policies accurately reflect overall USG strategic objectives
2. Focus on properly organizing, training, equipping, and resourcing the key communication capabilities[19]

To achieve the first task, the QDR calls for integrating communications assessments and processes horizontally throughout the department,[20] thus providing commanders, planners, and operators with increased understanding of the information environment and DoD communication capabilities at their disposal. Horizontal integration means eliminating stovepipes and reducing unnecessary overhead; providing functional experts to key staffs and planning groups. It calls

for continuous and greater cooperation and collaboration between supporting communication capability functional experts and operators within matrix organizations, not merely functional ones. This will yield greater integration of key communication capabilities into plans and operations because of increased familiarity on the part of commanders, planners, and operators with the effects that can be achieved by their employment.

The second key SC task specified in the QDR is to focus on properly organizing, training, equipping, and resourcing the key communication capabilities. The QDR specifies the DoD primary supporting capabilities to SC as PA, Defense Support to Public Diplomacy (DSPD), Military Diplomacy (MD), and Information Operations (IO) including PSYOP. Of these only PA and PSYOP are actually military capabilities in the sense that they have a force structure, technical sophistication, sustainability, and the ability to provide the requested capability to Combatant Commanders.[21] IO, DSPD, and MD are activities conducted by DoD to achieve specific information effects.

One could argue, therefore, that the QDR focus is on PA and PSYOP. While this argument is enticing to proponents of those two capabilities, the task must be considered more fully. The information operating environment continues to evolve; synchronization of a wide range of military capabilities and activities is necessary to achieve information effects. Therefore, there are three implied tasks that can be drawn from the QDR guidance. First, PA and PSYOP, as DoD communication capabilities, must be properly organized, trained, and equipped. Second, doctrine and authorities for the application of capabilities and activities to achieve information effects must be reviewed and refined. Finally, resources must be devoted to training commanders, operators, and planners on the information environment, its relevance to operations, and the capabilities and activities that may be employed to achieve informational effects.

The three overarching objectives of the Roadmap that directly address these issues are:

- Objective 1: Institutionalize a Strategic Communication process in DoD
- Objective 2: Define roles, responsibilities and relationships, and develop doctrine
- Objective 3: Properly resource, organize, train, and equip[22]

Objectives 2 and 3 align quite well with the vision as presented in the QDR. Objective 1, however, is problematic in that it creates a Strategic Communication Integration Group (SCIG) supported by an SC Secretariat that is specifically responsible for coordination across DoD and with the interagency on issues and policies with significant communication implications. Though the SCIG offers the appropriate level of rank to assure representation at the highest levels of the interagency, it actually serves to further frustrate the effective integration of DoD supporting communication capabilities internal to DoD by creating a redundant integration mechanism and an additional vertical layer of organization.

Is There a Need For a SCIG?

Integrating "communications efforts horizontally across the enterprise," as stated in the 2006 QDR, is the goal. This is a requirement for greater integration that has been translated into an additional organization, an organization that seeks to further isolate DoD communication activities from traditional departmental processes in order to facilitate integration—hence the flaw. The process, structure, and responsibilities already exist for integration within the department so why reinvent the wheel?

The reason for the development of this particular solution to the problem of integration is embedded within the very culture of DoD and highlights another fundamental flaw in the development of SC policy. A "culture reflects what the firm has learned across time through its responses to the continuous challenges of survival and growth."[23] The U.S. military traditionally creates working groups and functional teams to analyze and gain greater understanding of particular problems. Normally this is done because a problem is complex, or because it is an emergent problem, and responses or reactions are not well understood

and have not been institutionalized. Strategic Communication is an excellent example of such a problem. Not only is SC complex, but it is poorly understood. Further, only within the last decade or so, have military leaders begun to appreciate the importance of the information environment and its affect on the conduct of military operations. This appreciation unaccompanied by an increase in institutional and leader understanding about how to use existing capabilities to effectively shape the information environment has created a gap. In order to fill this gap, the QDR's SC working group has followed this cultural norm and created a new organization. The SCIG has been established, along with an SC Secretariat to coordinate across DoD, to develop policy guidance, provide guidance to Combatant Commanders, deconflict SC decisions arising out of the interagency, and incorporate SC processes into policy development, doctrine, strategy, planning, and operations.[24] The Joint Operations Planning and Execution System has been updated with SC guidance, even before the development and promulgation of SC policy. The goal of these activities is to place the institutionalization of the "process" on a fast track.

But the roles and responsibilities are unclear. The SCIG is not an authoritative DoD policymaking body, nor is it an organization that is integrated into Joint Staff planning processes. The creation of the SCIG provides an overarching DoD focal point for SC integration with other USG agencies but threatens to interfere with and even replace existing staffing processes and procedures. For example, while SC policies and processes are being developed and pushed by the SCWG, policies for IO and PSYOP are slow-rolled through the staffing process. Indeed, the current approved DoD Directive for PSYOP is over 20 years old, and its update remains in limbo in OSD staffing.

At first glance, the vast array of activities identified in the QDR as primary supporting capabilities to SC appear to warrant additional controls but, as indicated above, only PA and PSYOP are separate and distinct capabilities represented by forces and doctrine specifically established to conduct their functions. Both of these capabilities are doctrinally integrated into planning. In fact, the responsibility for their integration, coordination, and de-confliction across DoD rests with the Joint Staff. While the SCIG may serve an integrating function at

the policy level with other entities of the interagency, any coordinating responsibility within DoD parallels existing responsibilities already inherent to the IO/J39 architecture that already exists. Further, as singular communication capabilities that provide support to SC, both PA and PSYOP are already integrated into the military organization so why the need for another guiding entity? Creation of a separate "stovepipe" provides motivation to operators to leave the integration of the communication capabilities in the hands of the so called "experts" allowing them to continue to focus on their own areas of expertise such as integration of kinetic solutions. Effective integration is dependent upon greater understanding of available capabilities by those charged to employ them. Today's operating environment demands that warfighters be as comfortable employing non-kinetic capabilities as they are kinetic. In order to achieve this, the layers between them and their capability specialists should be reduced rather than expanded.

As a mechanism for improved integration with interagency SC processes, the SCIG offers some promise. This promise, however, is lost as leadership of the SCIG is divided between the Under Secretary of Defense for Policy (USD-P), the Assistant Secretary of Defense for Public Affairs, and the Director of the Joint Staff. The Roadmap fails to identify a single definitive lead for DoD support to SC, thus additional organization must be established to support this new executive body. Indeed, the new organization, called the Strategic Communication Secretariat, adds yet another vertical layer of SC architecture as it seeks to integrate communication efforts horizontally. The DSB Task Force on SC recommends that the focal point for DoD support to SC should be the USD-P and further recommends the reorganization of the OSD policy directorate to provide a focal point for all DoD support to SC. Such a designation is consistent with the USD-P role as the lead for interagency coordination as dictated by DoD regulation and more accurately reflects the QDR vision by restructuring existing architecture to enhance horizontal and vertical integration.

Developing an SC Culture

"Unity of effort ultimately entails the type of professional military education and leader development that leads to effective diplomacy, as

well as to military competence."[25] The entire concept of effective USG SC is predicated upon unity of effort. In the few short paragraphs devoted to SC in the 2006 QDR the goal of "achieving a seamless communication across the U.S. Government" is plainly articulated. It has been an ongoing struggle within the interagency, and also within DoD, to define the organization and structure necessary to achieve this unity. However, despite any formalized organization or structure the entire effort is doomed to failure unless a culture is first developed across the enterprise that inherently considers the information environment and is comfortable leveraging capabilities to shape it.

Such a culture is not easily developed. Only recently have military commanders begun to accept that understanding and affecting the information environment is an operational necessity. In a recent article on Information Operations, Colonel Ralph Baker, an Operation Iraqi Freedom Brigade Combat Team Commander noted:

> *I admit that while I was preparing to serve in Iraq as a brigade commander, I was among the skeptics who doubted the value of integrating information operations (IO) into my concept of operations. Most of my officers on my combat team shared my doubts about the relative importance of information operations. Of course, in current army literature there is a great deal of discussion about IO theory. There is significantly less practical information, however, that details how theory can be effectively translated into practice by tactical units.*[26]

Unfortunately, this type of skepticism is the norm. Employing capabilities to affect the information environment is not a new concept, but it has taken on an increased level of importance to commanders at all levels as the military engages in more and more counterinsurgency and stability type operations. In these types of operations, where the supportive will and cooperation of the people within the operating environment has become essential to success, commanders have been unable to effectively employ the kinetic capabilities for which they have been trained. Though perplexing to many, commanders like Colonel Baker are slowly gaining a greater appreciation for the power of information. He states, "We were probably a good 3 to 4 months into our tour before we gained the requisite experience and understanding of key IO factors. We then began to deliberately develop a structure and

mechanism to systematically synchronize our information operations throughout the brigade."[27] Colonel Baker realized the futility of seeking solutions through purely kinetic means and actively developed a structure to apply his capabilities, in a non-kinetic way, to achieve his objectives.

Two interesting points can be drawn from Colonel Baker's article. First, prior to being in a live combat environment, he was skeptical. Understanding and appreciation of information and its effect on operations can only be partially developed in training. The nuances of communication and the collateral effects of words and deeds in cultures other than our own cannot be adequately replicated in training simply because information effects are typically cumulative and require extended periods of time to achieve. Warfighters seek instant gratification. They appreciate the immediate effect that an air-strike has, but with communication the target must be persuaded over time. Thus, in training, commanders and staffs can apply Tactics, Techniques, and Procedures others have used in order to gain familiarity with the mechanics of employing various capabilities. But only in a live environment can they truly see whether they have achieved the effects they have deliberately sought. Necessity in a live environment drove Colonel Baker to embrace IO. His successful application of capabilities to achieve results in his battle-space converted him into an advocate of IO.

Second, only after three to four months in the operating environment did Colonel Baker establish the organization or structure he needed to effectively employ his IO capabilities. The structure and methods for employing them exists, however, in doctrine. Prior to his gaining an understanding of the "IO factors," he chose not to implement the IO structure within his organization. There are certainly many reasons for this, not the least of which is the lack of qualified IO specialists on his staff. The most likely contributing factor, however, was his skepticism and lack of understanding. That which we do not understand is rarely effectively integrated. The structure he created, and which doctrine advocates was not additive to his organization, but was, rather, a realignment of existing staff elements to achieve greater functional

effectiveness. His new IO structure was embedded within his S-3 element and, therefore, fully integrated into his operations.

If the QDR calls for integration of communication efforts across the organization, the lack of understanding among key leaders must be addressed. Few leaders have had the experiences of Colonel Baker. Fewer still, have staffs trained in the integration of communication capabilities. These are shortcomings the Roadmap seeks to address by establishing Joint Strategic Communication curricula for Joint Professional Military Education (JPME) and by reviewing PA and IO billet authorizations at all Combatant Commands. The Army has taken an additional step of establishing additional IO capability specialists on staffs all the way down to the Brigade Combat Team level in order to ensure integration of information capabilities.

Developing a culture within DoD and throughout the services that fully considers the information environment and how to employ capabilities to shape it will take training, education, and experience. More importantly, commanders at all levels must provide emphasis to overcome cultural obstacles to effective employment of non-traditional capabilities. Colonel Baker inherently understood this stating: "My…IO observation is that for all types of military operations the commander's vision and intent are essential, but when directing subordinate commanders to perform outside of their comfort zones, personal involvement is especially necessary to ensure that the commander's concept is executed according to the plan."[28] Effective integration of communication efforts will only take place when the relative importance and understanding of the doctrine is achieved. As commanders and operators who have successfully employed communication capabilities rise through the ranks, the culture will naturally develop, but the continuous integration of these capabilities in all plans and operations must continue in order to sustain it.

Supporting the Commander

> *We are not consistently achieving synergy and mass in our strategic communications….The collective belief is that we lack the necessary skills, resources and guidance to synchronize IO in order to achieve tangible effects on the battlefield.*[29]

Lieutenant General Metz's observation very succinctly highlights the requirements for meeting the vision of strategic communication identified in the QDR. It is the commander's responsibility to exercise effective strategic control within their organizations. He is supported at all levels, including the policy level, by staff elements traditionally charged with developing plans and policies that reflect his guidance and intent. However, if guidance from his higher is absent (read: lack of SC strategy), and necessary resources and expertise for the effective employment of communication capabilities does not reside within his own organization (read: lack of required billets and force structure), he must rely on his own experience level and that of his staff to effectively divine the intent of his higher command and integrate all available capabilities into his operations. This is no way to run a military operation and, while commanders such as Colonel Baker are clearly up to the challenge, a better alternative must be provided to provide the commander with the guidance and support he requires.

According to Ireland and Hitt, "top managers must acquire deep understandings of the competitive conditions and dynamics of each of the units or divisions for which they are responsible."[30] The information environment is certainly a new and challenging competitive environment that commanders must understand. Accordingly, commanders and their staffs must be as comfortable with the employment of non-kinetic capabilities as they are with traditional kinetic ones. The Roadmap identifies ways to provide commanders, and other government agencies, with assessment tools to better visualize and understand the information environment, and provide them with more tangible measures of the effectiveness of their efforts in trying to shape it. The Roadmap also requires a review of existing communication capabilities within DoD (PA, PSYOP, IO, and Visual Information) to determine whether their current size, structure, training, doctrine, and leadership are adequate to meet the needs of Combatant Commanders. Providing commanders with improved assessment capability and adequately resourcing their communication capability requirements will result in better decision support and access to greater expertise as they seek to achieve effects within the information domain.

Institutionalization of an effective SC culture implies that commanders and staffs at all levels understand the importance of maintaining favorable conditions within the information environment and the capabilities available to them to do so. To accomplish this, traditional planning and integration processes must be reinforced with necessary capability expertise. Building a parallel DoD SC process and architecture does not accomplish this. Traditional communication capabilities such as PA and PSYOP have well developed doctrine and significant organizational structure that enables them to contribute, but both are significantly under resourced in several key areas. Non-kinetic capabilities and programs are traditionally underfunded. The DSB in their 2004 report indicated that "funding for public diplomacy programs and military exchanges should be tripled."[31] It is counter-intuitive to develop new SC structure within DoD, while existing capabilities available to commanders compete for limited resources, and do without. Supporting the commander means providing proper guidance, resources, and expertise to enable him to effectively operate. The absence of these three requirements, as is the case relative to DoD primary supporting capabilities to SC, dictates a correction of these inadequacies before relieving the commander of the responsibility for the mission. The QDR articulates this requirement, and the Roadmap assigns tasks aimed toward correcting the identified capability gaps.[32]

Conclusion

In today's information environment every word, action, or event has potential strategic impact. USG policies and actions carry significantly more weight than the words we choose to convey them and, in fact, the nature of the information environment is such that we may have very little control over the words, images, or manner in which our actions are conveyed to target audiences across the globe. Recognizing this, the DoD directed, through the QDR, the integration of communication assessments and processes into its culture, as well as a renewed focus on properly resourcing its key communication capabilities. The Roadmap effectively provides implementing guidance to ensure that these objectives, identified in the QDR, are achieved. But the Roadmap reaches further and directs the development of an SC architecture within DoD. This third objective of the Roadmap represents a flawed

understanding of SC, and threatens to supplant existing authorities. It is necessary, therefore, rather than creating an entirely new approach to supporting SC or reorganizing traditional communication capabilities under a moniker, to remove those factors that limit integration of existing capabilities into the overall plan. Lieutenant General Metz was again on point when he stated: "The successful massing of information effects requires *the commander* [emphasis added] to clearly articulate his intent for the integration of all the available elements of operations in the information domain into the battle plan."[33] From an SC standpoint, the absence of a national SC strategy represents a gaping hole in commander's intent. The commander remains responsible, however, for integration of all available capabilities into his plan of operations. The commander does not conduct SC, he conducts military operations, but with a keen understanding of the information environment and adequate level of capability and expertise available to him he is able to make decisions and conduct operations in a manner that enables him to achieve specific effects within the information domain that, in turn, support USG strategic objectives. In today's information rich strategic environment, the main effort must be on adequately resourcing those processes and capabilities that currently exist so that they are able to meet the needs of the warfighter, while preparing future leaders to use all capabilities to compete in the information environment.

Winning the War of Perceptions: A Regional Approach to Implementing Interagency Strategic Communications

Colonel Matthew P. Beevers
United States Army

The printing press is the greatest weapon in the armory of the modern commander....In Asia we were so weak physically that we could not let the metaphysical weapon rust unused.

— T.E. Lawrence

Everyday, we fight a battle as important and as difficult as the counterinsurgency effort in Iraq and Afghanistan—the battle for mindshare within the world community. While the U.S. lacks a coherent, top-down, policy-driven national-level communications framework capable of advancing U.S. interests and values on a global scale; the interagency, by operating within a regional construct, is capable of successfully implementing strategic communications programs and achieving decisive global effects.

According to a May 2006 Government Accountability Office (GAO) report on U.S. public diplomacy, the U.S. government continues to lack an interagency public diplomacy strategy capable of guiding the activities of its disparate agencies.[1] The GAO found nearly identical challenges in a 2003 report.[2] State Department Regional Bureau Chiefs, Combatant Commanders, Ambassadors and Chiefs of Mission, Joint Force Commanders and a host of other agency executives are often left on their own to interpret and implement their individual versions of what they perceive the U.S. national communications strategy to be, and thus fail to leverage the vast array of assets available throughout the interagency. Current communication methodologies fail to exploit the 21st century technological and informational landscape—an environment where terror and insurgent organizations operate with great skill, and in some cases, dominate the information environment. As the policy formulation machine continues to churn in Washington,

the U.S. continues to lose the battle for share of mind within the world community.

Challenges Facing U.S. Strategic Communication and the Need for Change

The U.S. faces three primary strategic communication challenges. They include the lack of a viable national-level interagency communications strategy;[3] domestic political polarization and its negative effects on the unity of a national message; and the global dynamics of the information environment. Compounding these challenges is the fundamental shift in the very nature of the strategic environment in which the U.S. operates as it seeks to support its allies, check its strategic competitors and defeat its enemies. Many scholars refer to this shift in contemporary conflict and the associated change in operating environments as Fourth Generation Warfare (4GW), or the blurring of lines between war and politics, peace and conflict, and battlefield and safety.[4] The information environment is changing in much the same way.

If the U.S. is to be successful in communicating its message it must first understand the environment in which it operates and apply strategies that are appropriate to that environment. As the cliché goes, America is always fighting the previous war.[5] This is to say that the U.S. inherently attempts to take the tactics, techniques and procedures from previous conflicts and apply them to a current conflict—this is also the case with how it executes strategic communications. Today, the U.S. is operating in a 4GW information environment using Third Generation Warfare communication strategies and tactics.[6] The monolithic military public affairs and State Department public diplomacy bureaucracies churn out press releases and conduct press conferences ad nauseam while insurgents nimbly highlight their successful attacks by posting cell phone videos on the Internet and distributing DVD's in local bazaars. Former Secretary of Defense Donald Rumsfeld stated the obvious when he quipped, "For the most part, the U.S. government still functions as a five and dime store in an eBay world."[7]

Rumsfeld went on to chide the U.S. Government's public affairs operations for its reactive, rather than proactive posture, characterizing

the problem as an "unacceptable, dangerous deficiency."[8] While the content of insurgent Internet postings and DVDs may run afoul of Western standards of decency and conduct, the strategic effects they deliver are telling. They become indispensable tools for recruitment and fundraising. Terror and insurgent organizations clearly understand that they are in a war of perceptions and ideals and for the most part, leaders in the U.S. government and the military alike understand this as well—yet next to nothing substantive has been done to advance this concept.

Both the May 2006 GAO report on public diplomacy and the 2004 *Report of the Defense Science Board Task Force on Strategic Communication* draw strikingly similar conclusions and advocate for similar corrective measures. The reports conclude that while the U.S. government has dramatically expanded its public diplomacy and public affairs efforts globally (and especially in the Muslim world), it has failed to develop and deliver a comprehensive strategic communication strategy capable of aligning its diverse activities.[9] In its report, the Defense Science Board vigorously advocates for a Presidential directive to "coordinate all components of strategic communication including public diplomacy, public affairs, international broadcasting, and military information operations."[10] While these measures clearly have merit, their successful and sustained implementation remains highly unlikely given the poor success rate of prior attempts at corrective action and the U.S. Government's exceptionally short institutional attention span. The short-lived White House Office of Global Communications and the systematic deconstruction of the United States Information Agency by the State Department are just two examples of the government's track record on the issue.

There is, however, some evidence that both the Department of Defense and the Department of State are attempting to correct the myriad of public affairs and public diplomacy challenges they face. Karen Hughes, Under Secretary of State for Public Diplomacy and Public Affairs, recently testified that after more than 30 often sharply critical reports, the department's public diplomacy team is re-energized and re-invigorated, has implemented most of the key recommendations in those reports, and now has a place at the most senior policy tables

of government. She notes that public diplomacy programs are reaching more people around the world more strategically than ever before—making public diplomacy a national security priority.[11] Furthermore, the State Department has developed interagency plans to combat ideological support for terrorism in key countries as well as a strategic communications plan for the U.S. Government, and is in the process of creating an interagency counter-terrorism communications center.[12]

The Defense Department, under the auspices of the United States Joint Forces Command, developed and successfully deployed a capability called the Joint Public Affairs Support Element. According to Joint Forces Command, the support element is a modular, rapidly deployable capability that provides a constant flow of timely, accurate information from Combatant Commanders to news organizations that set up camp wherever American forces operate.[13] The element met with much success when it deployed in support of Hurricanes Katrina and Rita as well as the U.S. Disaster Assistance Center mission in Pakistan following the 7.6 magnitude earthquake that leveled parts of northern Pakistan in 2005. In Pakistan, that element maintained full-time liaison with the public diplomacy staff at the U.S. Embassy in Islamabad, coordinating and synchronizing its efforts.[14]

While it's encouraging that both departments may be improving their own strategic communication functions, it remains unclear if they are improving along similar trajectories, capable of achieving strategic alignment and viable interagency integration on a national scale. What is also unclear is if these efforts, while noble, will ultimately be successful given the national political polarization in the U.S. and its often contradictory rhetoric that tends to drown out a coordinated, synchronized and compelling national message.

The effects of the U.S. political system—the polarization it often brings and the by-product of contradictory messages it produces—challenge the government's ability to deploy a coherent U.S. strategic communication capability. This is especially true in communicating with the developing world, and the Muslim world in particular, where the cultural divide with the West appears to be greatest. The U.S. political system and its democratic foundation is arguably the most liberal, open and tolerant in the world. However, adversaries and

allies alike often misinterpret the discourse resulting from rampant U.S. internal political competition as they seek to understand the true direction of American foreign policy. Pepperdine University's Ronald Reagan Professor of Public Policy, James Q. Wilson, describes these effects:

> *Denmark or Luxembourg can afford to exhibit domestic anguish and uncertainty over military policy; the United States cannot. A divided America encourages our enemies, disheartens our allies, and saps our resolve—potentially to fatal effect. What Gen. Giap of North Vietnam once said of us is even truer today: America cannot be defeated on the battlefield, but it can be defeated at home. Polarization is a force that can defeat us.*[15]

In testimony before both the House and Senate on April 25, 2007, General David Petraeus, commander of coalition forces in Iraq, deftly chastised Congress and others in a warning that the vitriolic political rhetoric brought on by the current political polarization in the U.S. is clearly being heard by the terrorists and insurgents he is charged with defeating, making his job more difficult. In talking with reporters after his testimony, Petraeus pointed out:

> *I did mention at one point during each of the different briefings that I think it is always helpful to remember the various audiences out there as this wonderful democratic process goes forward, and those are our partners, our allies, our coalition partners, the enemy, and also, frankly, our men and women in uniform who are giving their all for this effort, and their families who are sacrificing a great deal as well.*[16]

These phenomena significantly degrade the fidelity of the U.S. national message while creating a multitude of less dramatic unintended consequences that require the strategic communications infrastructure to exhaust valuable resources explaining away the real and perceived differences between the U.S. national message and its actions. Time and resources would be better spent understanding the complicated global information environment in which it must operate.

As the nature of conflict is changing, so is the nature of the global information environment. The effects of fragmentation, diversification and transparency heavily influence today's asymmetric

global information environment. Fragmentation, both in terms of the potential target audience demographics and the increasing number of ways these audiences receive information, is adding layers of complexity to the development and implementation of an effective and efficient global communications strategy. The increasing diversification of these global audiences creates the need for high levels of precision in message development, since in most cases a single broad-based message must be individually tailored to specific audiences within a country and often tailored again to specific audiences within the same geographic region in a given country. Transparency is also driving change in the global information environment. Low cost, ubiquitous communication technologies and new forms of media such as blogs are driving this transparency, making it possible for messages to be received without any contextual frame of reference.[17] The fragmentation, diversification and transparency of today's global information environment have made it possible for "tactical" events to have strategic consequences. Addressing these factors requires a paradigm shift in the analysis, exploitation and assessment of the information environment.

Terror and insurgent organizations already recognize these factors and how they affect the information environment. They almost instinctively understand how to exploit the local, national and international media, tribal customs and beliefs, rumors and cultural predispositions toward mystery and conspiracy, and a host of other subtle but effective communication methods.[18]

The widespread use of video and cell phone cameras and the availability of new Internet-based content delivery services have enabled terror and insurgent organizations to gain immediate access to a global audience. The proliferation of these new methods of content delivery allow insurgent and terrorist organizations to convey a message through content that is sometimes false and at times, staged. In addition, these content delivery methods are quite effective when targeted at youth. Since nearly 50 percent of the Arab population in the Middle East is 18 years of age or younger, this trend is especially troubling.[19] Still images, video, and accounts of incidents rapidly traverse the globe, regardless of the factual nature of the content. Today, more insurgent and terrorist content reaches audiences through non-traditional means

than through the mainstream U.S. and international media. This enables insurgent or terrorist actions or the actions of the U.S.—either real or perceived—to have a detrimental affect against the U.S. on the stage of world opinion.

The way traditional media organizations process and deliver insurgent-generated content contrasts significantly from the way these media organizations process and deliver content relative to U.S. policies and actions. Traditional media organizations broadcast videos of insurgents emplacing and detonating improvised explosive devices in the vicinity of U.S. forces, often with deadly effect, without editorial constraint. The same is true with respect to third-party interviews and audiotapes from insurgent leaders. Often, insurgent manifestos find their way into the mainstream media without editorial comment, no matter how outlandish or blatantly false the content. By contrast, the posting of footage from U.S. and Coalition operations, or content highlighting successful U.S. combat operations posted to Internet services such as YouTube by U.S. service personnel meet with significant media skepticism, accusations of propaganda and congressional inquiries. Terror and insurgent groups exploit this double standard—real or perceived. The U.S. must recognize this as part of the information environment in order for it to compete effectively in the information battlespace.[20]

Unfortunately, the U.S. has been slow to recognize the impact of these challenges and has yet to adapt to, or counter them, in any meaningful way. The existing U.S. credibility gap highlighted by the polling firms Pew Research Center for People and the Press and Zogby International, along with the other challenges already discussed almost eliminates the delivery of a national message from Washington as a viable option.[21] These factors have converged to create a condition where attempting to execute centralized interagency strategic communication is increasingly becoming a "fool's errand." Clearly, time is running out—but there may yet be alternative approaches.

A Regional Approach

Delivering messages from global vantage points through the appropriate regional, cultural and ethnic prisms will maximize the

rate at which the messages penetrate their target audiences. What this approach seeks to achieve is regional—or decentralized—delivery of the messages supporting U.S. foreign policy themes. But how can a regional or "operational" entity achieve strategic effects? The answer is it cannot—at least not by itself. This approach advocates that multiple, regionally-based external communications organizations, each working in synergistic fashion, each delivering messages specific to their regions but supporting broad U.S. foreign policy themes can achieve decisive strategic effects. This approach does not, however, discount the need for a centralized planning body that has authority to determine strategic themes that support U.S. foreign policy objectives.

The State Department's Office of Strategic Communication and Planning holds some promise in delivering that strategic capability. Any central strategic communication capability must operate in the sense that its role is one of strategic policy formulation, broad-based theme development and media analysis and assessment, along the lines of the State Department's Rapid Response Unit.[22] In today's information environment, messages delivered by the perceived seat of U.S. government have little chance of reaching their target audiences and achieving decisive effects, making a decentralized approach crucial.

The current monolithic delivery methodology fails to take into account the specific regional, cultural and ethnic nuances that are the very heart of the challenges the U.S. faces in telling its story. A distributed, cellular approach of centralized theme development and decentralized message delivery is more appropriate given the asymmetric nature of today's information environment. In the private sector, this approach is often referred to as "narrowcasting" or "niche marketing"—the aiming of messages at specific segments of a public defined by values, preferences, or demographic attributes; and has a strong track record of achieving measurable results.[23] While this concept is not new, employing it through an integrated interagency framework is.

An integrated interagency strategic communications framework for the most part does not exist and will not be easy to employ. The U.S. currently employs, at best, *ad hoc* communications organizations

comprised of transitory personnel from a few branches of government that have little executive buy in and who view their participation as an additional task.[24] This is a recipe for an exceptionally poor learning curve, disjointed messaging and a lack of synchronization. The axiom of "Defense is from Mars and State is from Venus" also applies to strategic communications.[25] While military officers focus on the military aspect of foreign policy, Foreign Service Officers deal with all aspects of that policy. Detailed planning is a core activity of the military, while general planning is acceptable in the State Department; teamwork is paramount in the military, while individual achievement is key in the State Department.[26] The differing hierarchical structures, training methodologies and cultures all align to make synchronization and unity of message difficult—but not impossible. Developing a formal interagency framework for coordinating and synchronizing communications is the key to overcoming these differences.

In order to execute fully integrated interagency communication on a regional level, each of the players must be part of a vetted, resourced and task-organized entity. But what might that entity look like? Fortunately, models do exist that demonstrate success in interagency integration. The Joint Interagency Coordination Group (JIACG) is one such model.[27] Composed of U.S. Government civilian and military experts accredited to and tailored to meet the requirements of a supported Combatant Commander, the JIACG establishes regular, timely, and collaborative working relationships between civilian and military operational planners while providing the Combatant Commander with the capability to collaborate with other U.S. Government civilian agencies and departments.[28] These coordination groups have met with much success and have been widely lauded by the Defense Department and other government agencies. The Joint Staff's assessment in April 2003 found that JIACGs integrated U.S. Government objectives in each region, and created a forum for interagency operational planning and coordination.[29]

To truly be effective, a communications coordination group must go beyond typical Public Affairs, Public Diplomacy and Military Support to Public Diplomacy functions and act as a coordinating and synchronizing capability, supporting both military and civilian

regional leadership. This is not to say that an external communications JIACG needs to support every U.S. endeavor worldwide. However, consideration should be given to placing a JIACG with each country team and Combatant or Joint Task Force Commander operating where the U.S. must achieve strategic communications synergy across the interagency and cannot assume risk in delivering its message with high precision.

Each interagency player brings a unique set of attributes to the strategic communications construct. The State Department and the United States Agency for International Development (USAID) bring an existing global footprint (242 embassies, consulates and missions worldwide) and many programs that are "slam dunk" good news stories including a variety of U.S. foreign aid and humanitarian assistance programs, an array of youth and cultural exchange programs as well as initiatives that seek to improve the rule of law and just governance.[30] Traditional tools of U.S. public diplomacy, such as the Voice of America and Radio Free Europe/Radio Liberty, and radio services for Iraq, Iran and Afghanistan provide valuable support to the State Department's public diplomacy effort. The USAID's global assistance and development efforts are an untapped resource that can deliver a wealth of positive messages. The Advisory Group on Public Diplomacy for the Arab and Muslim World characterizes much of the agency's work as public diplomacy at its best.[31]

The Defense Department brings a wealth of institutional infrastructure, manpower, planning expertise and a comparatively robust budget to the mix. The Defense Department can also act as a synchronization hub given what is a typically broader geographic responsibility. Ambassadors are responsible for a single country whereas Combatant and Joint Force Commanders normally have authority over regions covering several countries. This dichotomy often requires military commanders to coordinate with multiple country teams in order to fully synchronize political-military efforts for a specific region.

Senior military leaders can be powerful instruments in supporting U.S. foreign policy objectives regionally. Moving beyond their traditional roles, these officers often act as "proconsuls"—an example

being former Coalition commander in Afghanistan, Lieutenant General David Barno (U.S. Army). Ann Scott Tyson of the Christian Science Monitor characterized the capability LTG Barno brought to the interagency effort in Afghanistan:

> *Combining a soldier's focus with a diplomat's finesse, Barno has, over the last nine months, molded a new, holistic approach to Afghanistan aimed at strengthening the central government against challenges from warlords and insurgents alike. In essence, he's turned a faltering, combat-centric U.S. military strategy on its head - and taken on a role beyond the usual scope of a U.S. military commander.*[32]

While the Department of State and the Department of Defense are typically the major players in projecting the American image and message globally, other government agencies—the Drug Enforcement Administration and Immigration and Customs Enforcement for example—can play significant supporting roles. The challenge is employing these assets in a coherent way, synchronizing and maximizing the value of each and delivering a communications platform that is larger than the sum of its parts. Every component of the communications team must execute its mission in a complementary fashion, each building on the other, in order to deliver seamless messages.

This presents a challenge since--as with any organization attempting to coordinate the actions of multiple entities--someone must lead. There are no easy answers here. Ultimately, the Combatant or Joint Task Force Commander and the Ambassadors in the region will have to make executive selections by consensus.

Deciding who should be in charge of a given coordination group pales in comparison to who ultimately decides what the regional messages should be and how best to deliver them. The task becomes much more difficult in a crisis situation. Since the State Department has primacy for implementing U.S. foreign policy, the Ambassador, who is the President's personal representative and senior U.S. official in a given country, directs all U.S. Government activities and personnel in that country. Military members operating under a Combatant Commander are the exception to that rule. The Ambassador is also responsible for approving U.S. Government strategy for that country, as outlined in

the mission performance plan prepared by the Embassy's country team, comprising the senior members of virtually every U.S. agency in that country.[33] In light of this, Ambassadors and State Department regional bureau chiefs should hold significant sway when deciding the strategic communications policy for a specific country or region.

A region's unique situation and requirements will drive the makeup and leadership of a supporting communications coordination group. At a minimum, representatives from the Combatant or Joint Task Force Commander, the country team or teams and other supporting government agencies will constituent the coordinating group. Both the Combatant or Joint Task Force Commander and the Ambassador(s) in the country or region should decide who will lead the group. Foreign Service officers and military officers both bring unique sets of leadership qualities to the interagency forum.

Formal personnel tasking and commensurate recognition of group members by participating agencies is crucial in ensuring the group's work not be viewed as an additional duty. Moreover, participating agencies must offer their best and brightest talent and resist the notion of retaining its "brain trust" and sending only risk-inclined, junior staffers to often far-flung locations where the security situation is at best, tenuous. In addition, the coordination group should be located as close to "edge" as possible. This means co-locating the coordination group with country teams at embassies or regional and local military command nodes.

The Defense Science Board summed their assessment of these organizational challenges as: "There is no such thing as a 'perfect' planning and coordinating structure…*the success or failure of new structures ultimately will be the people involved. But substance and structure are integrally related. Good organizations can help shape good outcomes* [emphasis added]." [34]

A case in point is the communications coordination group formed in Afghanistan in late 2003 with elements from agencies at the U.S. Embassy in Kabul and Combined Forces Command–Afghanistan (CFC-A).[35] The formation of CFC–A by the United States Central Command in the fall of 2003 and its stationing in Kabul in order to place more emphasis on political-military efforts was critical in

helping integrate diplomatic, information, economic and military operations.[36] This action ultimately set conditions for the creation of the communications coordination group.

While the communications coordination group was not a formal planning body per se, its mission, goals and objectives were essentially the same as that of a JIACG. The group's charter was to influence and synchronize the execution of external communications in support of U.S. foreign policy objectives (not to make policy), and to establish new interagency links (not to replace traditional agency chains of command).

It consisted of representatives from the Embassy's public affairs, political, economic, and cultural functional areas as well as public affairs and information operations representatives from CFC-A. While a Senior Executive Service public affairs official from the State Department's Afghanistan Reconstruction Group (reporting to then U.S. Ambassador to Afghanistan Zalmay Khalilzad) acted as leader,[37] the ranking military member was the director of public affairs for CFC–A.

The communications coordination group met weekly to discuss initiatives and events and to coordinate and synchronize supporting external communications efforts—ensuring that each agency's message was complementary and supported overall U.S. foreign policy themes. A core group, consisting of the senior State Department public affairs official, the CFC-A public affairs director and select Embassy functional area leaders, also met weekly to further refine specific themes and ensure message alignment between the Ambassador and the CFC-A commander. Other diplomatic and military officials participated depending on the situation. The core group also made routine visits to public affairs officials at the United Nations Assistance Mission to Afghanistan, the North Atlantic Treaty Organization's International Security Assistance Force, and the Afghan government to discuss the U.S. and Coalition positions on certain issues as well as to receive valuable feedback and maintain open channels of dialogue. They also established routine contact with other U.S. Embassies in the region, particularly Pakistan.

With no explicit chain of command existing between the military and Embassy staffs, the conundrum of requiring unity of effort without unity of command came into play. Ultimately the group relied on consensus building to deliver fully coordinated plans and recommendations. This was paramount in ensuring the viability of the group and the quality of its staff work.

This framework enabled the U.S. to achieve unity of effort in delivering anticipatory, coherent, mutually supporting messages. In-depth coordination between agencies within the group allowed for message synchronization in support of specific events or initiatives, maximizing their overall effect. Detailed coordination was absolutely critical in ensuring message symmetry between the Ambassador and the CFC–A commander, enabling them to essentially speak with one voice, preventing the public perception of "seams" in the U.S. and Coalition position on a given issue.

This was particularly important in dealing with Afghanistan's regional neighbors and ensured significant message repetition, critical to achieving a favorable collective memory in a range of target audiences. An example of that symmetry was the effort to articulate the U.S. position relative to Pakistan's efforts to rid the Federally Administered Tribal Areas of al-Qaeda and Taliban fighters in the spring of 2004. By April 2004, the Pakistani Frontier Corps was operating in the Tribal Areas but achieving only limited success. The Pakistan government in Islamabad was openly advocating amnesty—allowing foreign fighters to stay if they renounced violence and turned in their weapons. Seeking to pressure the Pakistan government into broader action, then U.S. Ambassador to Afghanistan, Zalmay Khalilzad, publicly chastised the Pakistanis, saying "America could not allow terrorist sanctuaries in Pakistan to fester indefinitely."[38] Ambassador Khalilzad's largely unveiled threat of direct American intervention created a torrent of criticism from Islamabad. While the Ambassador may have overstated the U.S. position with respect to direct American intervention in the Tribal Areas, public pressure still needed to be maintained on the Pakistani government. As the Coalition commander in Afghanistan, LTG Barno attempted to take a more conciliatory position while still

maintaining significant pressure on Islamabad by reiterating the U.S. stance, saying:

> *There are foreign fighters in the tribal areas who will have to be killed or captured. It's very important that the Pakistani military continue with their operations to go after the foreign fighters in particular, who in my view will not be reconciled. We have some concerns that the strategy could go in the wrong directions.*[39]

Through close interagency coordination, a more nuanced message was delivered. The theme remained the same—the U.S. expects Pakistani action in the Tribal Areas—but the message was delivered in a more palatable package. Protests from the Pakistan government largely faded.

Another attribute of the coordination group was the informational agility it delivered to both the Ambassador and the CFC–A commander. With a fully developed external communications platform, vetted through the interagency and grounded in U.S. foreign policy objectives, these two leaders were able to quickly counter pervasive enemy propaganda with metric-based examples of U.S. and Coalition efforts that were improving the lives of Afghans, rehabilitating the Afghan government and military, and rebuilding Afghan infrastructure.

One example was the Provincial Reconstruction Team (PRT) program.[40] PRTs, with their mission to extend the reach of the Afghan central government, establish security and enable infrastructure redevelopment programs on a regional scale was clearly a good news story and went a long way in countering Taliban propaganda. Often, both Ambassador Khalilzad and LTG Barno would attend the opening of a PRT, each taking the opportunity to extol the virtues of the program and its impact on Afghanistan's security situation and reconstruction. In the early spring of 2004, there was a general perception that the security situation was deteriorating in the south and east of Afghanistan. The Taliban were claiming to control parts of the region while the U.N. and a host of non-governmental organizations were routinely in the press expressing 'concerns.' The communications coordination group recommended that the opening of the Ghanzi PRT be used to focus attention on the security aspects of the PRT program, using the event

as a vehicle for improving local and regional perceptions of U.S. and Coalition efforts to secure the south and east of the country. At the opening of the Ghazni PRT in March 2004, both leaders took the opportunity to highlight the security aspects of the program. During his speech at the event and after citing a laundry list of reconstruction achievements, LTG Barno commented:

> *Wherever provincial reconstruction teams go, security follows. We're very much engaged in using those PRTs as a way to enhance security in the south and east, working in concert with our military forces stationed in the region and the Afghan government.*[41]

Echoing LTG Barno, Ambassador Khalilzad's stated:

> *Today, the Ghazni Provincial Reconstruction Team represents a milestone. The Ghazni PRT will help foster a safer, more secure Afghanistan. This PRT, like the others already established around the country, will provide security through the presence of Coalition forces while at the same time serve as an engine to jump-start regional reconstruction.*[42]

This level of message development was instrumental in enabling both leaders to react quickly to events, get ahead of the enemy's message cycle and deliver the right message at the right time—ultimately influencing perceptions in Afghanistan, across Central and South Asia, and throughout the world.

Conclusion

We have all heard it a thousand times: "perception is reality." By synchronizing the elements of interagency strategic communications, it is possible to achieve the Holy Grail—reality that equals perception. As the traditional lines between war and politics, peace and conflict, and battlefield and safety continue to blur, the need to influence the emotions, motives and objective reasoning of an array of target audiences becomes increasingly important and more difficult; while the consequences of failure become more severe.

The centralized dissemination of U.S. messages is not the answer. Political polarization, the lack of a national-level interagency external

communications strategy and the highly dynamic global information environment make the continued use of the U.S. government's current monolithic message delivery framework untenable. Only by deploying multiple regional strategic communications-centric JIACGs, each operating in synergistic fashion, each delivering messages specific to their regions while supporting broad U.S. foreign policy themes, can the U.S. expect to achieve decisive strategic effects and win the war of perceptions and ideals.

Prevailing doctrine defines strategic communication as encompassing the planning, execution, and assessment of integrated and coordinated U.S. government themes and messages that advance U.S. interests and policies through a synchronized interagency effort supported by public diplomacy, public affairs and military information operations in concert with political, economic, information and military affairs.[43] The Joint Interagency Coordination Group model can, in large measure, fulfill the doctrinal definition of strategic communication and be a viable construct for enabling regional interagency coordination and cooperation in the Fourth Generation Warfare environment. A strategic communications JIACG is absolutely crucial for each country team and Combatant or Joint Task Force Commander operating where the U.S. must achieve strategic communications synergy across the interagency and must deliver its message with high precision.

The communications coordination group that stood up in Afghanistan in 2003 serves as a successful example of applying the JIACG concept to strategic communications at a regional level. The group's success demonstrated that synchronized messages, developed and disseminated at the "edge," and tailored to specific audiences, can achieve decisive strategic effects. U.S. and Coalition efforts at maintaining public pressure on Pakistan to aggressively root out foreign fighters from the Federally Administered Tribal Areas and assuaging local Afghan fears while countering Taliban propaganda relative the perceived security situation in the south and east of Afghanistan are two examples of how this model has proved useful in enabling Ambassadors and military commanders to stay inside the enemy's message cycle, react quickly to enemy propaganda and speak with virtually one voice, "staying above the noise level of Washington."[44] The development of a

regionally focused interagency strategic communications infrastructure will, in large measure, set favorable conditions for improving how the world perceives the United States.

Section Two

Information Effects in the Physical Domain

Introduction

Dr. Jeffrey L. Groh

Professor, Information and Technology in Warfare
Department of Distance Education
U.S. Army War College

The implementation of network-centric warfare has implications for 21st century warfare in the information, cognitive, social, and physical domains. This section highlights four excellent student papers that examine potential information effects in the physical domain. "The physical domain is the traditional domain of warfare where a force is moved through time and space. It spans the land, sea, air and space environments where military forces execute the range of military operations and where the physical platforms and communications networks that connect them reside."[1] The ongoing efforts to fund, equip, and organize the network to support joint, interagency, intergovernmental, and multinational operations present strategic-level challenges and opportunities for the United States and coalition partners. The physical network is a critical enabler to achieve enhanced situational awareness and increased speed of decision. The 2006 Quadrennial Defense Review states, "The foundation for net-centric operations is the Global Information Grid (GIG), a globally interconnected, end-to-end set of trusted and protected information networks. The GIG optimizes the processes for collecting, processing, storing, disseminating, managing and sharing information within the Department and with other partners."[2] This section features U.S. Army War College Academic Year 2007 papers that examine the implications of cyber warfare and the organization, command and control, knowledge sharing, and vulnerabilities of a networked force.

Lieutenant Colonel Michael T. Barry earned the Colonel Don and Mrs. Anne Bussey Military Intelligence Writing Award for his strategy research paper. He investigates the vulnerabilities of a networked force in his paper "Always On: Achilles Heel of the Networked Force?" The author contends that, "The Achilles heel of the networked force is

that it is always-on, continuously exposed to detection." LTC Barry establishes his case for concern by presenting brief historical vignettes to include the sinking of the German battleship Bismarck in May 1941, German U-boat operations in World War II, and the Falklands campaign of 1982. He brings the argument full circle to examine today's digitized operational environment. He expertly examines the tactical, operational, and strategic implications of a robustly networked force. The paper concludes with detailed recommendations to mitigate the vulnerabilities of an always on networked force by educating and training initiatives, better understanding of adversary technology capabilities, and innovation to improve the situational awareness technologies that are not reliant on maneuver force transmissions.

Mr. Levon Anderson's paper, "Countering State-Sponsored Cyber Attacks: Who Should Lead?" looks at the pressing organizational requirements to respond to cyber attacks. This paper examines "how the United States is organized to protect cyberspace from its enemies, specifically state-sponsored and organized groups (including non-state international organizations, such as terrorist organizations). Since cyberspace is such a critical asset, the question emerges whether the Department of Homeland Security or Department of Defense should lead the cyber attack/counterattack. The author concludes with recommendations for strengthening the nation's cyber security.

Lieutenant Colonel Peter J. Beim received the U.S. Army War College Foundation writing award for his paper, "Network Operations: The Role of the Geographic Combatant Commands." He argues "The recent movement towards a more global control of NetOps, strengthening the overall role of United States Strategic Command, Joint Task Force–Global NetOps, and the Services in NetOps, has limited the Geographic Combatant Command's (GCC's) Command and Control (C2) of NetOps within their Area of Responsibility." The paper conducts a brief review of the pertinent command relationships, GCC network responsibilities, and current and emerging Service and Joint doctrine regarding network operations. The paper concludes with specific recommendations to balance the move toward centralized network command and control and GCC warfighting requirements for NetOps.

Mr. Daniel L.A. French in his paper "Winning the Peace: Building a Strategic Level Lessons Learned Program" examines the process to capture and share strategic lessons learned dealing with post-conflict operations. His argument is, "Together with Joint Forces Command, the Services are working to expand their lessons learned efforts at the operational level and to incorporate the Theater Strategic arena. These efforts remain focused on warfighting issues—Major Combat Operations. No comparable system exists at the strategic level to address post-conflict issues." The paper proposes an approach to achieve interagency and military cooperation on the collection, analysis, and sharing of strategic level lessons learned. Mr. French earned The Commandant's Award for Distinction in Research for this effort.

These papers should stimulate critical thinking about cyber warfare as well as how to organize network operations, mitigate vulnerabilities, and share knowledge in a fully networked force. Overcoming numerous obstacles to fully implement network-centric warfare (NCW) in order to leverage the effects of information in the physical domain continues to be a goal for the DoD. "Technical, cultural, and organizational impediments to accelerating the Department's progress in fully implementing NCW remain. Each can be overcome through focused efforts in areas such as network security, network interoperability, and understanding of the human and organizational behavior, and key NCW-enabling technologies."[3] The authors in this section provide sound recommendations to address several of the challenges to realize the potential of network-centric warfare.

Always On:
Achilles Heel of the Networked Force?

Lieutenant Colonel Michael T. Barry
United States Marine Corps Reserve

"We were able to monitor Israeli communications, and we used this information to adjust our planning."

—a Hezbollah commander, Lebanon, 2006[1]

The current military communications environment is characterized by radio systems which continuously transmit and receive information, resulting in near-real-time information exchange which has significantly increased battlefield situational awareness. This has been achieved, in part, through the fielding of several automated force tracking systems, such as the Force XXI Battle Command Brigade and Below/Blue Force Tracker transceiver (FBCB2-BFT) and the Movement Tracking System (MTS). The trend toward networking all warfighters with the information that enables them to rapidly assess a situation and make timely decisions continues unabated.[2]

The rapid adaptation of the these systems over the past decade, along with a variety of tactical radios, wireless data-linked Intelligence, Surveillance, and Reconnaissance (ISR) platforms, radio-controlled robots, and a growing catalog of radio-enabled battlefield sensors, reflect a fundamental change in the use of radio frequency spectrum on the modern battlefield. The fundamental change is this: the network-centric force is "always-on," which is to say, it is constantly producing radio frequency emissions in order to effectively share information in near-real-time.

Unfortunately, this networked, always-on communications environment has encouraged a relaxed, desensitized approach toward radio transmission security. Joint Publication 1-02 defines transmission security as, "The component of communications security that results from all measures designed to protect transmissions from

interception and exploitation by means other than cryptanalysis."[3] Radio communications are essential to sharing information within the battlefield communications environment and transmission security entails those actions taken to prevent friendly signals from being detected. A desensitized approach to transmission security presents potential adversaries with an opportunity to leverage commercially available technologies to passively conduct Radio Direction Finding (RDF) and radio frequency traffic analysis in order to more accurately choose the time and place to seek decisive action.

The risks assumed in forgoing transmission security might appear to be offset by the advantages gained with a networked, always-on force--especially in traditional forms of land warfare. These undisputed advantages include increased combat power, synchronized battlefield effects, speed of command, increased lethality, survivability, and responsiveness.[4] They contribute to the fact that the United States has no global peer competitor in traditional military capability.[5] The technical enabler of these advantages is the ability to transmit and receive information in near-real-time, providing commanders with enhanced battlefield situational awareness. The resulting shared situational awareness, or Common Operational Picture (COP), is derived from transmissions which are essentially continuous, or always-on.

It's unlikely that potential adversaries will allow this capability to go unchallenged. The National Military Strategy states that the "Global proliferation of a wide range of technology will affect the character of future conflict."[6] A forecast of future conflict ought necessarily to include enemy actions taken to mitigate the advantages of pervasive battlefield situational awareness made possible by persistent communications. Colin Gray states, "No polity, including the United States today, ever is permitted to enjoy for long, unchallenged, the benefits of a successful revolutionary way in warfare."[7] The challenge for U.S. forces is to ensure military effectiveness in the face of emergent styles of warfare that employ the same fundamental, globally sourced, dual-use technologies that have produced the advantages of the networked, always-on force.

In the radio frequency domain, the historical record provides ample reference to the use of passive RDF techniques in achieving decisive results. The assumption that an adversary can not, or will

not use passive RDF and spectral analysis techniques to detect the proximity and disposition of the current and future networked force, and use this knowledge to adjust his plans, may already be proving dangerously short-sighted. The Achilles heel of the networked force is that it is always-on, continuously exposed to detection. This awkward vulnerability needs to be quantified; training and education must lead to more decentralized command and control; and priority assigned to developing primarily passive, rather than transmission dependent, situational awareness communications architectures.

The Historical Experience

The same principles of transmission detection used by the U.S., its allies, and adversaries to gain military advantage in conflicts throughout the 20th century can be applied today. A review of radio communications from its inception just over a century ago reveals that the command and control advantages obtained through the use of radio were consistently challenged, and often countered, with adaptive signal detection techniques developed from the same fundamental technology.

The first documented work on the use of antennas for direction finding was conducted in 1904, just sixteen years after Heinrich Rudolf Hertz succeeded in transmitting the first radio wave.[8] Bellini and Tosi improved the work by fabricating the first RDF apparatus. As improved communications became a feature of military command and control during World War I, the refinement of RDF equipment continued. For example, the Royal Navy employed RDF to detect a critical movement of the German High Seas Fleet and subsequently committed the British fleet to battle at Jutland, achieving a decisive result. For the remainder of the war, the Royal Navy was not threatened on the high seas by the German fleet.[9] The British experience with RDF proved the value of technical discovery in an entirely new realm of science, which held promise for tremendous impact in the conduct of war.

The period between the two world wars was marked by broad technical innovation resulting in radar, wireless communications technology, and High Frequency Direction Finding (huff-duff).[10]

These advances, together with the evolution of integrated RDF techniques with operational plans, significantly influenced the conduct of operations during the Second World War. The experience of World War II suggests that whenever new capabilities were introduced in the realm of radio communications, they were soon met with counter-capability. A successfully demonstrated counter to enhanced command and control afforded by high-frequency radio communications was the employment of improved RDF capability. Furthermore, experience shows that the most effective counter to RDF was strict adherence to radio silence. When this was ignored, the ramifications often proved decisive.

In May 1941, the German battleship Bismarck posed a significant threat to British shipping in the Atlantic Ocean. After an initial confrontation with the British fleet, resulting in the loss of HMS Hood, the German battleship, slightly damaged in the confrontation, sought to break contact with pursuing British naval units. The British considered "Bismarck's destruction an imperative."[11] On May 26, 1941, the captain of the Bismarck, confident that he had eluded the British warships, transmitted a lengthy message to Berlin to report his situation. The signal was detected by British RDF assets and the Bismarck's position generally fixed. The Royal Navy converged upon the Bismarck and sank her.[12]

The Battle of the Atlantic did not end with the sinking of the Bismarck. With the entrance of the United States into the war, the sea lines of communication between the United States and Great Britain assumed strategic importance. The "wolf pack" technique employed by German submarines revealed one of the true dilemmas of emphasizing radio communications—how to weigh the value of the information obtained from transmitting against the risk to the originator of the transmission. This issue played itself out during the buildup of forces to invade the European continent.

> *Before that vast offensive could be mounted, the Allies had to win the Battle of the Atlantic. In this communications intelligence played a role of high importance. Indeed, in some respects the Battle of the Atlantic might be viewed as a duel between the Axis and the Allied cryptanalytic organizations. And while*

> *Donitz' B-Dienst had its successes, the Allied communications-intelligence agencies enjoyed the advantage of access to the extremely heavy traffic of the U-boat fleet.*
>
> *In part, this stemmed from Donitz' insistence on maintaining tactical control of his submarines so as to concentrate them in wolf packs on the richest prizes. He was aware of the danger in all the talk, but, he contended, 'The signals from the U-boats contained the information upon which was based the planning and control of those combined attacks which alone held the promise of really great success against the concentrated shipping of any enemy convoy.' His encouragement of communication led to an almost complete relaxation of radio discipline. U-boats went on the air to report a toothache on board or to congratulate a friend at headquarters on a birthday. U-boat command became 'the most gabby military organization in all the history of war.'*
>
> *Thanks to Commander Laurance F. Safford, head of OP-20-G and father of the Navy's communications-intelligence organization, the United States had, upon its entrance into the war, an Atlantic arc of high-frequency direction-finders to exploit the U-boat garrulity.*[13]

The effective counter to German U-boat strategy was to first detect a U-boat's transmissions, obtain a fix, and then to attack and sink it. The allies utilized RDF to help ensure that for the U-boats, "There was no way of avoiding a fix except by maintaining radio silence."[14] The Germans chose enhanced, centralized command and control over decentralized decisionmaking. This choice permitted allied RDF efforts to be decisive in the Battle of the Atlantic. It is worth noting the apparent and striking similarity between Grand Admiral Donitz' cited contention regarding enhanced command and control of the German U-boat fleet and the present capabilities offered by the networked, always-on force.

The period of the Cold War was marked by extraordinary advances in communications related capabilities and counter capabilities. Techniques of electronic warfare were continuously refined in order to obtain and maintain effective use of a contended electromagnetic spectrum. Pertinent to this paper is the recognition that during

this period passive monitoring and analysis of radio transmissions continued to provide valuable information. Passive monitoring of the radio frequency spectrum yielded for the United States (and likely the Soviets, too) "a wealth of useful intelligence," including the seemingly obscure yet prized information derived from merely detecting telemetry data transmitted by Soviet ballistic missiles during firing tests.[15]

The Falklands campaign of 1982 potentially marked the beginning of the current desensitized attitude toward radio transmission security. Rear Admiral Woodward, Commander of the British Task Force, made a conscious decision not to maintain radio silence in order to compensate for the absence of Airborne Early Warning capability. He judged that the always-on radar and radio communications which afforded him local situational awareness offset the recognized risks incumbent with forgoing radio silence. "I therefore assessed the balance of advantage lay with comprehensive communications between the British ships and aircraft, despite the risk of the Argentinians charting our whereabouts from them."[16]

The same sentiment was not shared by Argentinian pilots, who on May 4, 1982, flew their Exocet missile equipped Etendards, "never daring to open up on their own radios,"[17] attacked the British fleet, and succeeded in sinking HMS Sheffield.[18]

If the Falklands War, in modern times, introduced the notion that always-on, continuously emitting systems provide more security than what can be gained from maintaining radio silence, that presumption was not widely held until more than a decade later. It appears that an attitudinal change occurred coincident with the rapid increase in microprocessor technology overall, and the surge in widespread public adoption of the Internet, cellular phones, and personal digital assistants.

The U.S. consumer and business communications environment of the 1990's introduced a sense of urgency to get digitally connected. Widespread and rapidly growing use of Email, personal computing, and digital cellular telephony established new expectations for how information could and should be exchanged in a battlefield environment. Still, during the 1990's, transmission security was stressed both in

doctrinal field publications and training courses. For example, FM (Field Manual) 24-33, dated 17 July 1990, states:

> *We must not operate our radios unnecessarily. Minimizing transmissions will safeguard our radios for critical transmissions.... We must never forget that operating our radios unnecessarily increases the enemy's opportunities to gather information.*[19]

And again, citing from a 1998 radio frequency communications training manual:

> *When a message is transmitted by radio, the originator may know some of those who are receiving it, but will never know all of those who are receiving the message. You must assume that an enemy receives every transmission. Properly prepared messages using modern cryptographic systems may prevent an enemy from understanding a message. However, they can still learn a lot. For example, as time for a planned operation approaches, the number of messages transmitted increases. An enemy then knows that something will occur soon, and their forces are alerted. Strict radio silence is the main defense against radio intelligence.*[20]

In the 1990's, doctrine continued to recognize and propound the lessons learned from the experience of previous years' wars. That experience was that enemy forces could and likely would seek actionable intelligence simply by means of passively detecting, analyzing, and processing radio transmissions received on the battlefield. In spite of this doctrinal recognition, three factors during this period appear to have substantially derailed the traditional respect for transmission security. The first was Operation Desert Storm which heralded the supremacy of U.S. technology on the battlefield. The second was rising expectations, driven by the consumer electronics industry, promising that anyone, anywhere, and at anytime could be connected with the information they wanted. And the third contributing factor was the introduction of transmission techniques which, at the time, were difficult to detect with legacy RDF and spectral analysis equipment. These three factors, in concert with the previous Falklands experience, laid the foundations for creating the networked, always-on force. The next war would validate many, if not all of the benefits envisioned for that force.

Operation Iraqi Freedom, which commenced in 2003, provided an opportunity to examine the Network Centric Warfare (NCW) concept and its hypothesis that a "robustly networked force improves information sharing, collaboration, quality of information, and shared situational awareness resulting in significantly increased mission effectiveness."[21] Case studies published by the Center for Strategic Leadership discuss in rich detail the remarkable battlefield capabilities achieved through the networking of forces. These capabilities have been validated in recent combat operations in Iraq. The robustly networked force yields exceptional flexibility and combat power, even if "always-on." The studies suggest that even more combat efficiency remains to be gained by further inter-connecting forces on the battlefield. On the other hand, these case studies do not overlook the fact that enemies of the future will adapt or have access to dual-use technologies. The recent experience in Iraq suggests that future enemies must, and therefore will, seek novel, asymmetrical approaches to reduce the combat effectiveness of the networked force in a dynamic information environment.

To conclude this section on historical experience it is instructive to glance at the very recent past. In the summer of 2006, Israeli military forces conducted operations in south Lebanon. In September 2006, after hostilities had ceased, reports emerged suggesting that "Hezbollah guerrillas were able to hack into Israeli radio communications."[22] The reports proved inaccurate, or at least misleading. Hezbollah had not, apparently, intercepted and read Israeli tactical radio communications. James Bowden, the U.S. Army's senior program official for the Single-Channel Ground and Airborne Radio System (SINCGARS), clarified in an interview what actually took place:

> *It's not the hopping but the encryption that's very difficult, if not impossible, to break. What they did is use direction finding [DF] to locate frequency hoppers. In fact, they're easier to DF than conventional signals because you have more shots at it. With a commercially available system, you can probably find at least one of the frequencies.*[23]

The Israeli military has not publicly commented on the impact of Hezbollah's apparent success with RDF in these recent military operations. However, a former Israeli general, speaking on condition

of anonymity, said "Hezbollah's ability to secretly hack into military transmissions had 'disastrous' consequences for the Israeli offensive."[24] Additionally, Nizar Qader, a retired Lebanese army general, has further stated that, "The information collected by signals intercepts was being used to help direct fighters on the battlefield….These are tactics of a modern army."[25]

The experience from these recent findings show that passive RDF technologies combined with spectral analysis techniques continue to mature and adapt in tandem with modern radio transmission technologies. More revealing, perhaps, is the assertion that Hezbollah radio intelligence activities are the "tactics of a modern army." This assertion, coming as it does from an insurgent-like military organization, illuminates the present global technological environment wherein the foundations of digital command and control systems are fabricated with dual-use technologies, those that have both commercial and military applications. The digital features of the modern battlefield have become almost indistinguishable from those of consumer electronics.

Leading to the Present Situation

Mentioned above were three factors that contributed during the 1990's to a desensitized approach to transmission security. The present situation is explained by the evident convergence of military and consumer communications technology and a commitment to a style of warfare that emulates individual peacetime capability of being continually connected to digitized information.

The principle change in the communications environment over the past ten years has been the widespread adoption of digital technologies both in consumer electronics and in military command and control systems. In fact, many of these technologies are now shared, or dual-use, created by an Information Technology (IT) industry that caters to both global commercial and military markets. The CEO of Rambus, Inc., a company that provides microprocessor interface solutions for consumer computing and communications applications, recently stated, "The military used to drive electronics. Then, in the 1990's, it changed. Today, consumer electronics drives everything."[26] A benefit of incorporating consumer electronics technology into military systems is

cost savings. In an article addressing this relationship between military and consumer electronics, Geoffrey James found, "As they become more cost-conscious, defense electronics contractors are...drawing more heavily on existing commercial products to build the computing and communications infrastructure that will make NCW-enabled devices work together."[27] And time to market is another advantage. Technology acquisition and fielding is quicker if it is both familiar and on the shelf.

It is difficult to overstate the impact of this convergence of consumer and military economies as it pertains to the digitized battlefield. Not only are many of the underlying digital technologies shared, but the intellectual acumen and propensity for innovation has been globalized.[28] In the last century one could expect to find technical expertise applicable to military purposes in relatively niche locations. These were principally to be found in government agencies, select universities, and also within corporations focused on technology research and development for government use. This is no longer the situation. The commonality of computing hardware and software between military command and control systems and commercial IT ensure that skilled knowledgeable workers with innovative insight useful in military applications can be found wherever commercial IT development takes place—virtually everywhere. This produces both benefits and risks. On the one hand, military technical requirements can be met faster while incorporating complex solutions at reduced cost. Evolution of the network-centric force illustrates how fast this process is taking place. On the other hand, potential enemies have access to the same technology development life-cycle from which they, too, can produce or refine a system to enhance their warfighting effectiveness.

Nations tend to make war the way they make wealth.[29] With this thought in mind, Colin Gray offers that:

> *The current policy on transformation, which at the DOD level at least, is very much a high technology story, is a direct reflection on the trends in American society.…When America was predominately an industrial society, it waged industrial-age war on a scale in World War II that confounded foes and astonished allies. Now that America is evolving into a post-*

> *industrial society, wherein the manipulation of information is the key to prosperity, so, naturally enough, the Armed Forces must reflect that emerging reality.*[30]

A significant change over the past decade is found in the way America generates its wealth. A large cadre of corporate enterprise and technically savvy consultants has significant financial incentive to maintain a steady focus on technical solutions for meeting the challenges of modern warfare. In spite of its proven benefits, a potentially disruptive problem arises when, fixated on technology, U.S. forces become overly dependent on a particular style of warfare. A style of warfare characterized by a singular, pervasive, networked, and always-on force may be an example of this. In war, advantage can be gained from attacking a superior opponent's style of warfare. Given the historical record and the methods employed by adversaries in the Global War on Terrorism (GWOT), the American style of warfare is what enemies will seek to attack. Similar to technical methods employed by the Allies to defeat chatty German U-boats in World War II, passive RDF and spectral analysis provides asymmetrical fighters a technical avenue of approach toward defeating the American style of warfare.[31]

Vulnerabilities

The vulnerabilities evident from this discussion fall into three categories. First, a tactical vulnerability exists when enemies gain and use RDF technology for decisive effect. Second, at the operational level, a successful employment of passive RDF technology against U.S. forces exposes a vulnerability in the style of warfare U.S. forces are becoming dependent upon. And thirdly, from a strategic perspective, the disruptive employment of RDF and spectral analysis tools by potential adversaries illuminate the U.S. vulnerability of forfeiting to international competitors essential leadership in the development of key dual-use technologies.

Tactical Vulnerability

An emergent, if not already existent vulnerability for the networked, always-on force is that opposing forces will leverage the employment of

available and obtainable technology to conduct passive and moderately sophisticated RDF and spectral analysis. Employed by asymmetrical fighters, these passive measures will increase their combat effectiveness and enhance their ability to achieve decisive results while operating in complex battle environments. Spectral analysis and RDF equipment is available from manufacturers around the globe. The equipment capabilities characteristically keep pace with advances in transmission techniques.

> *Broadband radio direction-finding receiver advances instantaneously enable coverage of a large bandwidth at high speed to locate radio frequency emissions. Direction finding is a key function in electronic warfare radio reconnaissance systems. Broadband direction finders are now capable of overcoming frequency-hopping, low-probability-of-intercept and low-probability-of-detection techniques.*[32]

Historical experience shows us that valuable information can be gained through passive monitoring of the radio spectrum. The Al Qaeda Training Manual recognizes the importance of information, stating that, "Information about the enemy's intention provides early warning signs for the command, which in turn makes appropriate preparation and thwarts the enemy's opportunity." And also, that "Information benefits the Organization's command by providing information about movements of the enemy and his members."[33]

Asymmetric fighters characteristically favor passive means of gathering information. U.S. forces employ highly effective ISR assets which narrow the asymmetric fighter's options for how he can securely gather intelligence. Radio spectral analysis and RDF techniques offer a means to act passively in order to detect always-on ISR systems and combat formations while locating soft or special targets.

The position can be maintained that adherence to "radio silence" is not necessary when troops are in contact with the enemy. When forces are engaged in combat any effort to maximize speed in the decisionmaking cycle trumps concealing friendly presence from the enemy. After all, the presence of friendly forces is revealed to the enemy when they are shooting at targets. In traditional warfare, especially land warfare, this is a valid argument. However, a desensitized view toward, or worse,

a blanket dismissal of the historical experience may be short-sighted. The preferred style of warfare chosen by enemies of the United States in the GWOT is more similar to U-boat operations in the North Atlantic than maneuvering mechanized formations in open terrain. According the U.S. Marine Corps Combat Development Command's document entitled, "Marine Corps Operations in Complex and Distributed Environments,"[34] likely adversaries:

- Will distribute their operations to exploit our vulnerabilities and indirectly erode our influence
- Will try to mitigate our advantages by fighting in complex terrain (urban, mountain, jungle)
- Will seek to complicate operations by engaging in war among civilian populations

These techniques are illustrative of an adversary who does not think like the commander of a mechanized rifle regiment. This adversary will choose to fight or flee based on detecting the presence of, and if possible, the composition of the force maneuvering against them. The sum of historical experience strongly suggests that against a networked, always-on adversary, RDF technology promises a path toward decisive results on the battlefield. Given its passive nature, employment of RDF lends itself to being supportive of urban fighting, terrorist actions, and asymmetric attacks.

Operational Vulnerability

In war, dependence on any a particular style of warfare is itself a vulnerability. The current trend is toward operational and tactical dependence on the network-centric, always-on style of warfare. This dependence, combined with the aforementioned pervasive and desensitized attitude toward transmission security, has largely removed requirements to train in the absence of these systems.

And it is not only the guerrilla—the asymmetrical fighter, who does what is necessary, even illegal, to find a means to counter a competitive style of warfare. Developed nation-states find opportunity, too. Quoting from the Office of the Secretary of Defense Report to Congress on the Military Power of the Peoples Republic of China (2006):

> *China continues to employ covert and illegal means to acquire foreign military and dual-use technology. Individuals allegedly engaged in illicit technology transfers to China were arrested in the United States and Russia in the fall of 2005.*
>
> *China also continues to acquire key technologies and manufacturing methods independent of formal contracts. Industrial espionage in foreign research and production facilities and illegal transfers of technology are used to gain desired capabilities. Where technology targets remain difficult to acquire, foreign investors are attracted to China via contracts that are often written to ensure Chinese oversight, with the eventual goal of displacing foreigners from the companies brought into China.*[35]

The primary concern in the current environment is the methods cited for obtaining key technologies. These methods can readily be employed by rogue states and wealthy non-state actors seeking globally diffused technology or expertise. A style of warfare that is dependent on ubiquitous, always-on radio communications is vulnerable to being thwarted by an opposing style of warfare; a style enhanced through possession of instruments that passively detect and analyze all manner of radio frequency emissions.[36]

Strategic Vulnerability

The fact that advanced technology is being developed and obtained, legally or illegally, through access to the global digital technology knowledge-base illuminates a larger, strategic vulnerability. The networked, always-on force maintains traditional battlefield supremacy in partnership with the broader U.S. economy and in particular with the information technology industry. The IT industry is a cornerstone of the U.S. economy and displays American ingenuity and technical acumen. A looming strategic predicament is a disadvantageous position from which to compete in the globalized IT marketplace with innovative ideas. Testifying in March 2007, before the U.S. Congress, Microsoft Chairman Bill Gates stated, "The U.S. cannot maintain its economic leadership unless our work force consists of people who have the knowledge and skills needed to drive innovation….We simply cannot sustain an economy based on innovation unless our citizens are

educated in math, science and engineering."[37] Mr. Gates' comments regarding education and competitive innovation pertain to U.S. military capability. Military power made effective through dependence on technical enablers assumes preeminence in the application of math, science, and engineering. For several decades the U.S. information technology industry, to include universities and research centers, have ensured the U.S. capacity to wage war competitively; to dominate battlefields with networked information systems. However, absent an IT industry that continues to indisputably lead in innovation, reliance on technology for the effective employment of military power will prove detrimental.

A thorough discussion of the U.S. economy's influence on strategic military capabilities is beyond the scope of this paper. Suffice to say that a leading-edge indicator of the strategic challenge will be the use of advanced, dual-use technology, sourced from outside the U.S., effectively employed in exploiting the always-on vulnerability of the networked force.

Potential Exploit

A foreseeable exploit is envisioned by a non-traditional fighting organization, perhaps insurgents, who are in possession of modern RDF and spectral analysis hardware, software, and processing capacity. This fighting organization is faced with—maybe even surrounded by, a belligerent force constantly emitting radio frequency energy from every level of its organization. In this situation, two men take up temporary residence in a high-rise building near a coalition transportation hub. Over a period of time they observe and record patterns of signals (traffic analysis) and correlate these patterns with events later made public in the open media. They deduce from their observations and analysis that certain signals are present, others more pronounced, and still others disappear completely when high level U.S. political figures are passing through the transportation hub. With this intelligence, the two men are able to produce future unambiguous indicators based on real-time signal comparison in order to carry out an attack on a prominent U.S. political leader.

The example highlights what has been known since the dawn of radio: actionable intelligence can be collected and used by passively monitoring an enemy's transmissions. This intelligence can prove decisive. On a traditional battlefield, where formations maneuver against formations, detection of transmitted signals is of fleeting and often minor significance. However, for the fighter whose style of warfare necessitates he detect, avoid contact, and attack selectively; the ability to passively detect and analyze his opponent's use of the radio spectrum is of utmost significance. The asymmetrical fighter will employ passive RDF and spectral analysis against an always transmitting networked force because the opportunity exists. He exploits the opportunity in order to more effectively plan his maneuver and executes to achieve decisive effect.

Recommendations

Three recommendations are advanced which entail understanding a potential adversary's opportunity given readily available technology, educating toward decentralized command and control, and development of a situational awareness architecture that is not dependent on maneuver force transmissions.

1. Quantitative Investigation. First, a quantitative investigation must be made to demonstrate what a potential enemy can learn about U.S. forces with the same RDF and spectral analysis tools available in the global, commercial marketplace. There should be two primary objectives for this study. The first is to determine the limits of vulnerability and predict the most probable vulnerabilities an adversary will seek to exploit in order to enhance his style of warfare. These questions should be asked: "What information can be gathered using low-cost tools?" And, "What information can be gathered using moderately expensive commercial tools?" The second objective of this quantitative investigation should be to monitor the state of technological advancement in the marketplace with respect to RDF and spectral analysis technology. An accurate gauge of the level of pertinent technical diffusion throughout the marketplace is essential in order to shape training and forestall unnecessary fiscal waste.

2. Train and Educate for Passive (Listen-only) Network Connectivity. Training should not neglect the historical experience. Radio silence, i.e. transmission security, may be required to close with and destroy an illusive, technically savvy foe. Individual and unit training, in concert with doctrinal methods, should include training which emphasizes decentralized action under the guidance of a commander's intent in the absence of transmitting detectable signals. Greater responsibility will need to be assumed at lower levels of command and leadership. Decisionmaking should be decentralized. The implications are for a level of training and education that enables units and individuals to operate in a predominately passive mode with respect to the larger, networked force. These units and individuals will still be in receipt of near-real-time battlefield situational awareness information via passive receipt of the data. However, their own systems will not auto-transmit, nor will transmissions be initiated until a tactical decision cycle necessitates.

3. A Technical Solution. Technology may evolve to eliminate detectable communicative transmissions on the battlefield. Research should continue which leads to the fielding of truly covert, undetectable wave-forms for non-line-of-sight communications. But this research should not be the main effort. The global information technology environment will produce an antidote in short order given the convergence of defense and commercial related research and development in wireless technologies.

The preferred technical approach is to develop and field a primarily passive, digitized battlefield situational awareness architecture. This approach reaffirms the importance of transmission security on the battlefield, does not have to be more expensive, and can be equally effective for command and control of the networked force. The essence of this proposed architecture is that it leverages stand-off ISR capability to identify, and gather other information, about friendly forces rather than being dependent on transmissions from the units or individuals themselves. The collected data is combined and correlated and broadcast to the larger force, which in turn receives the information passively. Of course, the enemy force situation is combined and broadcast along with the ISR collected friendly force situation. The networked force

need not remain "always-on" and certainly not all of it all the time. Since much of the force will be trained, educated, and conditioned to operate in receive-only mode, vulnerabilities susceptible to exploitation by RDF and spectral analysis techniques can be minimized. With this architecture, command and control effectiveness is not reduced when maneuver units choose to maintain "radio silence." When a situation requires transmission (which might be frequently, but not "always-on") the unit or individual transmits. This primarily passive battlefield situational awareness architecture is an enabler for a professionally educated force; decentralized and controlled first through the commander's intent.

Conclusion

Historical experience, together with recent experience, serves to refresh the reality that technology is only an enabler and does not guarantee winning at war. Furthermore, when a style of warfare becomes dependent on a type of technology, as the German U-boat style of warfare became dependent on frequent radio transmissions to satisfy command and control requirements, a technical antidote is devised increasing the risk for defeat. Colin Gray warns that "The principle danger in the years immediately ahead is that U.S. Armed Forces will be so committed to their own network-centric transformation, that they fail to recognize the true character of potentially effective offsetting revolutionary change elsewhere."[38] The use of passive spectral analysis and RDF techniques by asymmetrical fighters will not represent, in and of itself, a revolutionary change, certain to offset the capabilities of the networked force. However, these techniques, adroitly employed to assist in achieving decisive effect, are indicative of a contemporary military enlightenment[39] well underway among our potential and actual adversaries. The revolutionary change is that their enlightenment finds its strength to flourish in the same global marketplace of ideas, digital technology, and innovation which has enabled ours.

Advanced military digital command and control systems are inseparably converged with the global information technology industry. Radio direction finding and spectral analysis techniques in the hands of the asymmetric fighter will present new challenges for

the American style of warfare. The capacity for innovative, creative leadership combined with genuine professional development must be strengthened and expanded. For U.S. military forces, this requires a regimen of training and education that ensures military success in the absence of always-on communications.

Countering State-Sponsored Cyber Attacks: Who Should Lead?

Mr. Levon (Rick) Anderson
United States Army

> *Our Nation's critical infrastructures consist of the physical and cyber assets of public and private institutions in several sectors: agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is the nervous system of these infrastructures--the control system of our country. Cyberspace comprises hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that make our critical infrastructures work. Thus, the healthy functioning of cyber space is essential to our economy and national security.*[1]
>
> —The National Strategy to Secure Cyberspace, 2003

What is cyberspace? How important is it to the overall United States National Strategy? The opening paragraph (cited above) in the introductory section of *The National Strategy to Secure Cyberspace* sums up the importance of cyberspace to the United States very clearly. An attack needing U.S. federal government response (counterattack) is defined as "a deliberate attempt by a state-sponsored or other organized group to destroy or threaten lives, property, the economy, and/or national security."[2] An organized-group could be any group that may pose a legitimate threat to the United States government and national security (including terrorist or insurgent organizations). An actual state-sponsored or organized group controlled cyber attack could undermine the U.S. information network infrastructure and disrupt the nation's functioning sectors—public, private, and governmental.[3] Once a cyber attack on the U.S. is determined or confirmed to have been conducted by a state-sponsored or other organized group, should the Department of Homeland Security (DHS) or Department of Defense (DoD) lead

the cyber counterattack? The purpose of this paper is to attempt to determine which federal government organization should lead the cyber attack/counterattack against state-sponsored or organized group cyber attacks on the United States homeland. It will discuss background information on cyberspace, current cyberspace roles of DHS and DoD, and other key players of cyber defense; provide a comparative analysis of DHS and DoD as lead for cyber attack/counterattack; present the results of analysis; and finish with recommendations and conclusions.

Background of Cyber Defense/Attack

The threat of a state-sponsored or organized-group (e.g., terrorist) cyber attack is a growing concern for many government and private strategists.[4] Many historians and military experts believe that in future wars, seizing and dominating information operations (including cyberspace) will be critical to winning the war. Indeed, the domination of information could be as important as dominating the air, sea and land battles today.[5] Understanding the role of cyberspace is critical to an effective national defense. We are quickly approaching an era when information systems will be being controlled, managed, and protected as weapon systems.[6] If the United States is attacked, it is a foregone conclusion that the United States will retaliate and make every attempt to seize the offense with an active defense.[7]

There is convincing evidence that other countries are already assigning a high priority to cyberspace and information warfare in their national and military strategies. "We are already at war in cyberspace," according to Lani Kass, director of the Air Force's Cyber Task Force. She claims countries and terrorists use cyberspace to wage asymmetric attacks on U.S. interests. "Countries such as China have been trying to extricate information from U.S. networks for more than a decade," Kass said. She added that "Chinese attacks on DoD networks are on the upswing, and China is now the United States' peer competitor in cyberspace."[8] China, like many other countries, including the U.S., is likely to sustain cyber attacks throughout any type of conflict (kinetic or non-kinetic). If not countered effectively, a well-planned and executed cyber attack could significantly cripple the use of a country's

critical infrastructure and could possibly provide the deciding blow for the attacker.

It is no secret that the United States has already detected preliminary cyber espionage activities from other state-sponsored or organized groups.[9] If our information systems are blatantly attacked, could we effectively defend and ultimately counterattack in a coordinated manner? This would be a huge coordinating effort. There are many security and control levels for all the Information Technology (IT) systems in the United States. Federal information systems appear to be protected by more stringent security measures than private and public systems. To improve the Nation's cyber security, the federal government may consider imposing stricter collaboration security requirements on public and private systems, as well as on state and local governments, especially those critical infrastructure systems that have national implications. These measures may be required to form a more cohesive team to fight and win the cyber war. The Hurricane Katrina incident proved our need to improve our response to emergencies at all levels.[10] A cyber war could significantly magnify the coordinating effort—nationally. The recommendation in the 2003 National Strategy to Secure Cyberspace that stated "state and local governments are encouraged to establish IT security programs for their departments and agencies, including awareness, audits, and standards"[11] seems too passive. In a major cyber attack, all U.S. citizens could be affected and almost all of them would be involved during the response and recovery/reconstruction phases of a cyber attack:

> *Cyber attacks on U.S. information networks can have serious consequences such as disrupting critical operations, causing loss of revenue and intellectual property, or loss of life. Countering such attacks requires the development of robust capabilities where they do not exist today if we are to reduce vulnerabilities and deter those with the capabilities and intent to harm our critical infrastructure.*[12]

Cyberspace is a critical component of our infrastructure; it is totally interconnected to the network and systems beyond the U.S. control and boundaries. Cyberspace's incredible global reach transcends all

perceived country or even continental borders. The U.S. has become helplessly dependent on the Internet.

> *Our economy and national security are fully dependent upon information technology and the information infrastructure. At the core of the information infrastructure upon which we depend is the Internet, a system originally designed to share unclassified research among scientists who were assumed to be uninterested in abusing the network. It is that same Internet that today connects millions of other computer networks making most of the nation's essential services and infrastructures work. These computer networks also control physical objects such as electrical transformers, trains, pipeline, pumps, chemical vats, radars, and stock markets, all of which exist beyond cyberspace.*[13]

With the outburst of globalization and the increased need to have more, better and faster service or products, IT is becoming more cumbersome and more complex than ever. This complexity creates coordination problems for any organization or country fighting the cyber war. This paper seeks to determine which U.S. organization is better equipped or positioned to lead the coordinated response to a confirmed cyber attack on U.S. information systems and critical infrastructure. Considering current roles, policies, and the criticality of cyberspace to the United States, DHS and DoD are the most likely government departments to lead the fight against a state-sponsored or organized group cyber attack.

Department of Homeland Security Role in Cyber Attack/Defense

Should DHS serve as the lead organization for cyber counterattacks against state-sponsored or organized group cyber attacks on U.S. cyber assets? The current role of the DHS is to secure the homeland—not a small task. This clearly includes the cyber war which is major part of the U.S. infrastructure. The 2002 *National Strategy for Homeland Security* seems to focus only on terrorist attacks on the homeland. Consider its definition of homeland security: "Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."[14] This somewhat limited definition was produced in 2002 shortly after the DHS was

created as a new cabinet-level department. Not all potential organized cyber attacks on the United States homeland will be conducted by terrorists. All the attention on terrorists, especially during the time the 2002 Homeland Security document was developed, may have been a significant contributing factor for this document's seemingly exclusive focus on terrorism—a very limited view of the cyber enemy or U.S. enemies in general. The U.S. must be prepared to fight the cyber war on U.S. territory against any type of adversary that threatens our national security.

The DHS mission is to protect the U.S. homeland from attack or from natural disasters. However, the cyber world is a different world—it has no rigorous boundaries. What happens when a cyber attack extends outside of the United States? Is countering such an attack still a DHS mission? There could be more than 100 federal, state, public, private, and international organizations that DHS must coordinate with to secure the homeland.[15] The DHS has established its organization as the focal point for managing U.S. domestic cyber incidents, including protecting the national critical information infrastructures. The DHS effort has focused mainly on cyber security measures. The Secretary of Homeland Security certainly has important responsibilities in cyberspace security, including developing a comprehensive national responsive plan for securing the critical infrastructures and resources of the U.S., as well as information technology and telecommunications systems (including satellites) and the physical and technological assets that support these systems.[16]

The Department of Homeland Security has been building and improving a very responsive system for sharing cyber information across the government and throughout the public and private sectors.[17] A robust system of this type must become operational as quickly as possible, no matter which federal agency leads the cyber fight against state-sponsored or organized group cyber attacks. So DHS has already assumed significant training and operational responsibilities to support the nation's cyber defense strategy, and this DHS responsive information sharing system is an integral part in the cyber defense/counterattack process. If DHS's mission area or span of control is limited to U.S. territory, can it legally conduct a cyber attack against a state-sponsored

or organized group outside of the U.S.? Or should DoD lead the cyber attack mission?

Because of its on-going national coordination and response effort, DHS will be one of the first government organizations to determine when a cyber attack has been launched.[18] Neither the DHS nor any other agency has the ability to instantly determine if an attack has been launched by an individual or by a state-sponsored organization.[19] There is no certain way to know initially when a system is experiencing normal or routine hacks by inexperience hackers (commonly called script kiddies), seasoned hackers, or organized groups that are staging a cyber-war on the United States. "The speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation-states difficult, a task which often occurs only after the fact, if at all. Therefore, the *National Strategy to Secure Cyberspace* works to reduce the U.S. vulnerability to debilitating attacks against our critical information infrastructures or the physical assets that support them."[20]

The strategy warns that "In wartime or crisis, adversaries may seek to intimidate the Nation's political leaders by attacking critical infrastructures and key economic functions or eroding public confidence in information systems."[21]

Department of Defense (DoD) Current Role in Cyber Attack on United States

The Department of Defense has steadily forged ahead of other agencies in planning for war against cyberspace adversaries. The Defense Department has been fighting the defensive cyber war with the Chinese and others and is equipped to conduct cyber attack if needed. The Department, in particular its military organizations, is dealing with the cyber espionage daily. The U.S. military has a robust information assurance program that strongly promotes the concept of "defense in depth," employing critical network systems that use the data/information security classification system effectively to reduce compromise of sensitive information. The examples that follow illustrate some of the DoD organizations that are blistering the trails in cyberspace.

A recent article, "Air Force to Create Cyber Command," described U.S. Air Force plans to create a Cyber Command to bring full-scale military operations to cyberspace, although no one knows whether the tactics and policies that the DoD currently uses to wage war will be effective on the cyber battlefield.[22] The Air Force is just one of DoD's examples of the military services' dedication to combating cyber problems.

The Joint Task Force-Global Network Operations (JTF-GNO) of the United States Strategic Command is the DoD organization chiefly responsible for operating and defending the DoD information infrastructure.[23] The JTF-GNO serves as the joint authority that coordinates and synchronizes all the military services and other DoD organizations' cyber actions. Much of the information about Computer Network Operations, which includes defense against cyber attacks and security breaches, as well as the related area of offensive computer network attack, are classified.[24]

One of the key DoD agencies for using and controlling cyberspace spectrum is the National Security Agency (NSA). NSA has a highly technical and efficient staff that supports DoD and other agencies in cyber actions. Details on the type of support to these organizations are sensitive and in some cases classified. NSA serves as a leader in computer network operations.[25] Although technically aligned with the DoD, NSA could offer some real advantages in leading the cyber war and could serve as the catalyst for merging the security-defense mission challenges between DHS, DoD, and others.

Other Key Players/Actors in Cyber War

Since information has become even more important to fighting and winning wars, it has become a viable critical vulnerability. Information dominance and superiority are now crucial to winning the war (kinetic or non-kinetic). Fighting and winning a cyber war has become a national effort. It is everyone's war.

> *Protecting the widely distributed assets of cyberspace requires the efforts of many Americans. The Federal government alone cannot sufficiently defend America's cyberspace. Our traditions of federalism and limited government require that*

> *organizations outside the federal government take the lead in many of these efforts. Every American who can contribute to securing part of cyberspace is encouraged to do so. The federal government invites the creation of, participation in public – private partnerships to raise cyber security awareness, train personnel, stimulate market forces, improve technology, identify and remediate vulnerabilities, exchange information, and plan recovery operations.*[26]

Private industry is a critical player in cyber war and plays a very important role in securing, defending, and protecting the U.S. infrastructure from cyber incidents. Industry, along with government research, will enable the U.S. to sustain its technological advantage by producing the best and most secure products. Industry will also play a key role in developing and implementing the best processes and advanced tools to combat cyber attacks. U.S. businesses must also be sensitive to national policies for preserving the technological advantage and honor the trade laws and policy on such matters as patents. The DHS has begun working with the private and public sectors on general awareness, as well as on specific issues impacting particular sectors.[27] The private sector owns and operates most of the U.S. cyberspace infrastructure.[28] Businesses are long-time partners in the effort to secure cyberspace, and many key players in the industrial sectors have developed plans to support *The National Strategy to Secure Cyberspace* by strengthening the security of their critical infrastructures.[29]

Although the private sector is an integral part of the overall cyber defense effort, more of the management burden and responsibility on active defense[30] must be assumed by the national government. Genuine defense requires the exercise of sovereign power, and implementation of active measures will have national impact.[31] The effects of cyber war on businesses could also jeopardize economic stability and disrupt the services of the personal computers of the general public.[32] Although the private sector may have better technology and excellent experienced personnel, the response to cyber attacks affecting national resources or assets must be provided to the government for monitoring, and command and control purposes in support of a national or international coordinated effort. The private sector should continue to clean or

stabilize internal systems but must follow the government's lead and advice if forensic or other evidence is solicited.

> *In general, the private sector is best equipped and structured to respond to an evolving cyber threat. There are specific instances, however, where federal government responses are most appropriate and justified. Looking inward, providing continuity if government requires ensuring the safety of its own cyber infrastructure and those assets required for supporting its essential missions and services. Externally, a government role in cyber security is warranted in cases where high transaction costs or legal barriers lead to significant coordination problems, cases in which governments operate in the absence of private sectors forces.*[33]

The general public of the United States is also a key player in protecting the nation's cyberspace. Given customer awareness training and education on the impact of a cyber attack to the U.S. infrastructure, the American public will be more inclined to do their part in this all-inclusive effort to win the cyber war. Although home computers are not considered part of the critical infrastructure, the expanse of the internet has made all systems connected to the internet possible "spoofing" targets. Spoofing occurs when hackers at all levels (including state-sponsored or organized group) actually use another person's home or office computer to hack into another computer (personal , industry, or government) or to carry a malicious code (e.g., virus, worm, etc…) payload to any other unprotected computer.[34] The malicious code could also penetrate a protected computer if the receiver thinks actions are originating from legitimate source—therefore trusted.

The DHS is working with the Department of Education and state and local governments to work with the general public (home users, students, children, and small businesses) on basic cyberspace safety and security.[35] Many believe vendors should play a more proactive role in ensuring home computers are secure. Even so, the general public must take their role seriously. But does recruiting the general public as cyber defense team members present legal concerns for the government entities involved in or leading the a cyber war?

The international community, which includes all the non-U.S. countries that are conceivably connected to the global network via the internet, is another very important player. Their roles could influence who leads the cyber fight. The only way to possibly fight and win the cyber war is to ensure at a minimum that our current allies support our effort to fight a global cyber war. The United States has recognized the importance of international involvement and commitment in cyber affairs and has engaged in several initiatives to help pave the way to fight the cyber war.[36] This issue has been made more noticeable with constant attacks by individual hackers from other countries.[37] These individual hackers could actually be fronting for a state-sponsored or organized group attack. To engage in effective dialogue with the international community on cyber war issues, the United States should first try to establish working relationships through current treaties and agreements.

It may be impossible to solve cyber incidents if the international community does not agree to share cyberspace to pursue or track cyber crime or attacks. Cooperation from the international community is critical; it will allow Internet service providers in different nations to create alliances to counter cyber crime or cyber attacks.

> *America's cyberspace joins the United States to the rest of the world. A network of networks spans the solar system and allows malicious actors on one continent to act on systems thousands of miles away. Cyber attacks cross borders at light speed, and discerning the source of malicious activity is difficult. America must be capable of safeguarding, and defending its critical systems and networks. Enabling our ability to do so requires a system of international cooperation to facilitate information sharing, reduce vulnerabilities, and deter malicious actors.*[38]

The legal policies of these cooperating states should not conflict with each other. The technical problems of pursuit and detection become more difficult if one or more of the nations involved has a legal policy that conflicts with that of the United States.[39]

Some observers claim that international cooperation such as that of the Council of Europe is very important for defending against cyber attacks and improving global cyber security. But others point out

that the treaty also contains a questionable protocol that violates the First Amendment of the U.S. Constitution.[40] Also, other laws that are being developed to address computer espionage and computer network attacks have clearly different legal characteristics. Computer network espionage, like any form of pure espionage, is not prohibited by international law,[41] but it is usually not lawful under domestic law of the targeted state. Computer network espionage usually involves very little, if any, force; it involves only as much intrusion as necessary to collect the required information from the adversary's systems.[42] Computer network attack, on the other hand, involves some kind of destruction with consequences in the physical world. Computer network attacks should be analyzed like any other use of force. Depending on the scope, duration, and intensity of the force employed, it may rise to the level of armed attack.[43]

Several U.S. interagency players are also critical for fighting and winning the cyber war and will have significant roles throughout cyber conflict. This analysis focuses primarily on what many believe are the obvious agencies (DHS and DoD) to lead the United States cyber effort against an organized cyber attack. These other key players offer some special capabilities and strategic viewpoints that must be considered when developing and assigning critical roles and responsibilities for fighting the cyber war, including the recovery/reconstruction phase. This analysis considers some of the major organizations with significant supporting roles in the cyber war, such as the Department of State (DoS) and Department of Justice (DoJ).

A case could be made for the DoS to play a lead role in reconstruction if the cyber war is fought on several international fronts. The DoS has very limited resources, some intra-departmental experience with modern cyber war technology, and possibly limited legal authority to engage in a war on U.S. territory in terms of United States Code (USC), Title 10 responsibilities which include attacking the enemy. However, cyber war pre- and post-hostilities' requirements and diplomatic functions in the international world should warrant strong consideration for DoS to assume lead role in post-hostilities cyber war, specifically the reconstruction involving international players. DoS would possibly also have the critical and dubious role (mentioned earlier) in establishing

international agreements and treaties to legally take the cyber fight across the globe. The DoS chairs the interagency International Critical Infrastructure Protection Working Group. This group serves as an interagency coordination mechanism on international cyber security matters of a bilateral, multilateral, or international nature."[44] Although the DOS will play a key role in resolving international cyber conflict and possibly a lead role in reconstruction effort, it must maintain its diplomatic advantage to remain effective as the major U.S. international political peacemaker and honest broker.

The DoJ also plays a key role in cyber security and could offer some advantages as the lead federal government agency to combat cyber crimes (individual or home-grown terrorists). Its law enforcement role, which deals with legal domestic issues related to federal statutes, provides great experience in cyber war and will be very helpful in verifying and confirming state sponsored or organized-group cyber activity. The DoJ should also play a key role in addressing all the legal problems that could be encountered in a cyber attack/counterattack. The current technological and processing experience the DoJ organizations have with national cyber defense issues also provides an excellent advantage in fighting the cyber war. However, the DoJ is not resourced or legally empowered to manage the cyber war on a large-scale national or international level for a long period of time.

This list of cyber interested agencies does not intend to be all inclusive. It primarily illustrates the magnitude and complexity of the coordination effort involved in potential cyber war. There are other key inter-agencies (i.e., Department of Commerce, Department of Treasury, Department of Transportation, and others) that are critical to the cyber war process.

Comparative Analysis: Department of Homeland Security and Department of Defense

Let's review in detail the two primary candidates this paper assumes have the best chance to lead the cyber attack/counterattack—DHS and DoD. They appear to be the two departments that should be considered to lead the cyber counterattack against a state-sponsored or organized group attack on the homeland. This paper assumes the United

States will not initiate a cyber war unless provoked, but will initiate an operational counter attack as part of a conflict or physical war declared by the President. However, this scenario includes the launching of a counterattack from a strategic defensive posture of guarding the U.S. homeland. This analysis compares two major organizations, DHS and DoD, for the lead role in the cyber counterattack against state-sponsored or organized group cyber attacks. The comparison is based primarily on four categories: resources, experience, legal status, and technology.

The DHS's mission is to secure the United States and DoD's mission is to defend the United States. There is some overlap in these organizations' responsibilities (secure vs. defend) that could create some legal and unity-of-command issues. The DHS has a disadvantage in resources (personnel and funding) compared to DoD. The DHS cyber experience of preparing some of the major players for the potential cyber war has grown considerably over the past two years according to senior DHS analysts. It has included many of the major players in recent exercises with very good results.[45] Although DoD participates in these exercises, it has not led a coordinated effort of this magnitude, which involves personnel and organizations from private industry and the public sector. Besides, DoD may have USC, Title 10 or/and USC Title 18 (Posse Comitatus) legal concerns with such a coordination effort (overseeing and law enforcement of private industry and American public computer responses). "Cyber defense on the domestic front is primarily a civilian law enforcement function which seriously limits DoD's role on cyber attack on the United States Homeland."[46]

The role of protecting the United States homeland cyber space seems to fall squarely into the realm of the DHS. Or does it? This would be a viable solution if the United States' security was only passive in nature. However, once the United States has determined it is under attack from a state sponsored or an organized group (e.g., terrorists); it will retaliate with an appropriate response.[47] The response or retaliation could be more than a return cyber attack. It could conceivably escalate into an all-out armed conflict, justified as self-defense or proportionate to loss of property or life.[48] In the cyber international legal world, there would have to be grave evidence without reasonable doubt warranting such

"drastic" measures.[49] In such a case should DHS relinquish control of cyber war to DoD, which has more resources and experience for waging war, even a cyber war?

We have noted that the DHS has a major legal role in cyber defense of the homeland from a domestic perspective. However, what is its role in responding to a state-sponsored or organized group attack? The DHS has limited resources and will depend heavily on DoD resources to fight the cyber war. The DoD's budget is about 10 times the size of DHS. The DHS would also be heavily dependent on DoD for technological support as well as relying on DoD's extensive cyber space experience. However, individual state Governors could activate and control National Guard resources through the State Adjutant General, who could coordinate cyber actions with DHS. This could alleviate DHS resource issues. This, however, will not help with legal issues where the cyber war expands across international borders via the Internet.

So to recap the analysis, DoD has a clear advantage over DHS in the matter of resources (i.e., Guard, Reserve and Active forces and budget), technical operational experience (daily attacks/defense), and technological capabilities. Although not involved extensively with external coordination efforts, DoD has a very effective internal cyber response system that does do some coordination with external sources. It brings experience and process maturity in teamwork, collaboration, and command and control to the cyber war. The DoD will also have the most advanced technological equipment used for combating cyber attacks. However, as illustrated earlier, DoD may have some legal hurdles to deal with when active-duty forces fight a cyber war on the homeland, especially if most of the resources reside with the active-duty force whose domestic activities may be restricted by Title 10 (Insurrection) or/and Title 18 (Posse Comitatus).[50] How will DoD or DHS legally control or give orders to their U.S. private business and citizen partners during cyber war? Should a cyber war on the U.S. be fought in compliance with the same principles, policies, and laws as an armed war on U.S. soil? Consider the following scenario regarding DoD's legal issues if armed and cyber wars were treated the same:

> *If circumstances warrant, the President or the Secretary of Defense may direct military forces and assets to intercept and defeat threats on U.S. territory. When conducting land defense missions on U.S. territory, DoD does so as a core, warfighting mission, fulfilling the Commander in Chief's Constitutional obligation to defend the nation. To fulfill this responsibility, DoD will ensure the availability of appropriately sized, trained, equipped, and ready forces. Currently, this capability is provided by quick reaction forces (QRFs) and rapid reaction forces (RRFs).*[51]

This scenario concludes that if all wars (kinetic and non-kinetic) were waged the same DoD could legally lead the cyber attack against state-sponsored or organized groups on the U.S homeland. However, as currently understood DHS has slight advantage in the legal aspects of leading the cyber fight on the homeland. DoD has a clear advantage on all other criteria—resources, experience, and technology for leading the war. Consider also the matter of command and control: DHS would probably have an easier time communicating with the private and public sectors since this is part of their current operations. On the other hand, DoD, although with more experience in command and control function, faces operational and legal issues in its efforts to coordinate with or manage public or private sector assets.

Results of Analysis between DHS and DoD for Organized or State-Sponsored Attack

Based on the analysis above, DoD is better resourced and positioned to lead the cyber war during an attack from state-sponsored or organized group adversaries using cyber capability. However, other major players must be involved and provide support as they would in any armed conflict.[52] Based on the foregoing criteria, DoD seems to be the logical choice to lead the effort against an attack. However, one key issue is DoD's legal status in leading a war effort that conceivably includes private industry and the general U.S. public. There are also issues regarding use of international cyberspace which we do not own.

Once the organized cyber attack has been contained or rebuffed, DoD seems to be the most logical department to lead the cyber

counterattack based on the most experience, more advanced technology, and the most resources (money and people). The clean-up and on-going defensive posture must be maintained even after the United States goes on the attack. Resource issues and warfighting experience are the most limiting factors for using DHS as the lead in a cyber counterattack against state sponsored or organized group attacks. However, as noted earlier, the legal issues and coordination with private and public sectors favor the DHS.

The DoD should take full advantage of DHS's role to secure the homeland and control the other players (private and public) and interagency partners. The robust response system DHS currently has in place and continues to update will be critical in helping to control and monitor the cyber challenges affecting the government, businesses and the general public.[53] This DHS role may be the most important part of the cyber warfare process. However, designating the DoD as the overall lead element during actual attack will better facilitate overall command and control and unity of effort. Total commitment by all responsible agencies is needed and expected to win the cyber war.

Recommendations

The DoD should lead the effort during a cyber attack or the hostility phase of the cyber war. Although time is of the essence, careful consideration and actual validation of enemy cyber attack must be confirmed before performing a counterattack. Once the enemy cyber attack has been confirmed the U.S. must take immediate and appropriate action.[54] The DoD, the DHS, and the DoS should serve as main agencies (with dedicated support from others; some listed in key players' paragraph above) to develop a comprehensive plan for three stages of the cyber war: pre-hostility, hostility, and post-hostility. Current interagency and external exercises conducted by DHS need to be expanded to include all players (including international community when feasible) through all stages of cyber war. Roles and responsibilities among the three major players (and others as well) must be carefully defined in specific detail as soon as practical. Also, the seamless transition among each as lead organization (DoD, DHS, and DoS) through the different phases of the cyber war must be planned and

exercised/rehearsed extensively. All three agencies will be intricately involved throughout each of the major stages; they must work as a team in support or lead roles. This collaborative effort will be met with legal challenges during a cyber war—nationally as well as internationally.[55] Legal experts in DoD, DHS, and DoS in coordination with DoJ should anticipate and address these legal concerns now. This critical planning effort must begin, before a "Pearl Harbor" type cyber attack is launched. International collaboration efforts must continue and cyberspace agreements or/and treaties developed soonest. Because of the complexities of cyberspace, this effort could be even more involved than "fly over" international requirements for military or commercial air space.

Conclusion/Summary

Cyber war should no longer be regarded as a fictitious event. It is a real potential wartime dilemma that must be taken seriously by all Americans and the international community in general. The effects of a cyber war, although not as deadly as a nuclear war or other weapons of mass destruction, could create similar catastrophic results. The fact that an all-out cyber war could potentially affect every home and every work place in America; seriously impact our economy; cripple our infrastructure (lights, power, energy, etc.); disrupt our military forces; and trigger many other devastating effects, makes it a critical concern for America.[56] The *National Strategy to Secure Cyber Space* states "securing cyberspace is a difficult strategic challenge that requires a coordinated and focused effort from our entire society—the Federal, state and local governments, the private sector and the American people."[57] Several U.S. agencies are currently working the very important cyber issues. However, to most effectively counter a cyber attack, the United States must focus its efforts by assuring command and control and unity of effort in cyber warfighting.

The cyber war's primary players, namely DHS, DoD, and DoS (if international cyber space reconstruction is warranted) must promote unity of command/effort; they must seamlessly transfer the lead role among one another as required for conducting defensive, offensive, and international cyber actions. The DHS should lead the U.S. national

reconstruction effort for the homeland. The U.S. cannot afford to wait for a state-sponsored or organized group cyber attack to happen to work out the very complex coordination functions and all legal implications of cyber security. The lead agencies for the various phases of cyber security should be designated quickly.

National strategic leaders should focus on the very aggressive response plan and exercises implemented by the DHS. This plan includes all the players—government, businesses, the American people, and even some international countries. Many of the businesses and government agencies have local, national, and international experience. All involved parties must continually maintain the defense, with DHS as the major coordinator for the homeland assets. All of the players need to work closely together and fix legal (domestic and international), communications, and coordination issues. The DoD should have the overall lead for the counterattack effort; the DHS should provide strong homeland cyber defensive support while maintaining the control of the complex national coordination process; and the DoS should assume lead of the reconstruction effort if international players involved. In the event of a cyber war, the roles of the supported and/or supporting commands among the major players must be transparent and confidently executed. Time is of the essence. Our international, national, state, and local policies must continue to emphasize protection of this very critical information attribute called cyberspace.

Network Operations: The Role of the Geographic Combatant Commands

Lieutenant Colonel Peter J. Beim
United States Army

Achieving the full potential of net-centricity requires viewing information as an enterprise asset to be shared and as a weapon system to be protected.

—2006 Quadrennial Defense Review Report

Who decides how the United States deploys information assets, the priority of emplacement of those assets and what actions are taken to secure the Global Information Grid (GIG) and those Joint and Service unique systems riding on it: the Services, the Geographic Combatant Commanders (GCCs), Joint Task Force–Global NetOps (JTF-GNO)? For the last few years that debate has raged in the Network Operations (NetOps) community with the pendulum swinging between a global vice Geographic CCDR focus.

Imagine the following scenario. The United States announces the decision to deploy and begins flowing forces in support of an operation in XCOM's theater.[1] Individual Services begin making decisions on how the information infrastructure will be emplaced to support the operation. An adversary begins to infiltrate key military systems supporting the deployment of military forces. While the adversary is unable to completely mask its efforts, the scope of the intrusion is underestimated as these incidents are all worked within Service channels. Connection requests begin flooding commercial websites, including those that support friendly logistics efforts, rendering them inoperative. XCOM takes action to change the Information Condition in its Area of Responsibility (AOR) affecting systems outside of its theater. A large number of viruses begin to wreck havoc on the Internet and quickly begin to infect Department of Defense (DoD) systems. Discussions begin within the JTF-GNO on whether or not

to disconnect the military points of presence from the Internet but the Services raise concerns over the Department's ability to continue to conduct logistical operations with commercial vendors.[2] XCOM is unable to ascertain the status of its theater networks and is worried about whether or not the GIG itself is secure. XCOM becomes concerned over its ability to prosecute the mission assigned to it.

The movement towards a more global control of NetOps, strengthening the overall role of United States Strategic Command (STRATCOM), JTF-GNO, and the Services in NetOps, has limited the Geographic Combatant Command's Command and Control (C2) of NetOps within their AOR. The centralization the Service portions of the GIG impairs the GCC's visibility of the GIG and their ability to support operations within their AOR. This paper will review existing command relationships, Geographic CCDR responsibilities, lines of operations and command relationships; existing and emerging Joint and Service doctrine and specific case studies and lay out recommendations for the role of the Geographic Combatant Command in NetOps C2.

The NetOps Environment

Command and Control of NetOps is a concept that has been evolving over the past decade. Each of the Services, the GCCs and the JTF-GNO has changed their organization and focus for NetOps and each has a stake in the outcome of this issue. To really understand why the NetOps role of the GCCs is an issue, one has to understand where the operations are taking place, what NetOps really is, how each of the organizations involved in NetOps is structured to perform their mission and the current C2 constructs.

Just what are we talking about; what is the GIG? As defined by DoD Directive 8100.1, it consists of the "globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to war fighters, policy makers, and support personnel." This includes government-owned along with leased communications and information systems and services, as well all software, security, services and anything else necessary to operate and secure the GIG, as well as the National Security Systems

as defined in section 5142 of the Clinger-Cohen Act of 1996.[3] By this definition, the GIG encompasses all DoD and National Security information systems at all levels, from tactical to strategic, as well as the interconnecting communications systems.

Most of the discussions on C2 of GIG NetOps center on defense of the GIG network, but NetOps encompass much more than that. NetOps include all actions taken to accomplish the three essential tasks of Enterprise Management, Network Defense, and Content Management, and are intended to provide assured net-centric services across strategic, operational and tactical boundaries in support of DoD's full spectrum of warfighting, intelligence and business missions.[4]

- Enterprise Management is the actual operation of the GIG. It is the technology, processes, and policy necessary to effectively operate the systems and networks that comprise the GIG and includes Enterprise Services Management, Systems Management, Network Management, Satellite Communications Management, and Electromagnetic Spectrum Management.[5]

- Content Management refers to the information itself on the GIG. It ensures information is available to users, operators, and decision makers in a timely manner. Content Management consists of the services that enable discovery, access, delivery, storage and integration of content on the GIG.[6]

- Network Defense is the protection of the GIG and all of the information that moves and resides on it. It is the policies, procedures, programs, and operations that protect the GIG and includes interagency coordination as required. It includes responsibilities for Information Assurance, Computer Network Defense, Computer Network Defense Response Actions and Critical Infrastructure Protection in defense of the GIG.[7]

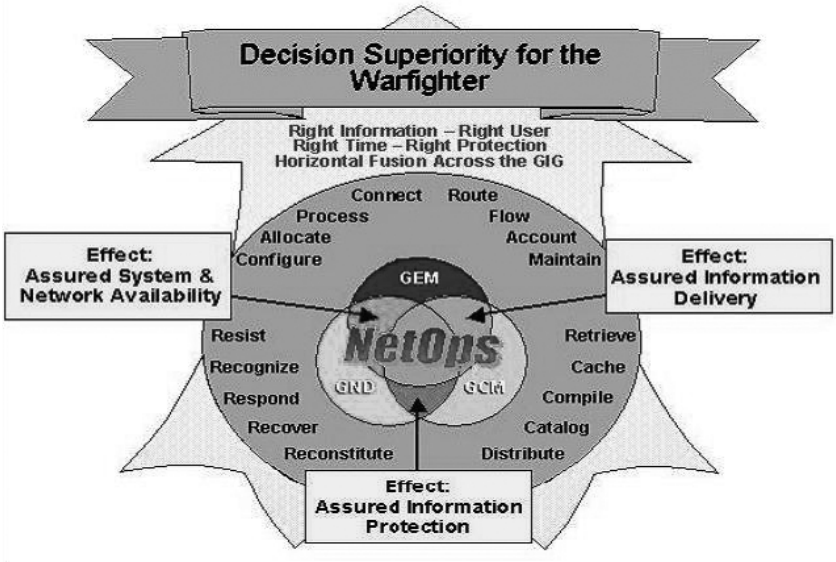

Figure 1: JTF-GNO NetOps Construct[8]

Now that the basic constructs of NetOps have been reviewed, the next step is to look at how each of the organizations involved in NetOps is structured to perform their mission. The key players in this discussion are the Services, the Geographic Combatant Commanders (CCDRs) and the JTF-GNO. All have been evolving their structures to meet the changing requirements as well as the changing threat.

The Services have been developing their NetOps missions and structures to meet the growing requirement for bandwidth, access to information, and control and defense of their portion of the GIG. Ten years ago all of the Services maintained some variation of regional control of their NetOps, but that has evolved into more centralized control. The Services have not implemented nor centralized NetOps in the same way. It is essential to understand how they are structured in order to understand why C2 of NetOps has become contentious.

Army NetOps Command and Control

The Army's focus has changed the least of all the Services. The Army continues to maintain organizations, now called the Theater NetOps and Security Centers (TNOSC), which are responsible for NetOps in

each GCC. The Army operates a single Global NetOps and Security Center (GNOSC) to which all the TNOSC report. The GNOSC has Technical Control (TECHCON) of all of the TNOSCs, but the TNOSCs belong to the Geographic CCDRs and are controlled by the Theater Network Command, typically the theater signal brigade under the control of the Army Service Component Command in the theater.

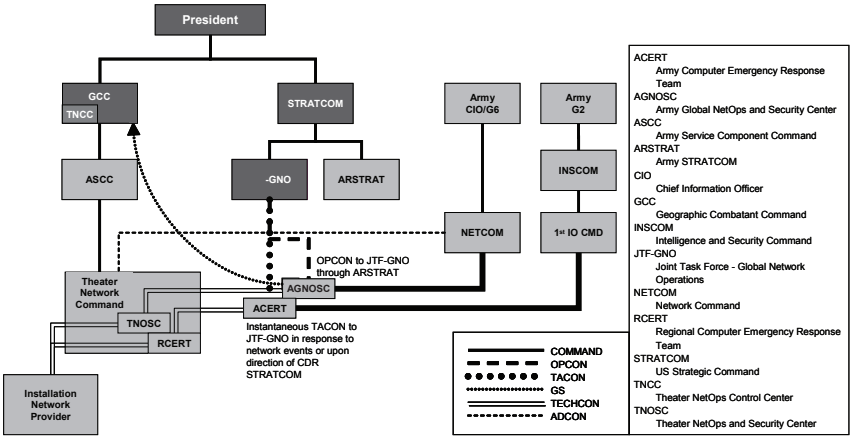

Figure 2: Army NetOps Structure[9]

The GNOSC provides NetOps Enterprise technical direction to the respective theaters while there is a theater NetOps presence that directs/controls NetOps in that theater. U.S. Army Network Command/9th Signal Command has technical and administrative control of the GNOSC, but the GNOSC is under operational control (OPCON) of STRATCOM through its Army element.

Air Force Command and Control

Taking a different approach, the Air Force has shifted its emphasis away from Major Command (MAJCOM) NetOps and Security Centers (NOSCs) to Integrated NetOps and Security Centers (I-NOSCs). Unlike the Army whose TNOSC are in each of the Geographic CCDR's theater and are assigned and report to the Geographic CCDR, the Air Force's I-NOSCs are not one for one with the Geographic CCDRs and report only to the Air Force NetOps Center (AFNOC) which is the Air Force version of the GNOSC. The Air Force realizes that the

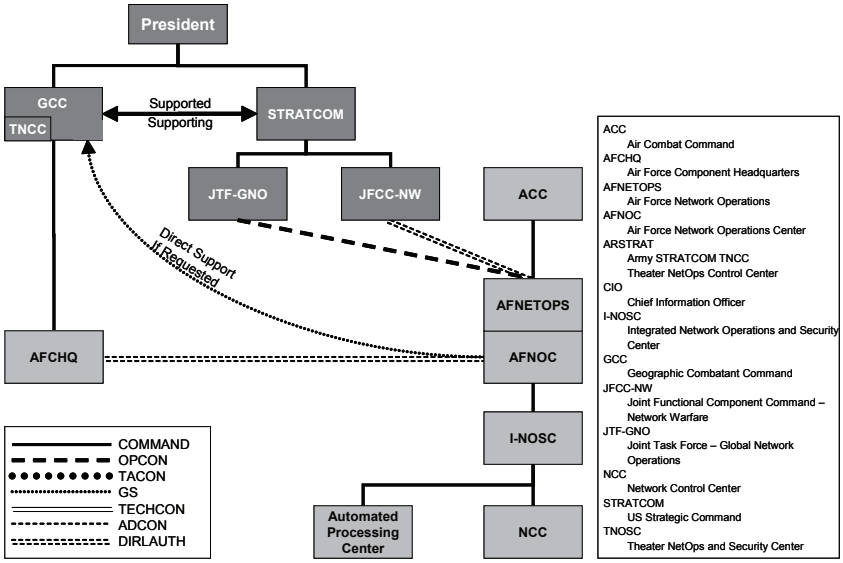

Figure 3: Air Force NetOps Structure[10]

Geographic CCDR must still be able to direct network activities within their AOR and has established a General Support relationship between the AFNOC and each GCC and established dedicated GCC liaison cells within the AFNOC.[11] Additionally, the Air Force has given the MAJCOMs the latitude to establish Communications Control Centers in their theaters to serve as the focal point for interaction between AFNOC and their respective CCDR.[12]

Navy NetOps Command and Control

The Navy, like the Air Force, has moved away from a regional focus to their NetOps. They have replaced their regional Navy Computer and Telecommunications Master Stations (NCTMS) with two Regional NOSCs (RNOSCs) under the Navy GNOSC (NAVGNOSC) to support all Navy NetOps world-wide. As much of their NetOps is conducted afloat, the Navy has established the Fleet NetOps Centers (NOCs), collocated with the two RNOSCs in the continental United States (CONUS) or with the NCTMS located in Naples and Bahrain. The Fleet NOCs are the tactical entry points for fleets operating in their operations area and provide them with all voice, video, data and network services, passing the fleet from one Fleet NOC to the next

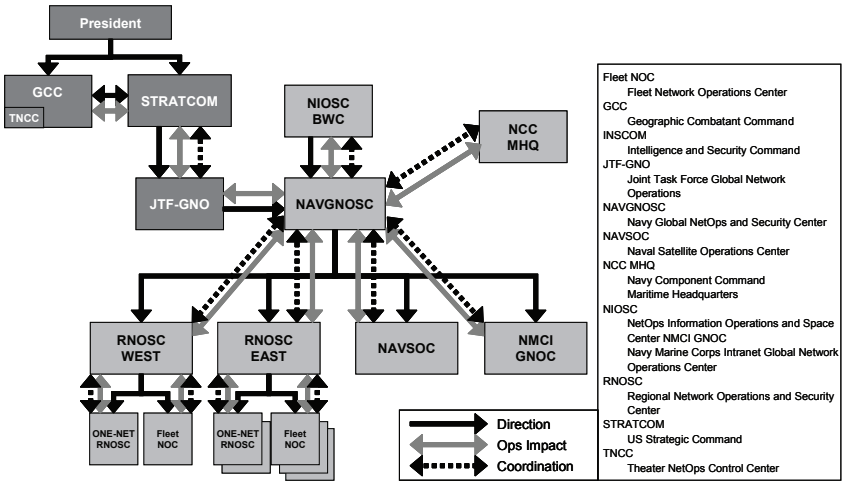

Figure 4: Navy NetOps Structure[13]

as it transits their operating areas.[14] The majority of their unclassified networks are run by contractors either under the Navy Marine Corps Internet (NMCI) contract in CONUS or the outside of CONUS (OCONUS) Navy Enterprise Network (ONE NET). To deal with this in the United States, the Navy established the NMCI Global NetOps Center (GNOC) to provide operational direction to the NMCI contractor for the Navy portion of the NMCI. OCONUS, they established TNOSCs that report directly to the RNOSCs responsible for their respective area. These TNOSCs are not assigned to the GCC in whose theater they operate.[15]

The basic organization to support global Navy NetOps is the NAVGNOSC and the East and West RNOSCs. The NAVGNOSC integrates separate common operational pictures from the Navy RNOSCs, the NMCI GNOC, and the Naval Satellite Operations Center (NAVSOC) to provide global C2 for networks and situational awareness to the JTF-GNO.[16] The Navy, unlike the Army, does not maintain a NetOps force assigned to the GCC. The support relationship established by JTF-GNO between the Services and the GCC does not enable the GCC to direct actions on the Navy portion of the GIG in their AOR. Any actions the GCC requires must be requested through the NAVGNOSC.

Geographic Combatant Command NetOps Command and Control

While none of the GCCs are organized exactly the same for NetOps within their AOR, they all have the same basic characteristics. Each GCC has established a Theater NetOps Control Center (TNCC) and has a Theater NetOps Center (TNC) run by Defense Information Systems Agency (DISA). None of the TNCCs are identical. U.S. Central Command (CENTCOM) has combined their TNCC with the DISA TNC and dubbed it the Central Region Theater NetOps Center while U.S. European Command (EUCOM) established a Theater Communication Control Center, which works for the J3 instead of the J6.[17, 18] But even with these differences, all the TNCCs are used by the GCCs for the C2 of the portion of the GIG in their AOR (also referred to as the Theater Information Grid [TIG]).

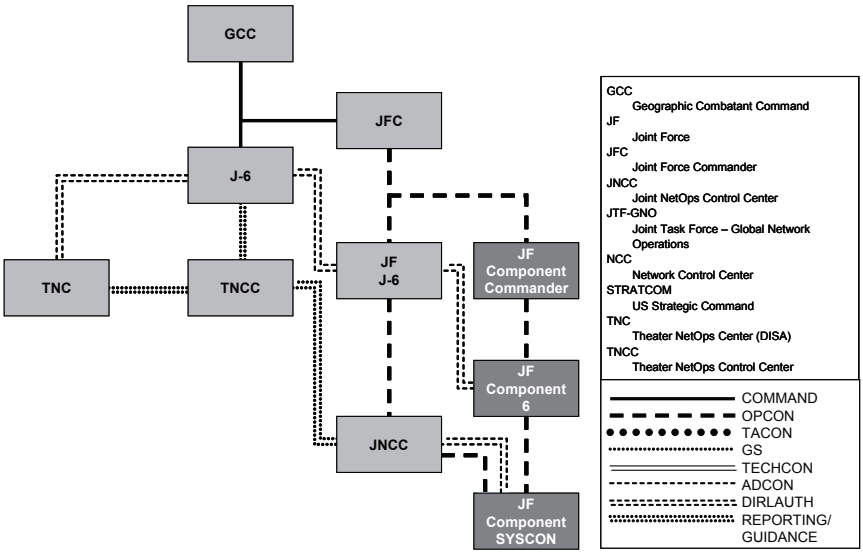

Figure 5: GCC NetOps Structure[19]

The TNCCs are the CGG's lead for prioritizing and directing theater GIG assets and resources in support of their missions and are the theater interface with DISA, the Services and JTF-GNO.[20] They monitor the status of their TIG through interaction with the TNC and the TNOSCs and determine the operational impact of proposed JTF-GNO actions. The TNCCs determine the operational impact of major

degradations and outages, and lead and direct TNC and TNOSCs responses to them in support of operational priorities. When there are no Service TNOSCs in Theater, the TNCC coordinates directly with the Service GNOSC for actions required by the GCC.

U.S. Northern Command (NORTHCOM) is in a unique position. While it is a GCC with an assigned AOR, most of the forces within its AOR, to include the NetOps forces, do not belong to NORTHCOM, but rather belong to U.S. Joint Forces Command (JFCOM) for Global Force Management. NORTHCOM does have a TNCC and component forces like the other GCCs, but those component forces have not established TNOSCs and so NORTHCOM must rely on the General Support provided by the Service NOSCs. This leaves NORTHCOM in a position where it is responsible for conducting operations within its AOR, but does not have visibility on its TIG nor the authority to direct actions on it.

STRATCOM NetOps Command and Control

Just as the Services and Combatant Commands have evolved their NetOps constructs, so has the DoD. For many years, there was no centralized control of Department NetOps. But in 1997 the Department conducted the Eligible Receiver exercise and found DoD networks vulnerable and the Combatant Commands, Services and Defense Agencies (CC/S/A) unable to coordinate a response.[21] That prompted the DISA to create an entity that would eventually become today's JTF-GNO charged with the operations and defense of the GIG.

JTF-GNO's C2 of NetOps has likewise developed. Prior to the current Unified Command Plan (UCP), C2 of NetOps was in the hands of the CCDRs who had oversight of component network management capabilities, while providing situational awareness of the GIG.[22] The initial version of the NetOps concept of operations (CONOPS) continued to focus on GCC control of NetOps within their AOR, stating that for theater issues, "Combatant Commanders will exercise their authority over forces assigned, including the authority to prioritize and direct changes in the GIG where and when appropriate in support of their missions....Combatant Commanders will exercise OPCON of their assigned NetOps forces and TACON of the TNC

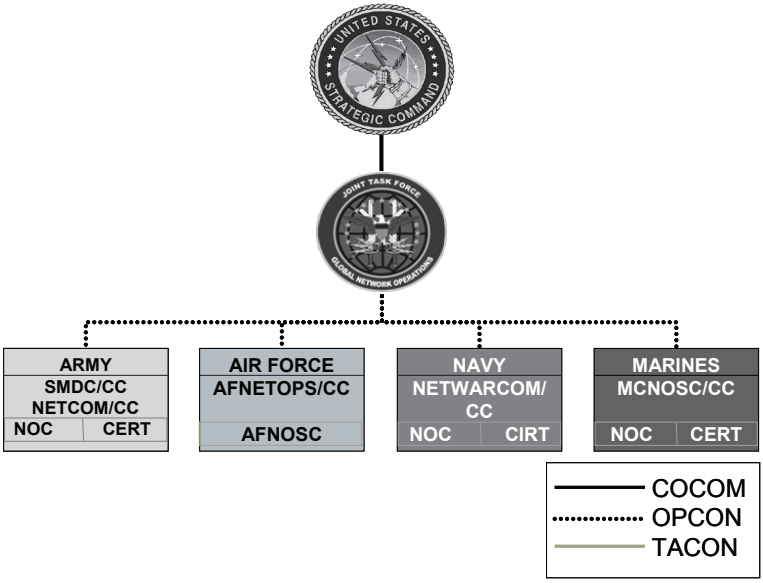

Figure 6: JTF-GNO NetOps Structure[23]

for Theater NetOps issues and will establish operational priorities for and assessments of NetOps actions in support of their missions."[24] Even for global issues, the initial CONOPS had JTF-GNO directing actions through the TNCCs of the Geographic CCDRs.

Subsequent versions of the CONOPS changed that focus. JTF-GNO has moved to a more global C2 architecture, strengthening the overall role of STRATCOM, JTF-GNO, and the Services in NetOps. JTF-GNO established three situational constructs in the CONOPS for NetOps C2: Global, Theater, and Non-Global. The determination of which construct to use is based on entities affected and the capability of the theater affected. This C2 structure is applied by event and leads to the possibility of a Geographic Combatant Command with multiple NetOps events occurring being simultaneously supported and supporting; sometimes in the chain of command for what is occurring and sometimes bypassed.[25]

Global Events

Global Events are activities that have the potential to affect the operational readiness of the GIG writ large and require coordination between affected CC/S/A.[26] The Strategic Command (STRATCOM)

Commander has the discretion to declare an event global any time activities cross a Geographic Combatant Command boundary, affects multiple combatant commands, affects other DoD Agencies or is beyond the GCC's capabilities.[27] Global Events include rapid spread of malicious code, allocation of satellite commuications (SATCOM) capabilities, loss of enterprise applications or any other NetOps event clearly not restricted to a single theater.

For Global Events STRATCOM is the supported command, issuing orders and direction through JTF-GNO to the CC/S/As.[28] JTF-GNO tasks its Service NetOps components to support the execution of global NetOps and issue direction directly from JTF-GNO to their respective Service NetOps forces around the globe. It is important to note that this direction does not go through the GCCs to the NetOps forces in their theaters.

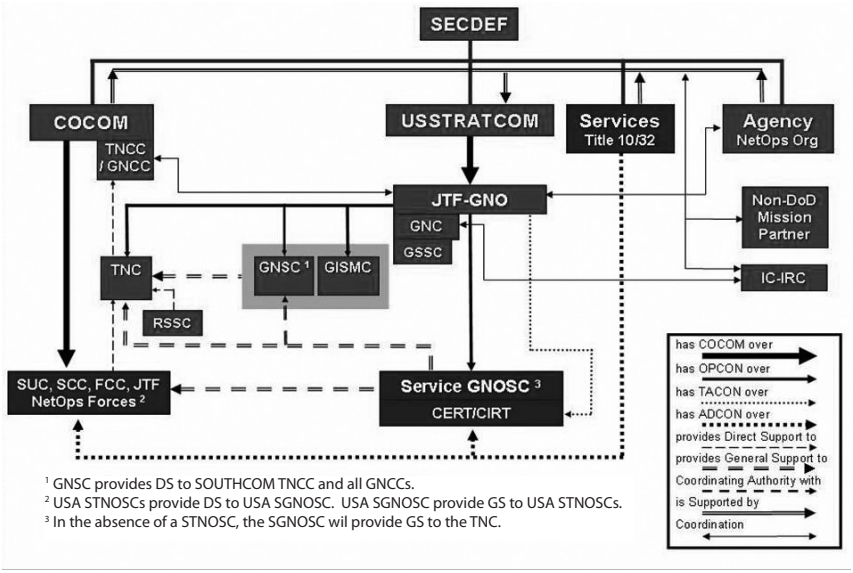

Figure 7: JTF-GNO C2 for Global Events[29]

While this supported relationship gives the STRATCOM Commander global authority, the CONOPS is quick to point out that it does not negate the CCDR's authority over NetOps forces assigned in the UCP.[30] JTF-GNO Service NetOps components are tasked to support the execution of operating and defending against global and non-global NetOps events, while synchronizing actions with affected

CCDRs and their respective components.[31] The CONOPS requires the CC/S/As to lead their respective responses to global NetOps events in accordance with STRATCOM and JTF-GNO direction.[32]

The CONOPS, as well as historical data maintained by JTF-GNO, acknowledges that most NetOps events begin in a local enclave that is under the control of the respective Geographic CCDR.[33] Properly handled at the local level, these events never become Global Events.

Theater Events

Theater Events are activities occurring within a theater that have the potential to affect the operations in only that theater. This is the major distinction between Global and Theater Events. The affected GCC becomes the supported command for all activities related to that event and STRATCOM assumes the role of a supporting command.[34] JTF-GNO Service NetOps components provide support to the GCC through their Service TNOSCs. If a Service does not have a TNOSC, the Service GNOSCs provides General Support (GS) to the TNCC. Providing General vice Direct Support means the GCC cannot direct actions of the Service GNOSCs on actions to take in their theater.[35]

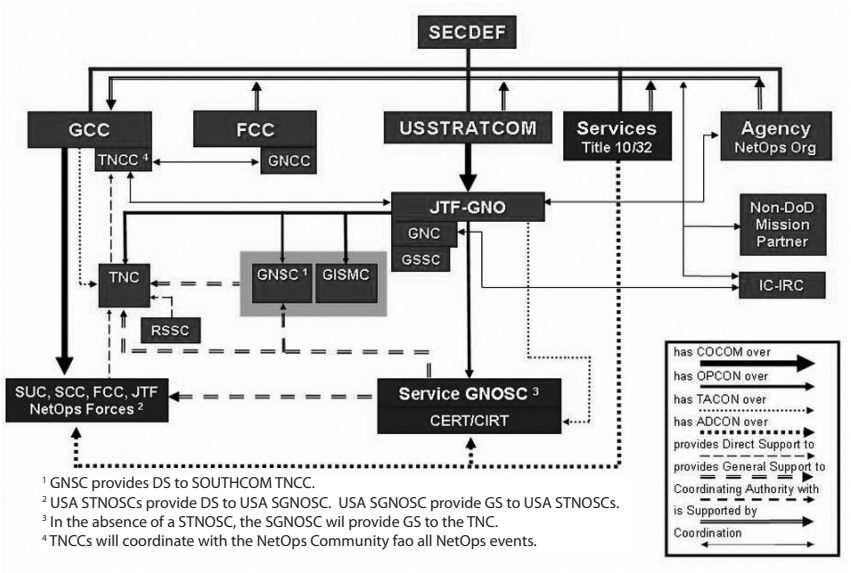

Figure 8: JTF-GNO C2 for Theater Events[36]

Non-Global Events

Non-Global Events are activities that affect Functional Combatant Commands, unassigned Title 10 Service forces or defense agencies. Since these forces have no AOR of their own, these events are considered neither global nor theater in nature. For Non-Global Events, Commander STRATCOM is the supported commander and JTF-GNO provides GS to the affected Functional CC/S/As as required. Non-Global Events most often occur within U.S NORTHCOM's AOR because that is where the affected forces and organizations are located. For the purposes of C2 discussions, Non-Global Events are the same as Global Events.[37]

Competing C2 Requirements

Service Requirements

Although there is not one single consolidated Service position, there is a consistent theme between the Services for the most efficient and cost-effective method of controlling their NetOps. Services, in accordance with their Title X responsibilities, have established unique networks, applications, and tools in support of their needs and connected them to the GIG. Each of the Services has a responsibility to operate their portion of GIG and this requires some degree of centralization of their NetOps along Service lines in order to achieve the desired efficiencies and fiscal return on investment.

The primary argument for centralizing control of the GIG is the global nature of NetOps. The Department's net-centric goals of improved military situational awareness and significantly shortened decision-making cycles can only be achieved through horizontal fusion of the networks and enterprise services all of which requires centralized control.[38] The most recent Quadrennial Defense Review report points to the need to "cut across legacy stove-piped systems" in order to achieve net-centricity.[39]

To make the best use of scarce resources, they must be committed when and where needed and this requires a global focus. Allocation of satellite bandwidth, Standardized Tactical Entry Point sites, bandwidth,

and NetOps forces themselves to support a particular mission must be done with an understanding of the global implications. From a Service perspective, centralization and enterprise management flattens the force structure required to operate and defend their networks.

Combat operations conducted by Geographic CCDRs no longer occur strictly within their own AOR. Ground forces in combat routinely reach back to remote Unmanned Aerial Vehicle pilots in CONUS to direct aircraft in support of their operations.[40] As the Prompt Global Strike program develops, commanders will be able to call for conventional strikes by weapons systems based far outside of their Area of Operation (AO).[41]

The Navy points out that its very nature is global and it has units constantly crossing Combatant Command boundaries. A Carrier Strike Group when deployed, for example, may not be all in one theater at all times. Additionally, actions taken by CCDRs on a theater level can have global implications. A change in network defense posture may have staggering financial costs for a Service Internet, but Combatant Commands may not have visibility on these kinds of ramifications.[42]

The nature of the threat to DoD networks is global as well. An enemy cannot easily attack physical infrastructure on opposite sides of the globe. In cyberspace, that occurs routinely. Information on attacks must be shared rapidly globally to ensure that methods used by attackers can be identified and defended against throughout the GIG. Intrusions, even failed intrusions, which may seem trivial on an individual basis, may show a larger pattern of intent when laid against the global backdrop of the GIG. Virus outbreaks by their very nature have global implications for the GIG. Once again, failure to recognize the global implications can have significant impact.[43]

The Navy stresses that there is no such thing as a theater view; all efforts in regards to NetOps must be global.[44] Their argument is that in fighting the network there are no geographic boundaries, the battlespace is shared by all of the DoD equally, and that to gain information superiority the DoD must be able to maneuver and mass effects by sharing information rapidly and globally.

Additionally, both the Air Force and Navy point out that NetOps forces are not apportioned to the CCDRs. Neither the Air Force nor the Navy has NetOps organizations (e.g. Service TNOSC) in a CCDR's AOR and the majority of their NetOps forces in a theater are simply installers and maintainers. Finally, they both note that the only reference in official documents to a CCDR with responsibility for the GIG is STRATCOM.

GCC Requirements

For the GCCs there are two main concerns regarding C2 of NetOps. First is the need for timely control of their TIG. Second is the need to operate their network as a weapon system to allow commanders to fight the network jointly through the full spectrum from routine daily operations to full-scale combat.

The Services, in the conduct of their Title X duties, have developed Service-unique solutions to support Service-unique missions. Each Service or agency organizes their NetOps forces in the manner they believe provides the most effective and efficient use of scarce resources. The GIG, however, is not a Service specific construct but a joint construct. The stove-piped systems and the method by which Services are deploying them degrade the effectiveness of the TIGs. When the Army developed a secure Internet Protocol (IP) phone solution, Secure Voice over IP (S-VoIP), ahead of the rest of the DoD and deployed it, it could not, for security reasons, be connected to the secure IP phone solution, Voice over Secure IP (VoSIP), adopted by the rest of the Department. This created two separate secure IP voice solutions that cannot connect within the Combatant Command AOR. The CCDR had to mandate disconnecting the Army S-VoIP within their AOR to ensure there would be a single, interoperable solution; but this solution precludes Army units in theater using a secure IP phone to talk to Army units outside of the theater.[45]

Several bases in a Combatant Command AOR serve multiple Services and agencies. There are multiple examples where the tenants have set up duplicative capabilities (satellite terminals, tech control facilities, etc.) on the same base with no interconnection. Situations abound where data sent from one side of a base to the other has to travel

back to CONUS first before being delivered to its recipient two miles away from the sender. Fiber cables are laid right next to one another and travel identical paths between buildings, but not interconnected because they belong to different Services or agencies. The CCDR has had to direct a solution to get the interconnectivity because the Services and agencies in theater are not operating jointly.[46]

Centralization of the Service's NetOps forces needs to be transparent to the GCCs and not impair their ability to conduct operations and direct action on the network when required. The Services must be able to effectively prioritize and react to direction from multiple supported Combatant Commands just as they did when the Services maintained NetOps forces in theater. The situation is exacerbated as forward-deployed forces become more dependent upon capabilities provided via reach-back over the GIG. The ability of the CCDR to orchestrate effects and fight the network is impaired when centralization causes Services' forces to be unable or unwilling to respond to the requirements of the CCDR.[47]

During the humanitarian assistance operation Unified Endeavor, conducted in the wake of the 2004 Tsunami, Pacific Command (PACOM) released direction to assigned forces to take specific network defense actions in preparation for the planned operation. The centralization of many Navy and Marine NetOps and defense functions at the Navy Global NetOps Centers made some relatively straightforward network defense measures beyond the ability of PACOM's assigned Marine and Navy forces to implement, thus increasing risk to PACOM and global networks and operations."[48]

The Combatant Commands are concerned that the increasing emphasis on centralized Service control of the GIG is degrading their ability to see and fight their portion of the GIG. With combat forces it is clear when a unit is training or conducting other functions under Service authority and when it is engaged in combat or other operations under the CCDR's authority.[49] The ability to command the forces operating in the information domain is as important as the ability to command forces in the air, land, sea and space domains. For command, control, communications and computer systems (C4S) and networks, as well as the forces that operate and defend them, the dual and in

some cases triple reporting chains make it unclear who is actually in charge at what point in the fight. During Global or Non-Global Events, the CCDRs are bypassed altogether and JTF-GNO operates directly through the Services. Though the Joint NetOps CONOPS is very specific about the requirement to coordinate actions with the CCDRs, in a fluid, fast-moving environment, that requirement can quickly become an afterthought.[50]

Information Assurance Vulnerability Alerts, Computer Tasking Orders and changes to Information Conditions issued outside of the Combatant Command are an example of this issue. These actions have direct influence on operations being conducted by the CCDRs in their theaters. When the Services try to direct actions on these Information Assurance Vulnerability Alerts and Computer Tasking Orders at an enterprise level, they cannot discern the affect on the CCDRs operations with respect to the manner and timing of the implementation. Only the CCDR has the insight to be able to do this. When a security threat triggered the Air Force Space Command to request an computer defensive status change the Air Force coordinated the action with JTF-GNO but did not notify or coordinate with NORTHCOM resulting in a significant challenges to NORTHCOM.[51]

In CENTCOM, this lack of control of NetOps forces within their theater affects their ability to ensure network availability to the commander when needed. The Navy operates numerous portions of the CENTCOM TIG. The Navy NetOps forces in the AO do not work for the Navy element of CENTCOM and report only to Navy Regional NetOps and Security Center West. The CENTCOM Central Region Theater NetOps Center, which is charged with maintaining and directing all NetOps actions for the CCDR, is not in the Navy NetOps forces reporting chain, so often does not have full situational awareness of all that is happening on the CENTCOM TIG. Workarounds have been established to address this issue, but no formal solutions are in place.[52]

For NORTHCOM, this lack of OPCON of NetOps forces created a significant predicament during relief efforts for Hurricane Katrina in 2005. During the operation, equipment from the Services flowed into Joint Operations Area (JOA) without approval and authority to operate.

This caused significant spectrum management and operational issues as NORTHCOM did not have visibility over what was flowing into the JOA and was unable to provide guidance or coordinate actions.[53]

While the Services are generally advocating a more centralized structure under JTF-GNO, it is worth noting that the Combatant Command that has been given responsibility for operation and defense of the GIG, STRATCOM, is not pushing for that centralized structure. In fact, STRATCOM has been instrumental in maintaining the GCC's role in NetOps with their Theater and Global Event construct and emphasis throughout the latest round of briefing on NetOps to the Joint Staff.[54]

Both the Services and the Combatant Commands are looking to centralize control of NetOps at the Joint level. The key questions that arise are:

- Who is in charge?
- At what level does centralization of NetOps take place: the Global level, Theater level or some other level?
- Are network effects simply a service that the CCDRs go to JTF-GNO to request or do the CCDRs have the need to direct and prioritize actions for networks within the theater?

In the end, the CCDRs are the ones charged by the President with accomplishing the Nation's military missions within their AOR.[55] Forces assigned to the CCDR are under their authority to accomplish those missions. There is no argument with this from those advocating a global control as they point to the fact that NetOps forces are under the control of STRATCOM.

But the GIG is now a key part of the CCDR's C2 capability; the commander's ability to conduct military operations. Without the GIG aircraft don't fly, ground units don't move, ships don't sail, and satellites don't provide information. Just as commanders need to be able to direct their combat forces and know their locations and status, they need to have control over the GIG and know its status. They must be able to see the scope, capability and status of their TIG; must be able to see how events outside of their theater affect their TIG; and must be able

to direct and prioritize actions in order to support their operations. If we truly believe the rhetoric about fighting the network, then CCDRs, not a centralized enterprise management operations center, must be given the appropriate control to conduct operations.

And, as long as the GCC structure remains in place, all missions conducted, even those by the Functional Combatant Commands, will occur in the Geographic CCDR's AOR. All aspects of NetOps have a physical component to them. Network Operation actions will affect those CCDRs and their operations. At the same time centralization is necessary to achieve the goals of net-centricity, to be able to effectively defend the network and to rapidly mass effects. This concept of centralization is not mutually exclusive from the need for the Geographic CCDRs to prioritize and direct their TIG.

Way Ahead

To achieve a viable NetOps C2 construct requires striking a balance between the needs of the Geographic CCDRs and the need to establish centralized control of the GIG. The current evolution of the Joint NetOps CONOPS and the transformation of the Services NetOps forces, organization and doctrine need to be leveraged to achieve that balance. To do this, the DoD should undertake the following:

- Create a single, unambiguous chain of command for NetOps making STRATCOM the supported command for all NetOps. This will answer the key question of who is in charge. Situational C2 constructs only add to the fog of war in what is already a fast-paced and fluid environment. A single chain of command will ensure that NetOps forces know whom they take direction from and whom they report to and this chain of command must include the GCCs.
- Give the GCCs authority over NetOps within their AOR by:
  - Modifying the UCP to give responsibility for NetOps within their AOR to the Geographic CCDR.
  - Modifying the existing GIG NetOps CONOPS to specify that Services without a Service TNOSC in the theater provide direct support from their GNOSC to the GCC.

– Specifying that all directives issued from JTF-GNO go to the GCCs for execution.

These changes will ensure that all elements in the theater respond to only one chain of command, through the GCCs to STRATCOM. This will also resolve NORTHCOM's dilemma of having responsibility for an AOR but no authority over its NetOps.

- Establish a Joint NetOps Center in each of the GCCs following the CENTCOM model of merging the CCDR's TNCC with JTF-GNO's TNC. This would essentially establish a Joint Component Commander in each of the GCCs for the cyber domain just as one is established for operations on land, air and space, and the sea.[56] To do this, the Combatant Command J-6 would wear two hats; one as the J6 for the Theater under the OPCON of the Combatant Command and the other as the Theater NetOps Authority, in charge of the Joint NetOps Center under the TACON of JTF-GNO.[57] All Service TNOSC would be under the TACON of the Joint NetOps Center. Any Service without a Service TNOSC in the theater would have their GNOSC in direct support of the Joint NetOps Center.
- Refocus centralization of the GIG and make STRATCOM the lead for this effort. The current centralization efforts focus on centralizing Service control of their NetOps and runs counter to the concepts behind net-centricity. Service-centricity creates unnecessary stove-pipes in information and processes and takes us away from the goal of "giving all users access to the latest, most relevant, most accurate information."[58] The Beyond Goldwater-Nichols report makes it clear that management and organization of Command, Control and Communications (which includes NetOps) should be in the hands of the Joint community.[59]

Conclusion

There is a pressing need to centralize C2 of NetOps. Flattening the network allows the DoD to increase efficiency, save costs and manage scarce resources. More importantly, this improves the ability of NetOps forces to manage and securely deliver timely, accurate information to decision-makers enabling them to rapidly mass effects.

This centralization must be balanced against the need for effective C2 of NetOps. The reliance on the GIG for all aspects of warfighting requires that commanders be aware of the status and capabilities of their TIG and be able to reprioritize efforts to support operations.

"[W]e must change the paradigm in which we talk and think about the network; we must fight rather than manage the network, and operators must see themselves as engaged at all times, ensuring the health and operation of this critical weapons system."[60] NetOps are crucial to fighting and winning our Nation's wars, from providing command and control, to reducing the decision cycle, to bringing assets outside of the theater of operations to bear. STRATCOM has made tremendous strides in moving forward the concept of NetOps and those efforts must continue. The Geographic CCDRs must be involved in the operations and defense of their portion of the GIG in order to ensure that we are able to successfully fight the network.

Winning the Peace: Building a Strategic Level Lessons Learned Program

Mr. Daniel L.A. French
United States Army

Let's start by recalling an old maxim attributed to the 19th century philosopher George Santayana that goes something like this: *those who cannot learn from history are doomed to repeat it*. Perhaps in no other endeavor or "life experience" is the impact of this maxim, or rather the failure to abide by it, so important, as in the conduct of warfare. The study of warfare—to include leaders and campaigns dating much farther back in time than Santayana's *discovery* of this truism—is replete with examples of leaders who have both acknowledged and abided by this maxim—and those who have not. Looking back only as far as World War II, generals Patton, Marshall, MacArthur, Guderian, and Rommel were noted military historians as well as brilliant strategists and tacticians—their successes on the battlefield are legendary, and attributable equally to their personal study of warfare as to their deep commitment not to repeat the mistakes of those who had gone before them. Many other military commanders, both past and present, also students of history, would likewise attribute their successes and failures at the operational and tactical levels to this simple, yet most astute concept. They would also place high value on the effort and resources required for mounting and sustaining effective lessons learned endeavors and for maintaining robust and well-managed repositories where this wisdom can be stored and from which relevant lessons can be retrieved. The renowned British strategist B.H. Liddell Hart noted:

> *…there are two forms of practical experience [lessons learned?], direct and indirect – and that, of the two, indirect practical experience may be more valuable because (it is) infinitely wider. Even in the most active career, especially a soldier's career, the scope and possibilities of direct experience are extremely limited.…The greater value of indirect experience lies in its greater variety and extent…the experiences not of another, but of many others under manifold conditions.*[1]

But what of our non-military national leaders; government agencies and other non-governmental organizations (NGO), international organizations (IO) and the diplomatic community who often find themselves in direct contact with the military, especially in the areas of stability, support, transition and reconstruction (SSTR) operations? All of these operations are now considered "core" in the spectrum of military operations; operations where the military should not necessarily have the lead, but most often does because "no one else can do it." Have these agencies and activities also not pursued a purposeful and effective lessons learned program? There seems to be little historical data to attest to this one way or the other—an issue noted often in this study. This gap or apparent gap of not having a structured, ongoing and managed lessons learned program outside the military environment leads to the underlying precept of this study—the need to incorporate, along with the military community, key political, diplomatic and interagency players—domestic and international—into a strategic level lessons learned environment.

At no time in the history of our Nation and perhaps the history of warfare has the interest in and need for capturing and learning from the lessons and experiences of others become more important than it is today. Likewise, at no time in history, given the *volatile, uncertain, complex, and ambiguous (V-U-C-A)* nature of the operational environment within which current military operations occur[2] (e.g. post-conflict operations in Iraq and Afghanistan, and the global war on terrorism (GWOT), which are projected to exist for the foreseeable future) is the task of getting *the right information to the right individual at the right time* more challenging for those who would subscribe to this business of "lessons learned."

Consider the volume of information and raw data that is or can be made available using existing Information Technology (IT) systems and architectures, and the powerful command and control systems on the battlefield today. Army C2 initiatives and enabling technologies like Force XXI Battle Command Brigade and Below, Command and Control PC, Battle Command on the Move, and Common Operational Picture are examples of systems and concepts, all developed with the goal of providing our military commanders with tactical and operational

"information superiority" thereby achieving "information dominance" during either combat operations or while performing post-conflict, stability and support operations.[3]

Unfortunately, these technologies are often based on a "more is better" mindset. What this leads to is the proverbial "information overload" syndrome where raw data and unprocessed information actually overwhelm the commander and his/her staff and is therefore more counterproductive than helpful. Each commander and his or her staff have to take time to sort, sift and filter out what is not of interest to them effectively nullifying any apparent advantage gained from pure volume. Equally important, we need to ask, "Who needs to know this information right now?" and "What is the best way to get this information to them as quickly as possible?" Although our IT development community continues to struggle with being able to provide the "dial-a-filter" capability (by level-of-command, geographical area, staff position) that our commanders need to automate this process or a major portion of it, we are not quite there yet.

Within the construct of warfare, lessons are learned, or need to be learned, across the full spectrum of conflict—all types of operations, all battlefield domains (air, land, sea and space) and at all levels, tactical through strategic. The U.S. military has developed a robust, comprehensive system to capture, analyze, and disseminate tactical and operational level lessons learned from major training events and ongoing conflict operations. The individual Services' lessons learned agencies, together with Joint Forces Command (JFCOM), are working to expand their lessons learned efforts further into the operational level and to begin to include observations, insights and lessons from the theater strategic arena. These efforts continue to be predominantly focused on warfighting issues—Major Combat Operations (what is referred to in the Joint Operations Planning Process as Phase II–Seize the Initiative, and Phase III–Dominate). No comparable system exists to address strategic/national, non-warfighting (non-kinetic) issues and activity especially in the area of post conflict operations (Phase IV–Stabilize, and Phase V–Enable Civil Authorities).[4]

Over the last two to three decades, U.S. Armed Forces have regularly been involved in conflicts where "winning the peace" has taken on greater

significance. Recent operations in Bosnia, Kosovo, Afghanistan, and Iraq have shown that increasingly in contemporary conflict operations, it is the 'war after the war' that counts. And this is the war we really have to "win" to be able to declare complete and lasting success. If we don't win in the post-conflict phase, the war may never be over. Accordingly, post-conflict operations often dominate the military planning process as well as the interests and energies of U.S. National Command Authority, Department of State and other government and non-government agencies both international and domestic. Many of these agencies have developed a lessons learned program of some sort. Both input to and output from these programs is provided in the form of mission reports, after action reports, or mission evaluations and often with a peacekeeping, stability operations focus. However, there is no single agency or process that has taken on the challenge of monitoring these efforts with the goal of sorting, analyzing, and globally sharing the key operational and strategic lessons learned coming from these agencies. Likewise the multitude of formats used, agency jargon and focus reflected in these documents, where they exist, and the lack of any type of database structure or searchable database environment within which to maintain them, significantly reduces the potential and the value of this information.

This study proposes an approach to achieve more comprehensive participation and cooperation by the interagency community on the analysis and sharing of strategic national level lessons learned through the implementation of a Strategic Lessons Learned Program (SLLP). Although this study will focus on the development of a U.S. sponsored program and its U.S. voluntary and mandated members, (the U.S. Armed Forces, Executive and other government agencies, and U.S.-based and sponsored NGOs) the incorporation of international participants will be mentioned throughout. The SLLP concept is expandable to readily include international membership and participation although there are still significant information security and information sharing issues that need to be overcome to allow full integration of and participation by the international community—issues beyond the scope of this study.

Service Programs: Tactical and Operational Lessons Learned

There exists today within each of the Services and JFCOM a robust lessons learned program that fulfills their needs at the tactical and operational levels. Each Service has an "official" lessons learned center or designated internal agency with the mission to "collect, analyze, disseminate and archive lessons learned from ongoing combat operations and training events" (or words to that effect) to include major national, Service and command level simulations supported exercises and experiments. These exercises include Joint/Unified Endeavor, Bright Star (U.S. European Command), Internal Look, Cobra Gold (U.S. Pacific Command), and Lucky Warrior (U.S. Central Command), among others. In most cases there are also doctrinal and/or Service level regulatory documents that articulate duties and responsibilities across and within the particular Service giving guidance as to how individuals, units and commands are to participate in and contribute to these lessons learned programs, such as Army Regulation 11-33: The Army Lessons Learned Program.

The Center for Army Lessons Learned (CALL)[5] is part of the Combined Arms Command (CAC) which is a major subordinate command of the Army's Training and Doctrine Command (TRADOC). CAC is commanded by a 3-star general and is located at Fort Leavenworth, Kansas. Of interest, the last two commanders of CAC have been Lieutenant General William Wallace (Commander, CJTF-5 during Phase I-III operations, Operation Iraqi Freedom [OIF] who is now the Commanding General, TRADOC) and, LTG David Petraeus (Commander, 101st Air Assault Division during OIF who, in February 2007, was named to take command of all U.S. military forces and operations in Iraq) thus giving the Army lessons learned program ideal oversight and guidance based on their personal experiences in Iraq and GWOT. The Director of CALL is an active duty Army Colonel.

The Air Force lessons learned program, directed by an Air Force Colonel, uses what they refer to as "XOL" as their lessons learned agency. The Air Force lessons learned cell is located in Rosslyn, Virginia, just a short distance from the Pentagon. XOL, and the USAF lessons learned group, is a subordinate agency of Department of the Air Force Deputy Chief of Staff, Operations (G-3).[6] In addition to addressing

system and platform specific issues (e.g. F-16, C-17 performance and vulnerabilities), the Air Force lessons learned cell focuses a significant amount of attention on multi-Service interoperability issues and other lessons learned at the operational level to include Army air-ground operations/close air support, Combat Search and Rescue, force protection/air base security, and ground convoy operations.

The U.S. Marine Corps (USMC) agency, the Marine Corps Center for Lessons Learned, is a subordinate organization within the Marine Corps Combat Development Command, located at Quantico, Virginia.[7] The U.S. Navy (USN) has a lessons learned cell to address multi-Service, interoperability issues as well as a group within their lessons learned program that is focused primarily on fleet operations/ fleet management and ship/system specific issues.[8] As with the Army and the Air Force, the USMC and USN agencies have a Colonel and Captain (Navy rank equivalent to a Colonel) respectively as their Director. For the joint community, the Joint Training Directorate and Joint Warfighting Center at JFCOM in Suffolk, Virginia conducts and manages the Joint Lesson Learned Program.[9] The joint lessons learned program occasionally reaches into the military, theater strategic level, but concentrates primarily on the operational level of war and on joint interoperability issues that are most often identified by the individual Services and submitted to JFCOM for further 'joint implications' analysis and resolution. The joint program's lessons learned data is sometimes redundant with the Services' data as information and raw data are regularly shared between the Service lessons learned activities and JFCOM. JFCOM will reassess input from the individual Services by providing additional analysis on the Service's source data to extract and more fully describe key joint interoperability issues. When appropriate, JFCOM reformats the information to be more appropriate for the joint audience and user community and to populate the joint lessons learned web-based databases and repositories. To better support the Army's transformation to a joint, expeditionary force, CALL, within their Joint Operations Integration Branch (JOIB), has embedded full time Army liaison officers within the Air Force and Marine Corps lessons learned agencies to provide real-time feedback through continuous interaction with these two Services. The JOIB at CALL also supports a small cell from the Joint Staff (J7) in their headquarters at Fort Leavenworth,

Kansas. This J7 cell provides additional connectivity and interaction across the Services as well as with the lessons learned cells maintained by the Geographic Combatant Commanders (GCCs)—e.g. U.S. European Command and U.S. Central Command, all of which have very active lessons learned programs.

As mentioned previously, the Department of Defense (DoD) lessons learned community is working to expand their lessons learned efforts even further into the operational arena and to incorporate both Theater Strategic (military focus) and National Strategic issues and concerns. However, we can expect that these expanded efforts will remain focused on warfighting— i.e. those issues and lessons determined from or during Major Combat Operations (Phase II / III), and the role of military forces in Stabilization (Phase IV) and Enable Civil Authorities (Phase V) operations—with little coverage of interagency operations except as it pertains to the role of military forces in SSTR operations as part of an interagency led project or program.

Another DoD agency that plays a significant role within the tactical and operational level lessons learned community is the Air, Land, Sea Application Center (ALSA) located at Langley Air Force Base, Virginia.[10] ALSA supports and is supported by all the Services and works closely with JFCOM and the Service lessons learned agencies to develop what are called multi-Service Tactics, Techniques and Procedures (MTTP) that focus on joint interoperability issues coming from operational theaters. ALSA vets all their products with the combatant commanders, the individual Services, and JFCOM before general release to the lessons learned user community—to include DoD, civilian agencies, and individuals. Often, MTTPs, along with other lessons learned products, form the basis for changes to existing joint and Service doctrinal publications. A particular area where ALSA products have shown to be most useful is in providing training on joint staff procedures, as used within a Joint Task Force (JTF) headquarters environment, for individual Service staff officers. Other specialty lessons learned programs have also been developed within the Services and DoD to provide just-in-time, tailored, and often mission-critical and truly life-saving information to our Soldiers and leaders in all the

Services. An example of such a program is the Improvised Explosive Device (IED) Defeat lessons learned program.[11]

From this discussion it is obvious that, at the tactical and operational level, we have robust lessons learned processes and agencies within the Services and the joint community and that a great amount of valuable information is available, accessible and continues to grow. The lessons learned process at these levels is in "high gear" and, for the most part, the Services are adequately resourced to do the job they need to do. "The U.S. military's 'lessons learned' process is exceptionally valuable in capturing useful knowledge from past U.S. military operations. However,…there is no system that can provide comparable information for non-military operations."[12] Additionally, no comparable system exists to address theater strategic (military focus) or national strategic issues, especially in the area of post-conflict operations which specifically includes SSTR operations. The Beyond Goldwater–Nichols Phase 1 Report concluded that "…there continues to exist…a consistent U.S. inability to effectively integrate political, military, economic, humanitarian and other dimensions of complex contingency operations."[13]

At the strategic level then, there is an apparent gap in the lessons learned environment both in construct and in content. Concerning content, as we move toward implementing a SLLP, we are beginning to understand that, at the strategic level, it is more and more important, if not absolutely essential, to address lessons learned from the interagency, civil-military and multinational perspective, and not just from the U.S. military or DoD perspective. A RAND study recognized this dilemma when attempting to analyze security sector reconstruction when it notes that it is important to, "emphasize qualitative issues over quantitative measures and to seek to identify and understand effects, positive and necessary, wherever possible.…[I]t is more valuable to understand why decisions were made and why programs were or were not implemented."[14] Overarching national strategy and policy, not just national military strategy (theater strategic), needs to be addressed within a strategic level lessons learned program to identify critical observations, insights and lessons that need to be captured, analyzed, and archived for future reference. There needs to be a separate

information campaign mounted to advise the larger strategic lessons learned Communities of Interest (COI) (to borrow a Knowledge Management concept) of the existence of the program itself, and the nature of the strategic level lessons learned data available. State-of-the-art information technologies need to be brought to bear to prepare this information for rapid distribution and access.

Strategic Lessons Learned: What's out there now?

On the DoD side, the individual Service programs, the JFCOM program and the programs managed by the GCC are beginning to move into the strategic level with the JFCOM program being the most aggressive. One of the major drawbacks for the Services and JFCOM in implementing a SLLP is finding strategic level analysts; individuals with the necessary skills, knowledge and attributes to do the necessary strategic level analysis; individuals with comprehensive knowledge of the planning and conduct of military campaigns and theater operations and experience in dealing with the civilian interagency community both international and domestic. On the interagency side, several agencies have already developed a lessons learned program that includes strategic level issues or have the makings of what could become a viable strategic lessons learned program—all almost exclusively focusing on peacekeeping, nation-building, and stability operations. Some of the U.S. agencies and organizations in the private sector that have existing programs include the U.S. Agency for International Development (USAID), the U.S. Institute for Peace (USIP), the Peacekeeping and Stability Operations Institute (PKSOI), the Center for Strategic and International Studies (CSIS), and the National Institute of Justice (NIJ). Internationally, the most robust and proactive agency is the United Nation's Directorate of Peacekeeping Operations (DPKO). The DPKO Best Practices Unit (BPU) "…has begun to generate the sort of timely, mission-analytic reporting that UN Headquarters, operations, and mission contributors have long needed."[15] "The BPU not only provides a repository for lessons learned but also facilitates their incorporation in education and training through clear analytical reports."[16]

The good news is that there are many agencies doing lessons learned. However, there are many challenges both in being able to find this information and in being able to use it. Within these programs, each agency mainly looks to 'help themselves,' expending little effort with the actions taken (data collected, analysis conducted, archives populated) and the products developed to prepare their potentially critical information for sharing and use outside their agency. Data is usually captured in post-event reports which are very often prepared in a proprietary format that neither lends itself to a common understanding of the content, nor to database operations and otherwise efficient web-based search and retrieval technologies. The content is focused intentionally either on internal agency and organizational interests, or on developing the specialized expertise the agency needs for its operations, using terminology and describing parochial processes, most of which are not understandable to a wider audience—civilian or military. For the international community, these products may be totally incomprehensible. The associated agency websites, if available, are seldom developed with any interest in providing a user interface that facilitates accessing their lessons learned information by non-agency personnel thereby making site navigation often complex and non-intuitive.

So, it appears that there is a significant volume of information on the interagency/non-military side, but getting to it, understanding it, and then being able to use it poses yet another set of challenges along the way to building a user-friendly, accessible and content-rich strategic lessons learned environment. Simply achieving awareness of who's doing what, what's available, and then gaining access to it in a relatively easy and efficient manner are problems the SLLP must be prepared to address and overcome. Not surprisingly, there is no single agency, program or process that has taken on the challenge of monitoring, assessing, and attempting to coordinate these disparate efforts. The goal of finding, sorting or cataloging, analyzing, normalizing, archiving and globally sharing key operational and strategic, non-military lessons learned information is a daunting task.

This study proposes an approach that can help both the military and the interagency communities to achieve significantly improved

cooperation on the collection, analysis, consolidation, and sharing of theater strategic (military focus) and national strategic level lessons learned, and the subsequent integration and application of these lessons into policy, procedures and programs needed to support future crises.

Why We Need a Strategic Level Lessons Learned Program

It is a reasonable expectation that future conflict operations involving the commitment of U.S. armed forces will include planning for and the conduct of what we have been referring to as SSTR—stability, support, transition and reconstruction—operations activities encompassing a combination of independent military, cooperative and simultaneous civil-military, and civilian interagency-only operations. Differing from our recent experience in OIF, it is expected that civilian agencies will be employed much sooner than they were in Iraq, and that civilian managed (non-combat) operations will likewise begin sooner and may even be conducted simultaneously with predominantly military led (combat/kinetic) operations throughout the geographic theater of operations; with the additional expectation that these strategic operations will more and more become the domain of the civilian interagency community. "…[T]here will be a continuing need for effective operational transitions between the peacekeeping forces of regional organizations [interagency] and coalitions [the military]."[17] As mentioned previously, the phasing model for joint operations includes a Phase IV–Stabilize, and a Phase V–Enable Civil Authority. Peace-building/peace-keeping will continue to be a major element of future military operations, with associated activities being conducted by both the military and the interagency community during these phases.

> *[O]ur Joint Forces also enhance their ability to operate in consonance with other U.S. Government agencies, and with NGOs and IOs…The specialized access and knowledge these organizations possess can facilitate prompt, efficient action to prevent conflict, resolve a crisis,…and restore civil government upon conflict termination.*[18]

"Soldiers, police and civilian personnel…rarely train together beforehand, and often have very little direct knowledge of the others' profession culture."[19] This will definitely complicate matters as they

attempt to work together in the complex Phase IV-V environment. Understanding professional culture helps to break down the barriers to cooperation and helps to build the trust and understanding that is so essential for achieving constructive discussions on the deficiencies and problem areas to be overcome. Even a simple listing of just the problems experienced during previous attempts to work together, regardless of solutions attempted or achieved, would go a long way to providing some awareness of 'what to expect' as well as helping leaders and planners focus on areas where military-civilian cooperation is critical to mission success—especially when working with and within the indigenous population—on the street corner, in their market-business-corporate community, and in the law enforcement and local and national political environment.

Before charging off 'full-speed-ahead,' a moment of honest introspection is perhaps appropriate. It is a disappointing fact that within the United States the lessons learned-After Action Review culture is very inconsistent and, in some instances, the necessary culture of sharing, cooperation and learning is non-existent outside of the military-police-firefighting communities. Within the interagency community many individuals, from action officer and staff level to the senior leadership don't "feel good" about the information-sharing process needed for an effective lessons learned program—especially when it comes to acknowledging, analyzing, discussing, and actually recording mistakes, shortfalls and deficiencies. These individuals are often reluctant to participate in open and constructive After Action Reviews (AAR); a situation attributable as much to not understanding the AAR process as to having experienced an AAR that was not properly conducted and facilitated. There is also always that lingering fear or concern that adverse consequences will result from openly admitting mistakes and/or problems, or, causing even greater trepidation, drawing attention to those mistakes or problems caused by leaders and supervisors. Within the SLLP, one needs to envision doing this in a multi-agency and even multi-national environment. Consider a team or unit made up of a collection of participants from just a few other nations or agencies conducting an AAR: considerations like national pride and agency loyalty begin to influence not only the level of participation, but also the 'integrity' of the input—i.e. just how truthful will they be; how much 'license' will be

taken in recounting the 'facts'? Integrating the interagency community by including them in various unit level military lessons learned events, where lives may be at stake, provides yet even more challenges and concerns and sometimes non-productive skepticism—especially from our military leaders at all levels.

Understanding each other's culture is an important component for any integrated lessons learned program. Within the military, "… staffs are generally not trained to appreciate the magnitude of the interagency process and the challenges inherent in dealing with dozens of other organizations in the operational area."[20] For the most part, cooperation and collaboration has been conducted in an ad hoc nature with varying levels of commitment from the interagency players and the military. Subsequent efforts to effectively integrate any lessons learned into civilian agency policy and operations is nominal at best, and any further tracking of these lessons and their application within the organizations, any effectiveness assessments are mostly non-existent. Of course, all of this makes it even harder to build for the future by learning from the past—the ultimate coin-of-the-realm for a lessons learned program. Within the interagency community, this "ad hoc approach to coordination and integration…should give way to a full time Interagency Operations Center (IOC)…"[21] under the direction of the National Security Council (NSC) with dedicated support from key players in the interagency community (e.g. USAID, Department of Justice, Department of the Treasury) and the military lessons learned community.

The establishment of this IOC under the direction of the NSC is consistent with guidance and responsibilities laid out in National Security Presidential Directive (NSPD) 44 which directs the Secretary of State to "…coordinate and lead integrated United States Government efforts, involving all U.S. Departments and Agencies with relevant capabilities, to prepare, plan for, and conduct stabilization and reconstruction activities."[22] Under the specific control of the Coordinator for Reconstruction and Stabilization (S/CRS), a position created by NSPD-44, the Secretary of State will "identify lessons learned and integrate them into operations" and "coordinate reconstruction and stabilization activities and preventative strategies with foreign

countries, international and regional organizations, nongovernmental organizations, and private sector entities…[to] facilitate…work with respect to these institutions and bodies."[23] The Directive attempts to ensure full cooperation and integration with the military lessons learned processes/programs by further directing the Secretary of State to "…coordinate such efforts with the Secretary of Defense to ensure harmonization with any planned or ongoing U.S. military operations…"[24] A Presidential Policy Coordination Committee for Reconstruction and Stabilization Operations is also established, chaired by the S/CRS, within which designated U.S. executive departments and agencies are to "assist in…responding to crises that occur, assessing lessons learned, and undertaking other efforts…to ensure a coordinated U.S. response and effective international reconstruction and stabilization efforts."[25]

Implementing a Strategic Lessons Learned Program

It is apparent from the discussion above that the beginnings of an infrastructure already exist for implementing a SLLP. On the interagency side, the NSC clearly has the documented authority and direction to take the lead and responsibility for participation in such a program, to include coordinating the participation of interagency players. In addition to NSPD-44, Presidential Decision Directive-56 (PDD-56), President Clinton's policy on managing complex contingency operations, gives very specific guidance and direction to the interagency community concerning lessons learned. "The PDD is designed to ensure that the lessons learned—including proven planning processes and implementation mechanisms—will be incorporated into the interagency process on a regular basis."[26] The PDD directs that "after the conclusion of each operation…the ExCom [will] charter an after-action review involving both those who participated in the operation and Government experts who monitored its execution. [The AAR] will include a review of interagency planning and coordination (both in Washington and in the field),…problems,…as well as proposed solutions, in order to capture lessons learned and to ensure their dissemination to relevant agencies."[27] But, is this really happening? What has been done to date? Where are these reports and how do others get to them? What "integration" has taken place? How do we know?

To better substantiate and define the military's roles and responsibilities, DoD Directive 3000.05 (DODD 3000.05) directs the Secretary of Defense (SecDef) to "…develop a process to facilitate information sharing for stability operations among the DoD Components, and relevant U.S. Departments and Agencies, foreign governments…International Organizations, NGOs, and members of the Private Sector…"[28] The SecDef is also directed creation of "a stability operations center to coordinate stability operations research, education and training, and lessons learned."[29]

Given just the number of operations conducted and ongoing as part of Operation Enduring Freedom and OIF, it would seem, at least for U.S. players, both military and civilian, that there should be a large amount of content, a lot of existing interagency lessons learned "out there—somewhere." It would also seem that we have a construct and the necessary, appropriate policy and guidance to implement a consolidated SLLP—one built on the most likely operational scenarios for future civilian-military interaction and cooperation during military operations and their associated SSTR operations. That same SLLP would support future pre-operational and operational planning, collaboration and execution, and facilitate the capture, analysis, vetting and dissemination of lessons learned from these SSTR scenarios and operations. But, policy and guidance does not a program make. Rather, what and where are the necessary resources to include funding and manpower which are equally as important as the intellectual and emotional commitment on the part of all players to make this a viable program? Before being able to answer these questions, it is necessary to go into some additional detail as to the structure and objectives of the SLLP. What follows is a discussion on the proposed organizational components and some proposed missions, roles and functions of the SLLP.

No single agency within either the DoD community or within the NSC-Interagency community will be able to effectively implement the SLLP, nor would it be economically feasible to establish a new organization to do this. The SLLP envisioned by this study is more of a confederation of member agencies and programs that include government, private sector, international and domestic, and individual

subject matter experts (SMEs), that can contribute their existing knowledge, data repositories, analysts, procedures and other resources to support the overall functioning and effectiveness of the SLLP. The SLLP will be a network-enabled confederation that works, using web-based collaboration technologies as well as traditional face-to-face seminars and discussion/study groups, to achieve a "massing of expertise"[30] effect to apply to a problem. Being able to rapidly mass, at any time, the resident expertise of the Services, various government agencies, Embassy teams, NGOs and IOs, and individual SMEs brings to bear an incredible capability to resolve strategic level issues and challenges—rapidly and effectively. SSTR operations, by their very nature means that expertise resides in multiple agencies, with individuals that may be deployed to ongoing contingency operations none of which can be readily assembled in a single location. Massing this expertise provides the most viable and efficient means to bring together not only the right individuals, but also the existing lessons learned data, and other functional/operational doctrine, regulations, study results, etc. needed to develop timely solutions to problems—solutions with a high probability of lasting success. The SLLP will act as the conduit within which this massing of expertise can take place The SLLP will also provide the environment within which we will be able to track what was done, by whom, with what resources and with what results.

The physical structure of the SLLP would consist of a core cell or master node with multiple functional nodes all working within an advanced technical infrastructure. The core cell would provide general oversight, direction, guidance and operational management of the SLLP; a technical support team would be included in the core cell to provide necessary IT capabilities. We will refer to this cell as the "Center for Strategic Lessons Learned" (CSLL). The CSLL along with its IT infrastructure is the component of the SLLP that would require new funding to implement. The CSLL would initially only need to be a small group of 20-30 personnel (military and DoD civilian) and a contractor support group. Any future growth of this cell would be dependent on increased scope and potential consolidation with other activities or agencies, which could actually bring significant cost-savings in the long term. The major functions of the CSLL would include:

- Coordination among agencies already doing lessons learned and lessons learned integration; managing an SLLP awareness program
- Development of an internal awareness of "what's out there" in the way of both military and interagency lessons learned capability and products
- Facilitation of online collaboration (massing expertise) and/or onsite issue resolution activities (e.g. host and attend seminars, study groups)
- Identification of gaps in the strategic lessons learned global knowledge base
- Development of a data/product normalization process
- Provision of internal "case workers" and managing an external SME database to respond to user queries within the construct of a Request For Information (RFI) system
- Provision of tailorable and focused dissemination of strategic level lessons learned products to senior civilian and military leaders
- Work general technical support and specific technical interoperability issues related to network operations across the community

The CSLL would be staffed by a small military leadership team and then manned with predominantly DoD civilian analysts and action officers. Contractors could also fill the analyst positions, having already mentioned the challenge in being able to find skilled, strategic level analysts. A contractor-based cell would form the technical team needed to conduct world-wide, web-based IT operations. There are other core activities and actions outside the direct purview of the CSLL that all agencies and players would have to perform or commit to performing that are critical for the overall effectiveness of the SLLP. In particular, "…all member states should…create appropriate national data bases of personnel trained for peace operations."[31] "The international community faces a major challenge in meeting the recent surge in demand for qualified peacekeepers."[32]

The functional nodes of the SLLP would consist of a group of government agencies and NGOs that would be referred to as the "primary" nodes with other relevant agencies and activities forming "secondary" nodes within the network. It is expected that the primary node members would already have a functional lessons learned program. The secondary member agencies and organizations may also have existing lessons learned programs or may just be agencies that the CSLL identifies that are important to the overall effectiveness of the SLLP. Both groups will continue to grow over time. The secondary agencies would join the confederation either as branches from the primary nodes or independently within the network. The IOC, mentioned above as an activity managed by the NSC, acting as the primary interface between the CSLL and the interagency community, would be an example of a primary node. For the interagency community, "forming a permanent IOC is the necessary first step toward improving civilian-military responses to contingencies [complex operations]. The [IOC] will improve responses in Washington, in the…regional commanders' headquarters, and in the field where unity of effort matters most."[33] Other key or primary nodes within the interagency community would include: the Department of State's Office of the Coordinator for Stability and Reconstruction (S/CRS), USAID, USIP, CSIS, NIJ, and the UN's DPKO-BPU. Also within the UN are the Peace Building Commission and the Peacebuilding Support Office, each of which can provide a wealth of operational expertise and lessons learned based on years of experience monitoring and reporting on SSTR operations. Over time, these key or primary nodes could be expected to develop their own special interest communities and "clusters" that would function independently, as branches from a primary node or within the main SLLP collaboration network—all using the Global Integrated Lessons Learned Network (GILN) infrastructure described below.

The key or primary nodes within the DoD community would include: the Service lessons learned agencies, ALSA, the JFCOM lessons learned cell, the GCC lessons learned cells, the ABCA (America – Britain – Canada – Australia) lessons learned activity, and the Army's PKSOI located at Carlisle Barracks, Pennsylvania. The PKSOI has recently been designated as a Field Operating Agency under the Department of the Army's G-3/5/7. The new Operational Integration Section:

> *serves as the fusion cell for PKSOI in support of JFCOM, Services, Geographic Combatant Commanders, interagency, allied and other foreign militaries, multinational organizations, and IOs/NGOs. Integrates current SSTRO & Peace Operations concepts, doctrine, and policy into operations, and experimentation. Capitalizes upon PKSOI and USAWC (Army War College) expertise and enlarges a multi-disciplinary SME network to provide expertise required by organizations preparing to participate in SSTRO & Peace operations.*[34]

This study recommends that the CSLL be integrated into the organizational structure of PKSOI—either within the proposed Operational Integration Section or as an independent section or directorate. The CSLL would sponsor independent lessons learned collection efforts, as well as collaborating with existing Service, JFCOM, or other agency planned collection efforts to meet strategic lessons learned requirements. The Services, JFCOM, and ALSA would be expected to support the CSLL's analytical work, providing their Service's and/or agency's perspective and assisting with the vetting of any CSLL specialized products. This group would also be expected to assist with the normalization of products originating in the interagency community. CSLL input to the Service and JFCOM efforts could result in a 'strategic annex' for their products as well as providing additional core data for any specialized products CSLL develops for the military strategic community.

The technical IT network, with associated collaboration tools, databases and structures, search and retrieval applications that will enable massing of expertise and that supports the day-to-day operations of the SLLP, will be referred to as the Global Integrated Lessons Learned Network (GILN). The contractor technical staff will be responsible for web development and management (including a set of state-of-the-art collaboration tools and applications), database design and implementation, access and security management, search and retrieval utilities that span the various member lessons learned repositories and databases and the on-line RFI system. A more detailed discussion of the technical specifics is beyond the scope of this study. This is a difficult undertaking that will take some time and money to fully implement and that requires a significant amount of coordination and

effort to provide a workable level of interoperability with other existing Service and interagency systems There may be associated technology costs which the various members would be asked to absorb to join and actively participate in the SLLP "digital confederation."

A challenging function of the CSLL mentioned above that warrants some additional explanation is a data and product normalization process—for both existing products and those yet to be developed by the SLLP participants. Earlier in this study it was established that current activity—analysis and product development—within the various agencies most often results in data and products that are very agency centric and perhaps of minimal use outside the source agency. These products would need to be sanitized of proprietary terminology/jargon/acronyms, biased analytical perspective, potential political overtones or "hidden agendas." The normalization process, as envisioned for this study, is an effort to take the existing information or new products as they are developed, in whatever format the source agency uses, and attempting to either restructure them using some mutually agreed-upon template, or to add metadata, summary data, or other content description—an abstract of sorts—to make the source information more understandable and usable across the multiple audiences that may have a need-to-know and want to use this information. The raw information (the source data) would have to be protected and maintained, but this would remain the source agency's requirement. Normalization should also result in data and products that are more internet search engine friendly. Given the amount of existing information and the fact that we are "late getting started," this normalization will be a time consuming and challenging operation, but it is required to facilitate the more effective use of the available data and products across the diverse strategic lessons learned community.

Another activity that warrants special attention is the implementation of a SLLP awareness program. This program would need to be conducted as an information operations or strategic communication effort. Its intent would be to establish a baseline of knowledge within the strategic lessons learned community, in order to demonstrate the existence of the SLLP, its membership and functions. This effort would identify those agencies that are actively conducting

lessons learned efforts and the type of lessons learned processes they are performing. It would identify associated products available, and inform as to where or how to access this information. A second objective would be to provide a mechanism for knowing when the various agencies will be conducting events such as seminars or conferences at which critical, emerging lessons learned information can be presented. Recurring events on an annual, semi-annual, and quarterly basis would be primary targets for the SLLP. Additionally, this effort would attempt to get on the agenda for these major gatherings and work toward having presentations and discussions on lessons learned, and to highlight their integration and application, as a core component of these meetings.

Concerning the dissemination of lessons learned, several agencies and activities exist that are ideal for packaging and distribution, and then monitoring feedback of strategic lessons learned products. The International Association of Peacekeeping Training Centers (IAPTC), sponsored by the Pearson Peacekeeping Centre in Canada is a prime example.[35] The IAPTC conducts an annual seminar where dissemination of lessons learned would be most appropriate and perhaps have the greatest potential for subsequent distribution and actual integration of lessons learned into doctrine, policy, training and education across a more global audience. These meetings could also be used to announce upcoming special mission or focused strategic level lessons learned collection efforts, solicit participation as the lead for the collection effort or participation as an interested member on a multi-agency, multi-national collection team.

When planning and conducting actual in-theater collection efforts, whether in the form of a directed collection team or as part of a longer duration or extended presence activity an area of concern is the adequacy and appropriateness of any pre-deployment training. Training programs would need to provide the most current and relevant information on the region, plus any special Embassy level information necessary to develop appropriate and necessary regional skills, capabilities and cultural, situational awareness for individual leaders, staff members and groups who may be involved in the collection and analysis of lessons learned data, either as their primary mission or as part of their day-to-day activity. For special mission or focused

collection efforts, much of the pre-deployment training, planning and preparation could also be completed online using the web-based collaboration tools and environment maintained by the CSLL or other Service and/or interagency training venues. Training products and online courseware would be made available via the GILN, JFCOM's Joint Knowledge Development and Distribution Capability, and other Service and agency web portals. The content in turn would be updated regularly and managed remotely by the Services, JFCOM, agencies and Embassies that develop the course syllabi and training products. These training and education products and services would be vetted with the various regional combatant commanders and Chiefs of Mission to ensure specific country, regional or in-theater pre-deployment training requirements are met. Additional pre-deployment activities such as querying the various SME databases to develop the team, providing biographical and background data on the individual members, developing a formal collection plan/issue template, movement planning and itinerary could be accomplished remotely via the internet greatly reducing the cost for these missions.

Conclusion

Many senior leaders, both civilian and military, have acclaimed "…the interagency process is broken." The implementation of a Strategic Level Lessons Learned Program, properly manned and resourced, would provide the necessary and appropriate processes and infrastructure within which to start "fixing" this deficiency. The conduct of stability, support, transition and reconstruction operations, Phase IV/V operations, civil-military operations, nation-building, or peacekeeping—whatever term you chose to use—will be prevalent in all future conflicts where our Armed Forces and U.S. interagency players are committed to achieve our national strategic objectives. The SLLP environment provides an ideal construct within which to capture the experiences and the strategic lessons learned of the military and the larger civilian, interagency community—and at the same time, enhance the ability of the interagency and the military to work more effectively and efficiently together to respond to strategic level issues and to solve strategic level problems. More so than winning the "shooting war," success in these non-combat operations will be the decisive factor in

determining the United States' overall success or failure—from both the perspective of the global community as well as the towns and communities within the United States who are asked to give their husbands and wives, sons and daughters by serving in the military. The success of the SLLP builds on and is actualized by robust, relevant, and ongoing tactical and operational lessons learned programs. These tactical and operational programs exist We are at the right crossroads in time to implement a strategic level lessons learned program. A strategic level lessons learned program, as described in this study, can and will help to ensure that "winning the peace" is a reachable goal. If our senior leadership is willing to provide the resources, DoD and the interagency community can provide the will and the energy to make this program work.

A final thought:

> *Fools say that they learn by experience. I prefer to profit by others' experiences.*
>
> —Field Marshal Otto von Bismarck

Endnotes

Preface

1. Reagan, Ronald. National Security Decision Directive 130. Washington DC: The White House, 6 March 1984. Available from http://www.fas.org/irp/offdocs/nsdd/nsdd-130.htm (accessed 23 December 2005).
2. Emergent NATO doctrine on Information Operations cites Diplomatic, Military and Economic activities as "Instruments of Power." It further states that Information, while not an instrument of power, forms a backdrop as all activity has an informational backdrop.
3. Neilson, Robert E. and Daniel T. Kuehl, "Evolutionary Change in Revolutionary Times: A Case for a New National Security Education Program," National Security Strategy Quarterly (Autumn 1999): 40.
4. R.S. Zaharna, "American Public Diplomacy in the Arab and Muslim World: A Strategic Communication Analysis," American University, Washington DC: November 2001, from http://www.fpif.org/pdf/reports/communication.pdf (accessed September 25, 2007), p. 2.
5. Groh, Jeffrey L. and Dennis M. Murphy, "Landpower and Network Centric Operations: how information in today's battlespace can be exploited," *NECWORKS*, Issue 1, March 2006.

Section One: Information Effects in the Cognitive Dimension

Information Operations Roadmap: One Right Turn and We're There

1. U.S. Department of Defense, *Information Operations Roadmap*, redacted ver. (Washington DC: U.S. Department of Defense, 30 October 2003), 2.
2. Ronald O'Rourke, *Defense Transformation: Background and Oversight Issues for Congress*, (Washington DC: Library of Congress, 9 November 2006), 1.
3. Ibid.
4. Williamson Murray and Robert H. Scales, Jr., *The Iraq War* (Cambridge MA: The Belknap Press of Harvard University Press, 2003), 245.
5. U.S. Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13 (Washington DC: U.S. Joint Chiefs of Staff, 13 February 2006), GL 9.
6. Alvin Toffler and Heidi Toffler, *War and Anti-War: Surviving at the Dawn of the 21st Century* (Boston: Little, Brown and Company, 1993), 33.
7. Ibid., 58.

8. Thomas L. Friedman, *The World is Flat: A Brief History of the Twenty-first Century* (New York: Farrar, Straus and Giroux, 2005), 133.
9. Toffler and Toffler, 67.
10. U.S. Army Training and Doctrine Command, Change 3 to TRADOC Pam 525-3-90, *Operational and Organizational Plan for the Future Combat Systems Brigade Combat Team* (Ft Knox KY: Unit of Action Maneuver Battle Lab, 16 December, 2005), 4-4.
11. Robert R. Leonhard, *The Principles of War for the Information Age*, 2nd ed. (Novato CA: Presidio Press, 2000), 19.
12. Ibid., 18.
13. Greg Mortenson and David Oliver Relin, *Three Cups of Tea: One Man's Mission to Fight Terrorism and Build Nations … One School at a Time* (New York: Viking Penguin, 2006), 274.
14. Murray and Scales, 240.
15. U.S. Department of Defense, *Information Operations Roadmap*, redacted ver., 6.
16. Ibid.
17. Ibid.
18. Ibid., 7.
19. Ibid., 22.
20. Ibid., 60.
21. Ibid., 63.
22. Ralph O. Baker, "The Decisive Weapon: A Brigade Combat Team Commander's Perspective on Information Operations," *Military Review* 86 (May-June 2006): 13.
23. Ibid., 21.
24. William M. Darley, "Clausewitz's Theory of War and Information Operations," *Joint Force Quarterly*, no.40 (1st Quarter 2006): 79.
25. Thomas F. Metz et al., Massing Effects in the Information Domain: A Case Study in Aggressive Information Operations," *Military Review* 86 (May-June 2006): 5.
26. Ibid.
27. Ibid., 6.
28. U.S. Department of Defense, *Information Operations Roadmap*, redacted ver., 23.
29. 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, 1 March 2007), 259.
30. Toffler and Toffler, 141-142.

Public Diplomacy: Key Enabler Of America's National Security Strategy

1. President George W. Bush, *The National Security Strategy of the United States of America* (Washington DC: National Security Council, 16 March 2006), Introductory letter.
2. Charles Wolf, Jr. and Brian Rosen, *Public Diplomacy: How to Think About and Improve It* (Santa Monica CA: RAND Corporation, 2004), 1.
3. David M. Edelstein and Ronald Krebs, "Washington's Troubling Obsession with Public Diplomacy," *Survival* 47 (Spring 2005): 90.
4. Wolf and Rosen, 1.
5. Ibid., 2.
6. United States Information Agency Alumni Association, "What Is Public Diplomacy?" Washington DC, updated 1 September 2002, http://www.publicdiplomacy.org/1.htm (accessed 27 December 2006).
7. Secretary Colin Powell, *U.S. Department of State and U.S. Agency for International Development Strategic Plan for Fiscal Years 2004-2009* (Washington DC: Department of State/USAID, 2003), 30.
8. Under Secretary for Public Diplomacy and Public Affairs Karen Hughes, U.S. Department of State, testimony at confirmation hearing before the Senate Foreign Relations Committee, Washington DC, 22 July 2005, http:www.state.gov/r/us/2005/49967.htm (accessed 21 February 2007).
9. *Pew Global Attitudes Project: Nine Nation Survey (2004)*. Final Topline (Washington DC: The Pew Research Center for the People and the Press, 2004), 24.
10. Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, *Report of the Defense Science Board Task Force on Strategic Communications* (Washington, D.C.: Department of Defense, September 2004), 14.
11. Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, 16.
12. Incorporated in January 2004 by interested private sector leaders, Business for Diplomatic Action seeks to counter anti-American sentiments that can harm U.S. business interests by helping to coordinate the outreach efforts of U.S. multinational corporations.
13. U.S. Government Accountability Office, 7.
14. The Library of Congress, Congressional Research Service, *CRS Report for Congress, U.S. Public Diplomacy: Background and the 9/11 Commission Recommendations*. RL32607 (Washington DC: Library of Congress, 1 May 2006.), Summary.
15. Bush, *The National Security Strategy of the United States of America*, 1.

16. U.S. Government Accountability Office, Report to the Chairman, Subcommittee on Science, State, Justice, and Commerce, and Related Agencies, Committee on Appropriations, House of Representatives, *U.S. Public Diplomacy: Interagency Coordination Efforts Hampered by the Lack of a National Communications Strategy*, GAO-05-323 (Washington DC: GAO, April 2005), 4.
17. "America's Mixed Message Abroad," a Gannett News Service Special Report, 14 July 2002, http://www.gannettonline.com/gns/mideast/diplomacy.htm (accessed December 24, 2006).
18. Wilson Dizard, *Strategy of Truth: The Story of the United States Information Service* (Washington DC: Public Affairs, 1961), 30.
19. Alan K. Henrickson, Professor of Diplomatic History, The Edward R. Murrow Center of Public Diplomacy, *The Edward R. Murrow Center of Public Diplomacy Home Page*, http://fletcher.tufts.edu/murrow/public-diplomacy.html (accessed December 24, 2006).
20. Wolf and Rosen, 4.
21. Hans Tuch, *Communicating with the World* (New York: St. Martin's Press, 1990), 15.
22. *The Edward R. Murrow Center of Public Diplomacy Home Page*, http://fletcher.tufts.edu/murrow/public-diplomacy.html (accessed December 24, 2006).
23. United States Information Agency Alumni Association.
24. U.S. Department of State, *Dictionary of International Relations Terms* (Washington DC: The Department of State, 1987), 85.
25. United States Information Agency Alumni Association.
26. Anna Tiedeman, *Branding America: An Examination of U.S. Public Diplomacy Efforts After September 11, 2001* (Boston: Tufts University, The Fletcher School, April 2005), 9.
27. Tuch, 3.
28. Joseph Nye, *Soft Power* (New York: Public Affairs, 2004), 18.
29. Tiedeman, 11-12.
30. "Defining PD," University of Southern California Center on Public Diplomacy website, http://usc.publicdiplomacy.org/mediawiki/index.php/definingPD.html (accessed December 27, 2006).
31. Powell, 30.
32. Edelstein and Krebs, 90.
33. Amol Shamra, "Congress Pushing for Renewal of U.S. Overseas Image-Building," *CQ Weekly Online*, August 10, 2002, http://library.cqpress.com/cqweekly/document.php?id=weeklyreport107-000000487112 (accessed October 9, 2006).
34. Tiedeman, 38-41.

35. Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, 16.
36. Edelstein and Krebs, 89.
37. U.S. Government Accountability Office, 1-4.
38. Under Secretary for Public Diplomacy and Public Affairs Karen Hughes, U.S. Department of State, remarks to the 2005 Forum on the Future of Public Diplomacy, http:www.state.gov/r/us/2005/55165.htm (accessed February 22, 2007).
39. President George W. Bush, *Presidential Address to a Joint Session of Congress and the American People*. 107th Congress, 2d session, 20 September 2001.
40. Barry Fulton, "Taking the Pulse of American Public Diplomacy in a Post-9/11 World," presented at the annual meeting of the International Studies Association (Montreal, March 2004).
41. Bush, *The National Security Strategy of the United States of America*, introductory letter.
42. Ibid., 49.
43. The Library of Congress, RL32607, 1-4.
44. Stephen C. Johnson, "Improving U.S. Public Diplomacy Toward the Middle East," Heritage Lectures 838 (February 10, 2004): 1-2.
45. The Library of Congress, RL32607, 5.
46. The Library of Congress, Congressional Research Service, *CRS Report for Congress, Public Diplomacy: A Review of Past Recommendations*. RL33062 (Washington DC: Library of Congress, October 31, 2005), 11.
47. Ibid.
48. The Reader's Digest Association, *Merriam-Webster's Deluxe Dictionary, Tenth Collegiate Edition* (New York: The Reader's Digest Association, 1998), 1466.
49. Oren Stephens, *Facts to a Candid World: America's Overseas Information Program* (Stanford: Stanford University Press, 1955), 29.
50. Nancy Snow, *Global Media Journal* 2, issue 3, Fall 2003 (West Lafayette: Purdue University, 2003), http://lass.calumet.purdue.edu/gmj./fa03,gmj-fa03-guesteditor-note.html (accessed December 23, 2006).
51. Ambassador Christopher Ross, "The Propaganda War: Is America Effectively Telling Its Side of the Story in the Anti-Terrorism Campaign?," transcript, Press Coverage and the War on Terrorism Forum co-sponsored by the Brookings Institute and Harvard University, Brookings Institute, Washington DC, January 16, 2002, http://www.brook.edu/comm/transcripts/20020116.htm (December 29, 2006).
52. General Richard B. Myers, *The National Military Strategy of the United States of America* (Washington, D.C.: The Joint Chiefs of Staff, March 2005), 1.

53. Office of the Undersecretary of Defense for Acquisition, Technology and Logistics, 5.
54. Myers, 1.
55. The "Global Commons" are those areas of the Earth shared by all. It is the atmosphere, hydrosphere, lithosphere, and cyberspace. A.P. Palmer, Institute of Cambrian Studies, Boulder CO.
56. Secretary Donald R. Rumsfeld, *The National Defense Strategy of the United States of America* (Washington DC: The Department of Defense, March 2005), 6-7.
57. Merriam-Webster's Deluxe Dictionary defines influence as "the act or power of producing an effect without apparent exertion of force or direct exercise of command." *Merriam-Webster's Deluxe Dictionary, Tenth Collegiate Edition* (New York: The Reader's Digest Association, 1998), 944. In order to fit the context in which it is used, the definition of influence in this paper is a slightly reworded version of the above definition.
58. Edelstein and Krebs, 94-95.
59. Rumsfeld, 6.
60. Ibid., iv.
61. Ibid., 8.
62. President George W. Bush, *National Strategy for Combating Terrorism* (Washington DC: National Security Council, September 2006), 5.
63. Ibid., 17.
64. Myers, 1.
65. Global Strike is defined as "responsive joint operations that strike enemy high value/payoff targets, as an integral part of joint force operations conducted to gain and maintain battlespace access, achieve other desired effects and set conditions for follow-on decisive operations to achieve strategic and operational objectives." Global Strike Joint Integrating Concept, ver. 1.0 (Washington DC: Defense Technical Information Center, 10 January 2005), 2.1.
66. Myers, 6-7.
67. Rumsfeld, 4-7.
68. Ibid., 15.
69. Rumsfeld, 5.
70. Ibid., 7.
71. John Donne, Meditation XVII, http://isu.indstate.edu/ilprof/ENG451/island/ (accessed January 1, 2007).
72. Rumsfeld, 7.

Strategic Communication: A Department of Defense Approach

1. Defense Science Board, *Report of the Defense Science Board Task Force on Strategic Communication* (Washington DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2004), 2.
2. U.S. Department of Defense, *Quadrennial Defense Review Report* (Washington DC: U.S. Department of Defense, February 6, 2006), 91.
3. U.S. Advisory Group on Public Diplomacy for the Arab and Muslim World, *Changing Minds Winning Peace: A New Strategic Direction for US Public Diplomacy in the Arab & Muslim World* (Washington DC: U.S. Department of State, October 1, 2003).
4. U.S. Congress, Senate, Senate Foreign Relations Committee, The Mission of Public Diplomacy: Karen Hughes; Nominee for Under Secretary for Public Affairs and Public Diplomacy, Testimony at confirmation hearing before the Senate Foreign Relations Committee, 109th Cong. 2d sess., July 22, 2005.
5. Jeffrey B. Jones, "Strategic Communication: A Mandate for the United States," *Joint Force Quarterly*, no. 39 (Fourth Quarter 2005): 180.
6. Condoleeza Rice, Remarks with Under Secretary for Public Affairs and Public Diplomacy Karen Hughes at Town Hall for Public Diplomacy, Loy Henderson Auditorium, Washington DC, September 8, 2005.
7. U.S. Government Accountability Office, *U.S. Public Diplomacy: State Department Efforts to Engage Muslim Audiences Lack Certain Communication Elements and Face Significant Challenges* (Washington DC: U.S. Government Accountability Office, May 2006), 5.
8. Ibid.
9. U.S. Department of Defense, *Quadrennial Defense Review Report*, 91.
10. Ibid., 3.
11. Jones, 180.
12. Robert Schoenhaus, Clarification of Strategic Communication-Concept and Process Talking Paper. (Washington DC: Interagency Strategic Communication Fusion Team, February 10, 2006)
13. U.S. Department of Defense, *QDR Execution Roadmap for Strategic Communication, 2006* (Washington DC: U.S. Department of Defense, September 25, 2006), 2.
14. U.S. Government Accountability Office, *U.S. Public Diplomacy State Department Efforts to Engage Muslim Audiences Lack Certain Communication Elements and Face Significant Challenges*, 5.
15. Duane R. Ireland and Michael A. Hitt, T*he Thinking Manager's Source* (New York: Academy of Management Executive, 2005), 38.

16. U.S. Department of Defense, *QDR Execution Roadmap for Strategic Communication, 2006*: 3.
17. U.S. Department of Defense, *Quadrennial Defense Review Report*, 31.
18. Defense Science Board, *Report of the Defense Science Board Task Force on Strategic Communication*, 7.
19. U.S. Department of Defense, *Quadrennial Defense Review Report*, 92.
20. Ibid.
21. About.com, "U.S. Military," http://usmilitary.about.com/od/glossarytermsm/g/m3958.htm (accessed February 3, 2007).
22. U.S. Department of Defense, *QDR Execution Roadmap for Strategic Communication, 2006*: 5.
23. Ireland and Hitt, 38.
24. U.S. Department of Defense, *QDR Execution Roadmap for Strategic Communication, 2006*: 5.
25. Max G. Manwaring, "Peace and Stability Lessons from Bosnia," *Parameters* (Winter 1998): 28-38.
26. Ralph O. Baker, "The Decisive Weapon: A Brigade Commander's Perspective on Information Operations," *Military Review* 86 (May-June 2006): 21.
27. Ibid.
28. Ibid.
29. Thomas F. Metz, et al., "Massing Effects in the Information Domain: A Case Study in Aggressive Information Operations," *Military Review* 86 (May-June 2006): 105.
30. Ireland and Hitt, 39.
31. Defense Science Board, *Report of the Defense Science Board Task Force on Strategic Communication*, 82.
32. U.S. Department of Defense, *QDR Execution Roadmap for Strategic Communication, 2006*, 7.
33. Metz, et al., 106.

Winning The War Of Perceptions: A Regional Approach To Implementing Interagency Strategic Communications

1. Government Accountability Office, *U.S. Public Diplomacy: State Department Lacks Certain Communications Elements and Face Persistent Challenges* (Washington DC: Government Accountability Office, May 2006, GAO Report 06-707T), 2.
2. Ibid.

3. Editors note: The publication of the *National Strategy for Public Diplomacy and Strategic Communication* occurred after the completion and submission of this paper. While that critical document addresses some of the authors concerns, its existence does not detract from the thesis or it's supporting research.

4. Lind William S., et al., "The Changing Face of War: Into the Fourth Generation," *The Marine Corps Gazette*, (October 1989): 22-26. In general terms, the fourth generation of warfare signifies war where one or more of the combatant parties are not nation states, but rather non-state actors, groups or networks affiliated by ethnicity, religion or ideology. For a more detailed analysis of Fourth Generation War see: Hammes, *The Sling and the Stone* (St. Paul, MN: Zenith Press, 2004), 1.

5. David J. Rothkopf, *Running the World: The Inside Story of the National Security Council and Architects of American Power*, (New York, NY, Public Affairs, 2006), 452. Rothkopf uses a variation of the old military maxim that "generals are always fighting the previous war" to argue that a deep human bias projects past experience onto new situations. For example, to assume that because an adversary or an ally or a battlefield is the same or similar, old rules still apply.

6. David W. Barno, "Challenges in Fighting a Global Insurgency," *Parameters*, 36 (Summer, 2006): 17. Barno highlights the essence of Hammes' definition of Third Generation War as the emergence in the 1920s and 30s of "blitzkrieg" and the age of maneuver warfare, with the offense once again gaining supremacy. This era of mounted mechanized maneuver continued from World War II through the Arab-Israeli wars of the 1950s and 60s, included Desert Storm in 1991 (perhaps its zenith), and culminated with the race to Baghdad in March 2003. For a more detailed analysis of both Third and Fourth Generation Warfare see: Hammes, *The Sling and the Stone* (St. Paul, MN: Zenith Press, 2004), 1.

7. Donald Rumsfeld, *New Realities in the Media Age: A Conversation with Donald Rumsfeld*, Council on Foreign Relations, New York, NY, 2006.

8. Ibid.

9. GAO Report 06-707T, 2.

10. Defense Science Board, *Report of the Defense Science Board Task Force on Strategic Communications* (Washington, D.C.: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, September 2004), 6.

11. Karen P. Hughes, "Testimony before the House Committee on Appropriations, Subcommittee on State, Foreign Operations, and Related Programs," April 19, 2007; http://www.state.gov/r/us/2007/83269.htm (accessed April 24, 2007).

12. Ibid.

13. Major Don Langley, "New "JPASE" sets the pace for joint military public affairs," Jan. 18. 2006; http://www.jfcom.mil/newslink/storyarchive/2006/pa011806.htm (accessed April 24, 2007).

14. Ibid.

15. Wilson, James Q, "Divided We Stand, Can a polarized nation win a protracted war?," *Commentary*, February 2006.
16. "Media Stakeout with Gen. Petraeus After a Closed Briefing with U.S. Senators," April 25, 2007, http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3950 (accessed April 25, 2007).
17. Defense Science Board, 19.
18. David W. Barno, "Challenges in Fighting a Global Insurgency," *Parameters*, 36 (Summer, 2006): 24.
19. Onn Winckler, "Middle Eastern Natural Environment," Yale University F&ES Bulletin, No.103, (1998): 461. While this reference is dated the data holds true today and has been cited by many in the Arab world including King Hussein of Jordan at the 2004 World Economic Forum.
20. "U.S. Denies POW Rescue Staged," 29 May 2003, http://www.cbsnews.com/stories/2003/05/29/iraq/main556060.shtml (accessed 3 June 2007). This CBS report questions the motives behind the videotaped rescue of PFC Jessica Lynch from an Iraqi hospital in the early days of Operation Iraqi Freedom. The House Oversight and Government Reform Committee held hearing on this matter in May 2007. For insight into the effects of insurgent videos posted to Internet services such as YouTube see: Edward Wyatt, "Anti-U.S. Attack Videos Spread on Web," October 6, 2006 http://www.nytimes.com/2006/10/06/technology/06tube.html?ex=1180929600&en=ee80864d59062544&ei=5070 (accessed June 3, 2007).
21. Government Accountability Office, *Interagency Coordination Efforts Hampered by the Lack of a National Communication Strategy* (Washington DC: U.S. Government Accountability Office, GAO Report 05-323, April 2005), 5.
22. Hughes. According to Hughes, the Rapid Response Unit constantly monitors international media, informs American policy makers with a concise daily report of what is driving world news from the Middle East to Latin America, and provides our U.S. position on those issues to an email list of several thousand senior officials, from Cabinet secretaries to military commanders.
23. Robert J. Dolan, *Strategic Marketing Management* (Boston MA: Harvard Business School Press, 1991), 111. In this business school text, Dolan offers an excellent overview of niche marketing. In a compilation of essays titled "The Media of Diaspora," author Hamid Naficy explores narrowcasting relative to engaging minority audiences through the medium of television. Naficy offers some very insightful ideas and they have broad applicability regardless of the message delivery medium. For a more detailed review see: Karim Haiderali Karim, ed. The Media of Diaspora, (London, UK: Routledge, 2003), 52.
24. Defense Science Board, 25. The report points to the Office of Global Communications (OGC) and the Strategic Communications Policy Coordinating Committee (PCC) as examples of lackluster interagency coordination. At the time the report was published the OGC had devolved into a second tier

organization devoted principally to tactical public affairs coordination and had failed to engage in strategic direction, coordination, and evaluation. The PCC, despite its authority which included interagency support for international broadcasting, foreign information programs, and public diplomacy as well as the development of strategic communications capabilities throughout the government, had a marginal impact and at the time the report was published had not met for more than a year.

25. Ricky L. Rife, "Defense is from Mars State is From Venus," Research Project, (Carlisle Barracks: U.S. Army War College, 1998), 1. In his paper, Rife goes into significant detail on differences, cultural, organizational, etc…between DOD and DOS.

26. Tucker B. Mansager, "Interagency Lessons Learned in Afghanistan," *Joint Forces Quarterly*, 40 (1st Quarter, 2006): 81.

27. Joint Warfighting Center, U.S. Joint Forces Command, *Doctrinal Implications of the Joint Interagency Coordination Group*, (Suffolk VA: U.S. Joint Forces Command, 27 June 2004), 5. The pamphlet states that JIACGs provide a mechanism, through habitual relationships with civilian planners, to expeditiously integrate multi-agency operation planning that implements political-military missions and tasks. In short, the JIACG provides the requisite interagency perspective to the Combatant Commander in both joint planning and operations.

28. Joint Staff, Interagency, *Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations,* Vol. 1, (Washington DC: U.S. Joint Chiefs of Staff, 17 March 2006), xii.

29. Joint Staff (DJS), Joint Interagency Coordination Group (JIACG) Assessment, GENADMIN 010947ZApr02, 3; quoted in Matthew F. Bogdanos, "Joint Interagency Cooperation: The First Step," *Joint Forces Quarterly*, 37 (2nd Quarter, 2005): 14.

30. Department of State/USAID, Joint Strategic Plan 2007-2012, (Washington DC: U.S. Department of State, April 2007), 58.

31. GAO Report 05-323, 16.

32. Ann Scott Tyson, "A U.S. Proconsul in Afghanistan," July 29 2004, http://www.csmonitor.com/2004/0729/p06s01-wosc.html (accessed April 27, 2007).

33. Matthew F. Bogdanos, "Joint Interagency Cooperation: The First Step," *Joint Forces Quarterly* 37 (2nd Quarter, 2005): 15.

34. Defense Science Board, 62.

35. This and the following accounts of activities of the communications coordination group in Afghanistan come from the author's experiences as the director of public affairs for Combined Forces Command-Afghanistan from November 2003 to May 2004.

36. Mansager, 82.

37. The Afghanistan Reconstruction Group (ARG) was created by the National Security Council to take a non-traditional approach to reconstruction efforts in Afghanistan. The ARG brought high-ranking former U.S. private-sector executives and government employees to serve in the embassy in Kabul. The ARG's charter was to apply its private-sector experience and expertise in an advisory role to both the U.S. government and the Afghan government.

38. "U.S. Afghan Envoy Angers Pakistan," April 6, 2004, http://news.bbc.co.uk/2/hi/south_asia/3603885.stm (accessed May 29, 2007).

39. "U.S. Concern at Pakistani Strategy," 3 May 2004, http://news.bbc.co.uk/2/hi/south_asia/3679699.stm (accessed May 29, 2007).

40. Levon Sevunts, "Hammer Often Mightier Than Sword," *The Washington Times,* May 29, 2005, http://washingtontimes.com/world/20050529-112421-5433r.htm (accessed May 29, 2007). This Washington Times article offers a balanced view of the mission of a PRT.

41. "New Provincial Reconstruction Team Opens in Afghanistan," March 4, 2004, http://www.globalsecurity.org/military/library/news/2004/03/mil-040304-centcom02.htm (accessed June 3, 2007).

42. Ibid.

43. Department of the Air Force, Public Affairs Operations, Air Force Doctrine Document 2-5.3 (Washington, D.C.: U.S. Department of the Air Force, 24 June 2005), 41.

44. Christopher Griffin, "A Working Plan: Hope isn't the only strategy for Afghanistan," *Armed Forces Journal*, April 2007, http://www.armedforcesjournal.com/2007/04/2587549 (accessed April 28, 2007). Griffin offers an insightful analysis of the interagency process that occurred in Kabul under the tenure of both Ambassador Khalilzad and Lieutenant General Barno. He also underscores the sobering loss of interagency cooperation that resulted when both leaders departed the country.

Section Two – Information Effects in the Physical Domain

Introduction

1. Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare* (Washington DC: Office of the Secretary of Defense, Office of Force Transformation, 2005), 20.
2. Department of Defense, "Quadrennial Defense Review Report" (Washington DC: Office of the Secretary of Defense, February 6, 2006): 58
3. Office of the Secretary of Defense, *The Implementation of Network-Centric Warfare*, 11.

Always On: Achilles Heel Of The Networked Force?

1. Mohamad Bazzi, "Hezbollah cracked the code; Technology likely supplied by Iran allowed guerrilla to stop Israeli tank assaults," *New York Newsday*, 19 September 2006, www.lexis-nexis.com (accessed December 27, 2006).
2. John B. Tisserand III, *Network Centric Warfare Case Study: U.S. V Corps and 3rd Infantry Division (Mechanized) during Operation Iraqi Freedom Combat Operations (March to April 2003) Volume III: Network Centric Warfare Insights* (Carlisle Barracks PA: U.S. Army War College, 28 August 2006), 21.
3. U.S. Department of Defense, Department of Defense Dictionary of Military and Associated Terms, Joint Publication JP 1-02 (Washington DC: U.S. Department of Defense, 12 April 2001, amended through 8 August 2006), 548.
4. Tisserand, C-1.
5. Donald H. Rumsfeld, *The National Defense Strategy of the United States of America* (Washington DC: U.S. Department of Defense, 2005), 5.
6. U.S. Joint Chiefs of Staff, Richard B. Myers, Chairman, *National Military Strategy of the United States of America* (Washington DC: U.S. Department of Defense, 2004), 6.
7. Colin S. Gray, *Recognizing and Understanding Revolutionary Change in Warfare: The Sovereignty of Context* (Carlisle PA: Strategic Studies Institute, U.S. Army War College, 2006), 46.
8. Abraham Marcus and William Marcus, *Elements of Radio,* ed. Ralph Horton (New York: Prentice-Hall, 1948), 5.
9. Joseph D. Modell, *Transmitter Hunting: Radio Direction Finding Simplified* (New York: McGraw-Hill, 1987), 1-3.
10. Anthony Brown, *Bodyguard of Lies: The Extraordinary True Story Behind D-Day* (Guilford, CT: The Lions Press, 2002), 22.

11. Ibid., 56.
12. Ibid.
13. David Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet* (New York: Scribner, 1996), 504-5.
14. Ibid., 270.
15. Dr. Alfred Price, *War in the Fourth Dimension* (London: Greenhill Books and Mechanicsburg, PA: Stackpole Books, 2001), 25.
16. Admiral Sandy Woodward with Patrick Robinson, *One Hundred Days: The Memoirs of the Falklands Battle Group Commander* (Annapolis, MD: Naval Institute Press, 1997), 3.
17. Ibid., 5.
18. Ibid., 3-20.
19. U.S. Department of the Army, *Communications Techniques: Electronic Counter-Countermeasures*, Army Field Manual FM 24-33 (Washington DC: U.S. Department of the Army, 17 July 1990), Ch. 2, Sec. 2-1 b.
20. U.S. Department of the Navy, Navy Electricity and Electronics Training Series Module 17—Radio-Frequency Communications Principles, Navy Publication NAVEDTRA 14189, September, 1998) 3-37.
21. Tisserand, 1.
22. Bazzi.
23. David A. Fulghum, "Doubt As a Weapon; Lebanon fighting produced an information warfare coup for Hezbollah and Iran," *Aviation Week & Space Technology*, November 27, 2006, www.lexis-nexis.com (accessed December 27, 2006).
24. Bazzi.
25. Ibid.
26. "We Finally Get our Paws on PlayStation 3," *IEEE Spectrum Online*, December 20, 2006, http://spectrum.ieee.org/dec06/comments/1668 (accessed March 29, 2007).
27. Geoffrey James, "The war at home; How the war in Iraq is changing the relationship between defense and commercial electronics," *Electronic Business*, January 1, 2006, www.lexis-nexis.com (accessed December 27, 2006).
28. The International Monetary Fund's proposed definition for globalization is "the growing economic interdependence of countries world-wide through the increasing volume and variety of cross-border transactions in goods and services and of international capital flows, and also through the more rapid and widespread diffusion of technology." See Terrence R. Guay, *Globalization and*

Its Implications for the Defense Industrial Base (Carlisle Barracks PA: U.S. Army War College, February 2007), 1.

29. Alvin Toffler and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little, Brown, 1993), 3.
30. Gray, 20.
31. Ibid., 43.
32. Clarence A. Robinson Jr., "Position Fixing Methods Use Broadband Direction Finders," *Signal*, October, 1998, www.proquest.com (accessed December 27, 2006).
33. Jerrold M. Post, M.D., ed., Military Studies in the Jihad against the Tyrants: The Al-Qaeda Training Manual (Maxwell AFB, AL: USAF Counterproliferation Center, 2004), 86.
34. Lieutenant Genneral James F. Amos, "Marine Corps Operations in Complex and Distributed Environments," 11 January 2007, http://www.mcwl.quantico.usmc.mil/file_download.cfm?filesource=c:%5CMCWL_Files%5CC_P%5CDistributed%20Operations%20Summary%20dtd%20011107.pdf (accessed March 29, 2007).
35. Office of the Secretary of Defense, Annual Report to Congress – Military Power of the People's Republic of China 2006 (Washington, D.C.: U.S. Department of Defense), 6, 22.
36. Geoffrey James captures how advanced technology becomes available when he states, "...the need to make NCW happen quickly, at a reasonable cost, increases the speed with which technology gets transferred to the commercial sector. This, in turn, means that mainstream semiconductor firms will be able to bring commercial products based on NCW-related technology to the market far sooner than would otherwise be possible."
37. Associated Press, "Gates Voices Concern About U.S. Education," *New York Times*, March 8, 2007, http://www.nytimes.com/2007/03/08/business/ 08gates.html?ei=5088&en=db607b26877228ae&ex=1331010000&partner=rssnyt&emc=rss&pagewanted=all (accessed March 29, 2007).
38. Gray, 14.
39. Gray, 24. Colin Gray states, "It is difficult for a proud and self-confidently dominant military power to accept the notion that there can be more than one contemporary military enlightenment."

Countering State-Sponsored Cyber Attacks: Who Should Lead?

1. George W. Bush, *The National Strategy to Secure Cyberspace*, February 2003, 1.
2. Department of Homeland Security, "Cyber Incident Annex," National Response Plan, (Washington, D.C., Homeland Security Office, August 2004), 2.

3. Stephen J. Lukasik, Seymour E. Goodman and David W. Longhurst, *Protecting Critical Infrastructures Against Cyber-Attack*, (Oxford University Press for The International Institute for Strategic Studies, 2003), 7-10.
4. Justin Blum, "Hackers Target U.S. Power Grid; government Quietly Warns Utilities to Beef Up Their Computer Security [Final Edition]," *The Washington Post*, Mar 11, 2005: sec E.01, www.proquest.com (accessed February 6, 2007).
5. Josh Rogin, "Air Force to Create Cyber Command," FCW.com, Nov 13, 2006, 2, http://www.fcw.com/article96791 (accessed December 4, 2006).
6. Ibid.
7. Lukasik, Goodman and Longhurst, 23-24.
8. Rogin, 3.
9. Chris Gonsalves, "DOD Attacks Renew Fears; Speculation Swirls about Cyber-terrorism," *eWeek*, Vol 22, Issue 35, September 5, 2005 (New York), 37, www.proquest.com (accessed February 6, 2007).
10. White House, *The Federal Response to Hurricane Katrina: Lessons Learned* (Appendix A.1) (Washington, D.C.: The White House, 23 February 2006), 87, http://www.whitehouse.gov/reports/katrina-lessons-learned.pdf (accessed February 27, 2007).
11. Bush, 48.
12. Ibid., 6.
13. Ibid., viii.
14. Ibid., 2.
15. "Department of Homeland Security Releases Cyber Storm Public Exercise Report," U.S. Federal News Service, Including U.S. State News (Washington, D.C., September 13, 2006) www.proquest.com (accessed February 6, 2007).
16. Bush, 6.
17. "DHS Conducts First Full-Scale Cyber Security Exercise," Defense Daily, (Potomac: Feb 15, 2006, Vol 229, Issue 30): 1, www.proquest.com (accessed February 6, 2007.
18. Ibid., 2.
19. Michael Vatis, "International Cyber-Security Cooperation," in *Cyber Security: Turning National Solutions into International Corporation*, ed. James Lewis, Volume 25, Number 4, (Center for Strategic and International Studies Press, 2003): 14.
20. Bush, viii.
21. Ibid.
22. Rogin, 1-2.

23. Army War College, *Information Operations Primer*, AY07 Edition (November 2006): 83.
24. Clay Wilson, "Information Operations and Cyberwar; Capabilities and Related Policy Issues," in Congressional Research Service, Library of Congress, 2006): 7-8.
25. Army War College, *Information Operations Primer*, 87-90.
26. Bush, xiii.
27. "DHS Conducts First Full-Scale Cyber Security Exercise," Defense Daily, (Potomac: 15 Feb 2006, Vol 229, Issue 30) www.proquest.com (assessed February 6, 2007): 1.
28. Lukasik, Goodman and Longhurst, 51-52.
29. Bush, 41.
30. Lukasik, Goodman and Longhurst, 35.
31. Ibid.
32. Lukasik, Goodman and Longhurst, 59-60.
33. Ibid., ix.
34. Gonsalves, 37.
35. Bush, 39.
36. Lukasik, Goodman and Longhurst, 83-84.
37. Roger W. Barnett, "A Different Kettle of Fish: Computer Network Attack," in *Computer Network Attack and International Law*, ed. Michael N. Schmitt & Brian T. O'Donnell, 25-26 (Naval War College, Newport RI, 2002).
38. Bush, xii.
39. Wilson, 10.
40. Ibid., 11.
41. Department of Defense, Office of General Counsel, "Implications of Espionage Law" (Appendix VIII to *An Assessment of Legal Issues in Information Operations*) in *Computer Network Attack and International Law*, ed. Michael N. Schmitt and Brian T. O'Donnell (Naval War College, Newport RI, 2002), 516-519.
42. Thomas C. Wingfield and James B. Michael, The Naval Postgraduate School, An Introduction to Legal Aspects of Operations in Cyberspace, (Naval War College, Newport RI, 2004); 13.
43. Ibid.
44. Department of Homeland Security, "Cyber Incident Annex," *National Response Plan*, (Washington DC: Homeland Security Office, August 2004), 7.

45. "Department of Homeland Security Releases Cyber Storm Public Exercise Report," U.S. Federal News Service, Including U.S. State News, (Washington, D.C.: Sep 13, 2006) www.proquest.com (accessed February 6, 2007).

46. Bush, xii.

47. T*he Law of International Conflict: National Security Law in Cyber Space*, 2000, Aegis Research Corporation, 41-46.

48. Wingfield and Michael, 13.

49. Daniel B. Silver, "The Prospect that Law will be Clarified," in *Computer Network Attack and International Law*, ed. Michael N. Schmitt & Brian T. O'Donnell (Naval War College, Newport RI, 2002), 77-79.

50. Douglass C. Lovelace, "Key Strategic Issues List," Strategic Studies Institute, Army War College, July 2006, 41 & 50.

51. Donald Rumsfeld, *Strategy for Homeland Defense and Civil Support*, Department of Defense, June 2005, 26-27.

52. Horace B. Robertson, Jr., "Self-Defense Against Computer Network Attack," in *Computer Network Attack and International Law*, ed. Michael N. Schmitt & Brian T. O'Donnell (Naval War College, Newport RI, 2002), 132-133. "Computer network attacks as 'armed attacks.'" It is important that what is under discussion here is not what may be lawful in an ongoing armed conflict (jus in bello) but rather actions by hostile individual, group, or State against another State while the target state and the State of origin of the actions are not yet engaged in armed conflict (jus ad bellum). In an ongoing armed conflict (war), it is unquestionably legitimate for a State to attack its enemy's military telecommunications infrastructure, including military computer networks. Attacks on other telecommunications and network facilities which serve both military and civilian clientele legitimate military objectives, provided that the international humanitarian law of armed conflict is observed with respect to proportionality, including limiting collateral damage. It is a matter of indifference whether the mode of attack is kinetic or electronic, although the former may be more objectionable since it is more destructive and may cause more long-lasting effects. In examining whether a computer network attack "attack" may constitute an "armed attack," Article 51 cannot be construed in isolation but rather must be read in the context of other articles of the Charter, particularly Articles 2(4), 39, 41 and 42.

53. "DHS Conducts First Full-Scale Cyber Security Exercise," *Defense Daily*, (Potomac: 15 Feb 2006, Vol 229, Issue 30) www.proquest.com (accessed 6 February 2007):1.

54. Silver, 86. Sharp has proposed a rule that appears both sweeping and simple: Any computer network attack that intentionally causes any destructive effect within the sovereign territory of another state is an unlawful use of force within the meaning of Article 2(4) that may produce effects of an armed attack prompting the right of self defense.

55. David Tubbs, Perry G. Luzwick, and Walter Sharp, "Technology and Law: The Evolution of Digital Warfare International Law Studies," in *Computer Network Attack and International Law*, ed. Michael N. Schmitt & Brian T. O'Donnell (Naval War College, Newport RI, 2002), 6. "Despite the difficulties in application, I am persuaded that we will be well served by applying the core principles of international law to information age warfare. We cannot in our zest for tactical mission success, lose sight of our goals as a nation—to protect life and liberty, in our country and throughout the world."
56. "Department of Homeland Security Releases Cyber Storm Public Exercise Report," U.S. Federal News Service, Including U.S. State News (Sep 13, 2006 Washington, D.C.) www.proquest.com (accessed February 6, 2007).
57. Bush, vii.

Network Operations: the role of the Geographic Combatant Commands

1. XCOM is intended to refer to a notional Geographic Combatant Commander.
2. Joint Task Force–Global Network Operations (JTF-GNO) is charged by U.S. Strategic Command (STRATCOM) with carrying out STRATCOM's mission of operating and defending the Global Information Grid (assigned to STRATCOM in the 2006 Unified Command Plan).
3. U.S. Department of Defense, *Global Information Grid (GIG) Overarching Policy*, Department of Defense Directive 8100.1 (Washington, D.C.: U.S. Department of Defense, September 19, 2002), 8.
4. Net-centric is "relating to or representing the attributes of net-centricity. Net-centricity is a robust, globally interconnected network environment (including infrastructure, systems, processes, and people) in which data is shared timely and seamlessly among users, applications, and platforms. Net-centricity enables substantially improved military situational awareness and significantly shortened decision making cycles. Net-Centric capabilities enable network-centric operations and NCW." U.S. Department of Defense, *Data Sharing in a Net-Centric Department of Defense*, Department of Defense Directive 8320.2 (Washington DC: U.S. Department of Defense, 2 December 2004), 8.
5. Joint Task Force–Global Network Operations, Joint Concept of Operations for Global Information Grid NetOps, ver. 3 (Offutt Air Force Base NE, U.S. Strategic Command, 4 August 2006), 5. This document is referenced hereafter as Joint CONOPS for GIG NetOps, ver. 3.
6. Ibid., 7.
7. Ibid., 6.
8. Ibid., 10.

9. U.S. Department of the Army, *Draft Concept of Operations for LandWarNet (LWN) NetOps (NetOps)* (Washington DC, U.S. Department of the Army, 21 June 2006), 21. This diagram is a modified version of LandWarNet NETOPS Organization Structure. The diagram was modified to make it consistent with the other diagrams within this paper. Note that while this CONOPS is not yet finalized, it is the author's belief the items referenced will not change significantly, and the publication still provides a legitimate, Service-level reference.
10. U.S. Air Force, Air Force NetOps, United States Air Force Network Operations Functional Concept (Langley Air Force Base, VA: U.S. Air Force, Air Combat Command, 12 October 2006), 16. This diagram is a modified version of AFNetOps C2 Structure diagram. The diagram was modified to make it consistent with the other diagrams within this paper.
11. Ibid., 18.
12. Ibid.
13. U.S. Navy, Naval Network Warfare Command, Navy Concept of Operations for Global Network Operations, Version 1.0 (Norfolk VA, Naval Network Warfare Command, September 7, 2006), 13.
14. Ibid., 11.
15. Ibid., 12.
16. Ibid.
17. Lieutenant Colonel Benjamin J. Barris, CENTCOM J6, e-mail message to author, November 21, 2006.
18. Author's personal experience as the EUCOM Theater Network Defense Chief in 2005.
19. U.S. Joint Chiefs of Staff, Joint Communications System, Joint Publication 6-0 (Washington, D.C., U.S. Joint Chiefs of Staff, March 20, 2006), III-2.
20. Joint Publication 6-0, III-1.
21. Hunter Keeter, "DISA Stands Up Computer Network Defense Center," Defense Daily 203, no. 30 (August 12, 1999): 1, www.proquest (accessed October 3, 2006).
22. Deputy Secretary of Defense, "GIG Network Operations," Guidance and Policy Memorandum 10-8460, August 24, 2000, referenced in Joint CONOPS for GIG NetOps, ver. 3: 4.
23. Joint CONOPS for GIG NetOps, ver. 3, 24.
24. Joint Task Force–Global Network Operations, Joint Concept of Operations for Global Information Grid NetOps (Offutt Air Force Base NE, U.S Strategic Command, May 5, 2004), 22. This document is referenced hereafter as Joint CONOPS for GIG NetOps, Version 1.
25. Joint CONOPS for GIG NetOps, ver. 3, 11.

26. Ibid., 2.
27. Ibid., 11.
28. Ibid.,13
29. Ibid., 14.
30. Ibid.
31. Ibid.
32. Ibid.
33. Ibid., 3 and 14.
34. Ibid., 3.
35. General Support is the support provided by the supporting force to the supported force as a whole rather than to a particular subdivision of the supported force. U.S. Joint Chiefs of Staff, Unified Action Armed Forces (UNAAF), Joint Publication 0-2 (Washington DC, U.S. Joint Chiefs of Staff, July 10, 2001), III-10. Direct Support is a mission assigned to a force requiring support to another specific force and authorizing the supporting force to answer directly to the supported force's request for assistance (Ibid). This requirement to respond directly to the supported forces requests is a key distinction between Direct and General Support.
36. Joint CONOPS for GIG NetOps, ver. 3, 15.
37. Ibid., 3.
38. U.S Department of Defense, DoD Chief Information Officer Strategic Plan for Information Resources Management (Washington DC: U.S. Department of Defense, June 2004), 12.
39. U.S Department of Defense, Quadrennial Defense Review Report (Washington DC, U.S. Department of Defense, February 6, 2006), 70.
40. Ibid.
41. Noah Shachtman, "Hypersonic Cruise Missile: America's New Global Strike Weapon," *Popular Mechanics*, January 2007, http://www.popularmechanics.com/technology/military_law/4203874.html (accessed Dec 22, 2006).
42. Lieutenant Commander Julie R. Fluhr, NETWARCOM, N55, e-mail message to author, November 29, 2006.
43. Ibid.
44. Navy response to JTF-GNO's NetOps CONOPS.
45. Barris.
46. Ibid.
47. Colonel Jennifer L. Napper, J6, U.S. Pacific Command, *NETOPS Command and Control; A GCC Perspective* (Camp H.M. Smith HI: U.S. Pacific Command, March 2006), 5.

48. Ibid., 4.
49. Ibid.
50. Brandon Sade, EUCOM J6, e-mail message to author, October 11, 2006.
51. Briefing, NORTHCOM NetOps Discussion Points, 3
52. Barris
53. NORTHCOM Briefing, 4.
54. Briefing, Joint CONOPS for GIG NetOps, 02 Aug 2006, 10-12
55. UNAAF, vii.
56. During joint operations, the Joint Force Commander may set up his force with subordinate land (Joint Force Land Component Commander), air and space (Joint Force Air Component Commander) and sea (Joint Force Maritime Component Commander) commanders as fits his operation.
57. This proposal was adapted from a concept provided to JTF-GNO by EUCOM J-6 in response to the staffing of Joint CONOPS for GIG NetOps, ver. 3, August 4, 2006. The EUCOM proposal had the GCC as the supported command for all NetOps, and the SGNOSCs in direct support of the component 6's vice the JNOC.
58. U.S. Department of Defense, National Defense Strategy of the United States of America (Washington DC: U.S. Department of Defense, March 2005), 14.
59. Clark A. Murdock, et al., *Beyond Goldwater-Nichols: U.S. Government and Defense Reform for a New Strategic Era* Phase 2 Report (Washington DC: Center for Strategic and International Studies, July 2005), 82, 85-86.
60. General Peter J. Schoomaker, *Serving a Nation at War: A Campaign Quality Army with Joint and Expeditionary Capabilities* (Washington DC: U.S. Army Public Affairs, Army Strategic Communications, June 29, 2004), 19.

Winning The Peace: Building A Strategic Level Lessons Learned Program

1. B.H. Liddell Hart, *Strategy*, 2nd Revised Edition (New York: Meridian, 1991), 3-4.
2. Harry R. Yarger, "Strategic Theory for the 21st Century: The Little Book on Big Strategy," *The Letort Papers*, (February 2006): 18. Yarger further develops and expands on the concepts of V-U-C-A from the "Strategic Leadership Primer," prepared for the Army War College in 1998; Roderick R. Magee II, Editor.
3. Information superiority/dominance: the operational advantage derived from the ability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. (U.S.

Department of the Army, *Operations*, Field Manual 3-0, (Washington DC: U.S. Department of the Army, June 2001).

4. U.S. Department of Defense, Joint Operations, Joint Pub 3-0 and Joint Operations Planning, Joint Pub 5-0 (Washington DC: U.S. Department of Defense/Joint Staff, August 2006) discuss the phases of operations, within a military campaign, and provide detailed definitions of each of the phases (Phasing Model see Figure IV-9, Joint Pub 5-0).
5. See http://call.army.mil for command briefing, mission statement and organizational information on CALL and access to Army Lessons Learned repository and databases. Note: CALL also maintains a separate website to facilitate handling of CLASSIFIED information. This is accessible on the SIPRNET at: http://call.army.smil.mil.
6. See https://afknowledge.langley.af.mil/afcks/defaullt.asp for command briefing, mission statement, organizational information on USAF Lessons Learned cell and access to USAF Lessons Learned repository. NOTE: Access to Lessons Learned requires site registration.
7. See http://www.mccll.usmc.mil for command briefing, mission statement, organizational information on MCCLL and access to USMC Lessons Learned repository
8. See http://www.nwdc.navy.com/NLL/nllsoverview.aspx for command briefing, mission statement, organizational information on USN lessons learned cell and access to USN Lessons Learned repositories.
9. See http://www.jfcom.jwfc.mil/about/abt_j7.htm for information on the Joint Lessons Learned program. NOTE: most of JFCOM's actual lessons learned data, briefings and reports are only accessible through the SIPRNET.
10. ALSA products can be reached at https://wwwmil.alsa.mil. Access requires registration.
11. The Joint IED Defeat Organization (JIEDDO) was established in June 2005 as an activity of the Department of Defense (DoD). JIEDDO provides lessons learned Tactics, Techniques, and Procedures (TTP), Smart Cards and other products that can be accessed via CALL's SIPRNET website.
12. James Burack, William Lewis and Edward Marks, Workshop Directors, "Civilian Police and Multinational Peacekeeping–A Workshop Series: A Role for Democratic Policing," (Washington DC: National Institute of Justice, October 1997), 18.
13. "Beyond Goldwater-Nichols: Defense Reform for a New Strategic Era", Phase 1 Report, (Washington DC: Center for Strategic and International Studies, March 2004), 60-68.
14. Andrew Rathmell, et al, *Developing Iraq's Security Sector; The Coalition Provisional Authority's Experience* (Santa Monica CA: Rand Corporation/National Defense Research Institute, 2005), 4.

15. The Challenges Project, Meeting the Challenges of Peace Operations: Cooperation and Coordination (Elanders Gotab, Stockholm, 2005), 37, Item #8.
16. Ibid., 116, Item #6. See http://pbpu.unlb.org/pbpu.
17. Ibid., 16, Item #22.
18. U.S. Department of Defense, Unified Action Armed Forces (UNAAF), Joint Pub 0-2 (Washington DC: U.S. Department of Defense/Joint Staff, 10 July 2001), I-10.
19. The Challenges Project, 124, Item #24.
20. Thomas Gibbings, Donald Hurley and Scott Moore, "Interagency Operations Center: An Opportunity We Can't Ignore," *Parameters* 28, (Winter 1998-1999): 107.
21. Ibid., 102.
22. George W. Bush, Management of Interagency Efforts Concerning Reconstruction and Stabilization National Security Presidential Directive/ NSPD-44 (Washington DC: The White House, 7 Dec 2005).
23. Ibid.
24. Ibid.
25. Ibid.
26. The Clinton Administration's Policy on Managing Complex Contingency Operations: Presidential Decision Directive May 1997 (Washington DC, NSC White Paper). This document was rescinded by the Bush administration and replaced with NSPD-44; the guidance and direction for the interagency concerning lessons learned operations was captured and is available in the Handbook for Interagency Management of Complex Contingency Operations published by OASD (S&R). You can obtain a copy by calling 703-614-0421.
27. Ibid.
28. U.S. Department of Defense, Military Support for Stability, Support, Transition, and Reconstruction (SSTR) Operations DoD Directive 3000.05 (DODD 3000.05.) (Washington DC: U.S. Department of Defense/Office of the Secretary of Defense (OSD), 28 Nov 2005).
29. Ibid.
30. Kelly Houlgate, Major, USMC, "A Unified Command Plan for a New Era," (Carlisle Barracks PA: USAWC Selected Readings, *Implementing National Military Strategy*, Vol I, 5 Dec 2006–7 Feb 2007), 1-2. Major Houlgate introduces the concept of "massing expertise" as a capability goal for DoD and the military community. This concept or capability would also be a significant enabler for the SLLP.
31. The Challenges Project, 26, Item #59.

32. The Challenges Project, 115, Item #2.
33. Gibbings, et al. Parameters 28, 108.
34. From "PKSOI Organization Overview to Concept Plan." This concept plan was submitted as part of the initiative to transition PKSOI to a Field Operating Agency (FOA) under HQDA, G-3/5/7. The Organization Overview is Annex 3 to the Concept Plan.
35. The Challenges Project, 127, Item #38. The Pearson Peacekeeping Centre was established at the request of the Government of Canada in 1994. The International Association of Peacekeeping Training Centres (IAPTC) is an open and voluntary association of centres, institutions, and programs dealing with peace operations research, education, and training. It was initiated by Canada's Pearson Peacekeeping Center (PPC) in 1995. The IAPTC promotes better understanding of peacekeeping, its goals and objectives, and of the methods used in training for peace operations of all types. It is intended to broaden contacts between various international organizations, peacekeeping training centres and institutions, universities, and other interested groups, leading to more effective peace operations. See http://www.iaptc.org for details on IAPTC and the Pearson Centre. (Description of Pearson Centre and IAPTC above is taken from this website.)