

The Maxwell Papers



Maxwell Paper Anthology

Award-Winning
Papers AY 2010

Air University

Allen G. Peck, Lt Gen, Commander

Air War College

Robert C. Kane, Maj Gen, Commandant
Daniel Baltrusaitis, Col, PhD, Dean of Research
Michael Masterson, Lt Col, PhD, Series Editor

Air Force Research Institute

John A. Shaud, Gen, PhD, USAF, Retired, Director

Air University Press

Belinda Bazinet, Richard Bailey, Jerry Gantt,
Demorah Hayes, Jeanne Shamburger, Project Editors
Carolyn Burns, Sandi Davis, Tammi Long, Andrew Thayer, Copy Editors
Ann Bailey, Prepress Production
Daniel Armstrong, Cover Design
Daniel Armstrong, Illustrations

Please send inquiries or comments to:

Editor

The Maxwell Papers

Air War College

325 Chennault Circle, Bldg. 1401

Maxwell AFB, AL 36112-6006

Tel: (334) 953-7074

Fax: (334) 953-1988

<http://www.au.af.mil/au/awc/awcgate/awc-mxwl.htm>

AIR UNIVERSITY
AIR WAR COLLEGE



Maxwell Paper Anthology
Award-Winning Papers AY 2010

Air University Press
Air Force Research Institute
Maxwell Air Force Base, Alabama

April 2011

20110727017

This Maxwell Paper and others in the series are available electronically at the Air University Research Web site <http://research.au.af.mil> and the AU Press Web site <http://aupress.au.af.mil>.

Disclaimer

Opinions, conclusions, and recommendations expressed or implied within are solely those of the authors and do not necessarily represent the views of Air University, the United States Air Force, the Department of Defense, or any other US government agency. Cleared for public release: distribution unlimited.

Air University Press
Air Force Research Institute
155 N. Twining Street
Maxwell AFB, AL 36112-6026

Contents

<i>Maxwell Paper</i>	<i>Page</i>
DISCLAIMER	ii
FOREWORD	v
ABOUT THE AUTHORS	vii
48 ARTICULATION BEYOND THE BUMPER STICKER: REVAMPING AN INCOMPLETE AND CONFUSING MASTER TENET	1
Col Rolanda Burnett Sr., USAF	
49 THE DANGEROUS DECLINE IN THE US MILITARY'S INFECTIOUS-DISEASE VACCINE PROGRAM	17
Col Kenneth E. Hall, USAF	
50 LEGAL AND ETHICAL ASPECTS OF THE DECISION FOR WAR: A CASE STUDY	39
Lt Col Michael Rafter, Canadian Forces	
51 DEVELOPING A US EUROPEAN COMMAND INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE STRATEGY FOR FY 2010-15 ...	55
Lt Col Kevin M. Coyne, USAF	
52 INFLUENCE OPERATIONS AND THE INTERNET: A 21ST CENTURY ISSUE: LEGAL, DOCTRINAL, AND POLICY CHALLENGES IN THE CYBER WORLD	69
Col Rebecca A. Keller, USAF	
53 US NATIONAL SECURITY AND ENVIRONMENTAL CHANGE IN THE ARCTIC	85
Lt Col Lars Helmrich, Swedish Air Force	
54 CONSIDERATIONS FOR A US NUCLEAR FORCE STRUCTURE BELOW A 1,000-WARHEAD LIMIT	101
Lt Col David J. Baylor, USAF	

<i>Maxwell Paper</i>	<i>Page</i>
55 GETTING WAR FIGHTERS WHAT THEY NEED, WHEN THEY NEED IT.	119
Col Carl E. Schaefer, USAF	
56 DEVELOPING A SITUATION AWARENESS ENVIRONMENT FOR THE DISTRIBUTION PROCESS OWNER: RECOMMENDATIONS FOR US TRANSPORTATION COMMAND.	137
Lt Col James Michael Doolin, USAF Reserve/YC-3, DAF civilian	
57 THE NEED FOR A GLOBAL SPACE-TRAFFIC- CONTROL SERVICE: AN OPPORTUNITY FOR US LEADERSHIP	153
Lt Col Matthew C. Smitham, USAF	
58 READY OR NOT? REPEAL OF "DON'T ASK, DON'T TELL"	171
Col Julie C. Boit, USAF	
59 SCIENCE AND TECHNOLOGY INTELLECTUAL CAPITAL: A CRITICAL US ASSET	189
Col Stella T. Smith, USAF	

Foreword

It is my pleasure to introduce the Air War College *Maxwell Paper Anthology*, a compilation of the award-winning papers from our 2010 graduates. Since we published the first Maxwell Paper in May 1996, we have distributed 47 papers demonstrating the highest level of analytical creativity and scholarship. The 12 papers presented here provide insight into and promote discussion on topics of importance to senior leaders.

In the opening paper, Col Rolanda Burnett argues that the Air Force master tenet of centralized control with decentralized execution is no longer applicable. He highlights the tenet's key doctrinal strengths and weaknesses and explains how it can be improved. In the next paper, Col Kenneth Hall describes how the emphasis on bio-engineered threats since 9/11 has had unintended consequences for the US vaccination program. He concludes that we are all at great risk because of inattention to common diseases that affect our entire population. Our Canadian international fellow, Lt Col Michael Rafter, analyzes the legal and ethical implications of the United States' 1970 incursion into Cambodia to determine if it was justified.

Several of our papers address the influence of emerging technology and trends on US security strategy. Lt Col Kevin Coyne examines the US European Command's intelligence, surveillance, and reconnaissance (ISR) strategy and suggests a road ahead for ISR integration. Col Rebecca Keller analyzes the intersection of influence operations (IO) and cyberspace operations. She identifies current operational and legal constraints on the execution of IO using cyber technology and offers remedial actions to enhance the use of the Internet as a military IO tool in today's cyber world. Another international fellow, Lt Col Lars Helmrich of the Swedish air force, critiques US Arctic policy and argues for an increased leadership role for the United States. Lt Col David Baylor analyzes the strategic implications of a reduction in nuclear weapons and asks the important question "Are there different negotiation considerations and dynamics in play when Russia and the United States go below 1,000 strategic warheads?" These papers all tackle the influence of change on the strategic environment while another batch addresses how change should influence the Department of Defense (DOD). Col Carl Schaefer assesses the DOD's procurement system and concludes that the services could learn from the Special Operations Command's streamlined acquisition system. Lt Col James Michael Doolin evaluates technologies to meet the US Transportation Command's need for a situational aware-

ness tool. And Lt Col Matthew Smitham argues that the time is ripe for a US-led space traffic control system.

Our anthology closes with a pair of papers that address DOD human capital challenges. Col Julie Boit analyzes the "Don't Ask, Don't Tell" policy and offers specific policy implementation recommendations for the DOD. Col Stella Smith examines the potential loss of intellectual capital as measured by the number of undergraduate and graduate degrees earned in science, technology, engineering, and mathematics. Her analysis suggests dire consequences for the US technical base and our ability to deter future adversaries if this critical capability is allowed to atrophy.

The Maxwell Paper compendium provides a short summary of the best research at Air War College. I hope you will find that the papers stimulate thinking and discussion on a wide range of topics. As with all Maxwell Papers, the Air War College publishes this anthology in the spirit of academic freedom and open debate. We encourage your engagement on the issues raised by the papers in this collection and solicit your responses.

A handwritten signature in black ink, appearing to read 'R. Kane', with a large, stylized flourish extending from the end.

ROBERT C. KANE
Major General, USAF
Commandant, Air War College

About the Authors

Lt Col David "DJ" Baylor is assigned to Air Combat Command (ACC), Langley AFB, Virginia. His assignments include weapons and tactics officer and scheduler, 79th Fighter Squadron, Royal Air Force (RAF) Upper Heyford, England, and instructor weapon system officer (WSO), training officer, and wing scheduler, 522d Fighter Squadron, Cannon AFB, New Mexico. At the 34th Bomb Squadron, Mountain Home AFB, Idaho, he was the chief of plans, responsible for the development of a "light strike" deployment package that became the standard for deployment of all B-1 units; to prove his concept, Colonel Baylor led two deployments to Shaikh Isa AB, Bahrain. For his innovative solutions to deploying the B-1, Twelfth Air Force twice nominated Colonel Baylor and his crew for the Curtis E. LeMay Trophy; his team won ACC's outstanding bomber crew trophy in 1998.

Colonel Baylor has also served as an instructor WSO and flight commander at the B-1 schoolhouse, Dyess AFB, Texas, and later as the 7th Operations Group executive officer and assistant director of operations for the 9th Bomb Squadron, where he participated in Operation Enduring Freedom in 2002; the commander's nuclear strike advisor and Mobile Consolidated Command Center chief, US Northern Command; and commander and professor of aerospace studies, The University of Georgia. He holds a BS, mechanical engineering, Pennsylvania State University, where he was a Distinguished Graduate (DG), Air Force Reserve Officer Training Corps; master of military operational art and science, Air Command and Staff College, Maxwell AFB, Alabama, where he was a DG; and master of strategic studies, Air War College, Maxwell AFB.

Col Julie C. Boit is assigned to Headquarters Air Force, The Pentagon, Washington, DC. As a career personnel officer, she has served in several stateside and overseas assignments, including base-level tours at Kelly AFB, Texas; Kunsan AB, Republic of Korea; and RAF Mildenhall, UK. Colonel Boit has commanded at the flight, detachment, and squadron levels, leading the Military Personnel Flight, RAF Lakenheath, UK; Detachment 2, United States Air Forces in Europe (USAFE) Mission Support Squadron, Italy; and 437th Mission Support Squadron, Charleston AFB, South Carolina. Additionally, she has served at Headquarters Air Force Personnel Center, Randolph AFB, Texas, and at Headquarters European Command, Stuttgart, Germany. She is a graduate of the US Air Force Academy and earned a master's degree in business administration from St. Mary's University, San Antonio, Texas; a master's degree in National Security and Strategic

Studies from Naval War College, Newport, Rhode Island; and a master's degree in Strategic Studies from the Air War College in 2010.

Col Rolanda Burnett Sr. is a foreign affairs specialist with the Office of the Secretary of Defense. He was the deputy chief, Air and Space Operation Center Requirements Division, Requirements Directorate, Air Combat Command headquarters staff, Langley AFB, Virginia, and commanded the 705th Training Squadron, 505th Command and Control Group, and 505th Command and Control Wing, Hurlburt Field, Florida. At the 609th Combat Plans Squadron and Headquarters Ninth Air Force, United States Central Command Air Forces, Colonel Burnett was pivotal in developing and executing the air campaign strategy in support of Operation Iraqi Freedom.

His other assignments include the 912th Air Refueling Squadron, Robins AFB, Georgia, where he deployed in support of multiple operations to include Desert Calm and Restore Hope; Kadena AB, Japan, where he was chief of navigation training, standardization and evaluation/instructor navigator, and flight commander/instructor navigator; and the 54th and 55th Air Refueling Squadrons, Altus AFB, Oklahoma, where he served as a Combat Crew Training School (CCTS) instructor navigator, executive officer, flight commander, and chief CCTS evaluator navigator. Colonel Burnett is a graduate of Air War College; the Army Command and General Staff College, Leavenworth, Kansas; and the School of Advanced Airpower Studies, Maxwell AFB.

Lt Col Kevin M. Coyne is a career intelligence officer with 20 years of signals intelligence experience at the operational and headquarters levels. He is the chief of the Intelligence, Surveillance, and Reconnaissance Policy Division, the Pentagon. He has served as commander, 390th Intelligence Squadron (IS), Kadena AB, Japan; board chair, Joint Staff/J2 Battlespace Awareness Functional Capabilities; and operations officer, 488th IS, RAF Mildenhall, UK. Prior to this, Colonel Coyne was the RC-135 program element monitor at the Pentagon, responsible for supporting aircraft and sensor procurement for all variants of the RC-135 fleet. At the 97th IS, Offutt AFB, Nebraska, he served as chief, Current Operations, and chief, Force Applications, providing airborne cryptolinguist support to RC-135 Rivet Joint, Cobra Ball, and Combat Sent operations.

At Headquarters USAF, he served as an intelligence watch officer and as a focal point for intelligence relationships with NATO partners, overseeing the functional employment of theater signals intelligence systems and working reconnaissance employment issues. Colonel Coyne served as a flight commander at signals intelligence units in Korea and Greece supporting U-2 and RC-135 operations. He has

deployed in support of Operations Iraqi Freedom, Southern and Northern Watch, and NATO's Bosnia Implementation Force.

James Michael "Mike" Doolin led the chief information officer (CIO) Support and Distribution Portfolio Management Division, Command, Control, Communications, and Computer Systems Directorate, US Transportation Command (USTRANSCOM), Scott AFB, Illinois, where he was responsible for USTRANSCOM CIO support and management of the Department of Defense distribution information technology (IT) systems portfolio. Doolin is also a lieutenant colonel in the USAF Reserve, serving as a deputy operations center chief in the J3 at USTRANSCOM. Colonel Doolin recently served two years on active duty as a joint mobility operations officer in the Current Air Operations Branch of the USTRANSCOM Operations Center. These assignments enabled him to gain experience and insights into the daily operations of USTRANSCOM as the distribution process owner.

Doolin's combined civilian and military career spans over 34 years of federal service in the IT and logistics professions, including both line and staff assignments ranging from the squadron and group level as a traditional guardsman with the Hawaii Air National Guard to combatant command level as a civilian at both US Pacific Command and USTRANSCOM. He holds a master of science degree from Central Michigan University and is a 2010 graduate of Air War College.

Col Kenneth Hall is the deputy command surgeon, HQ USAFE, Ramstein AB, Germany. He has served as the commander of the 27th Special Operations Medical Group, Cannon AFB, New Mexico. Colonel Hall has supported numerous combat operations, including Operations Iraqi Freedom, Enduring Freedom, and Desert Storm. His other military positions include deputy command surgeon and command public health officer at Headquarters Air Combat Command, Aerospace Medicine Squadron commander, command public health officer and health promotion director at Headquarters United States Air Forces in Europe, chief of public health and prevention at the Air National Guard Readiness Center, medical inspector at the Air Force Inspection Agency, and base public health officer at state-side and overseas installations. Colonel Hall holds a bachelor's degree in biology from Virginia Tech, a doctorate in veterinary medicine from Auburn University, and a master's in public health from Harvard University and is a recent graduate of the Air War College. He is a chief Biomedical Sciences Corps officer and is board certified in veterinary preventive medicine.

Lt Col Lars Helmrich has been a pilot in the Swedish Air Force since 1990. Colonel Helmrich has served as commander of a Gripen squadron and as wing commander (flying). In 2008 he commanded

the Swedish Red Flag detachment. He is a graduate of the Swedish Defense College Staff Course and Senior Staff Course and is a recent graduate of Air War College.

Col Rebecca A. Keller is a career intelligence officer with one career broadening tour in the computer and communications career field. Her intelligence assignments have been varied and include signals and imagery intelligence, targeting, information operations, and collection management. Colonel Keller has served as a flight commander, operations officer, squadron commander, and deputy division chief on a major command staff. She was commissioned through the Air Force Reserve Officers' Training Corps, University of St. Thomas, St. Paul, Minnesota and is a recent graduate of Air War College.

Lt Col Michael Rafter is a member of the Canadian Forces. He has served on the North Atlantic Treaty Organization staff in the Allied Movement Coordination Center, Supreme Headquarters Allied Powers Europe, Mons, Belgium; as a United Nations peacekeeper in Haiti; and as an air mobility advisor to the African Union's Darfur Integrated Task Force, Addis Ababa, Ethiopia. His varied operational and headquarters assignments throughout Canada include postings to Kingston, Ontario; Goose Bay, Labrador; Winnipeg, Manitoba; Cold Lake, Alberta; Ottawa, Ontario; and Toronto, Ontario. As an air mobility officer, he qualified as a loadmaster on the C-130 Hercules aircraft and travelled extensively in support of Canadian Forces operations in the Arctic, the United States, Europe, Africa, and Australia.

He holds a bachelor of arts in history from the Royal Military College of Canada and completed his training as a logistics officer with a specialization in movements and transportation. Colonel Rafter has a master of arts in war studies and defence studies from the Canadian Forces Joint Command and Staff Program and a master of strategic studies from the USAF Air War College.

Col Carl Schaefer is the commander of the 46th Operations Group, Eglin AFB, Florida. He has served as a squadron commander, a T-38 instructor pilot (IP), and an F-15E IP and led combat missions during Operation Allied Force. Colonel Schaefer graduated from the USAF Test Pilot School in 2000 and has conducted developmental flight tests in the F-15, F-16, and T-38. A command pilot with over 2,800 hours in 30 aircraft types, Colonel Schaefer is a United States Air Force Academy, Air Force Institute of Technology, and recent Air War College graduate.

Col Stella Smith is the commander of the 552d Maintenance Group, Tinker AFB, Oklahoma. Her operational assignments include various aircraft maintenance positions at Griffiss, Kunsan, McChord, and Tinker Air Force Bases. She has also held staff assignments do-

ing research at the Air Force Logistics Management Agency, managing aircraft maintenance contracts for Air Education and Training Command, and serving as a Headquarters Air Force legislative liaison to the US House of Representatives.

Colonel Smith deployed in support of Operation Iraqi Freedom, standing up the strategic airlift maintenance capability at Balad, Iraq, as well as to Headquarters European Command in support of Operation Enduring Freedom. Colonel Smith commanded the 62d Logistics Support Squadron, 62d Maintenance Squadron, and 332d Expeditionary Aircraft Maintenance Squadron and was the deputy commander of the 552d Maintenance Group. She holds a bachelor's degree in Soviet area studies from the US Air Force Academy, a master's degree in maintenance management from the Air Force Institute of Technology, and a master of strategic studies degree from Air War College.

Lt Col Matthew C. Smitham is assigned to the Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, Space and Intelligence Capabilities Office, the Pentagon, Washington, DC, where he oversees major system acquisitions within the space and intelligence portfolios for the Department of Defense. He was the payload deputy program manager for a next-generation imaging satellite constellation at the National Reconnaissance Office, Chantilly, Virginia, and led a system program office that directed a contractor team in the development, integration, test, launch, and initialization of the mission payload.

Colonel Smitham has served in a variety of technical management, leadership, and staff positions in the Air Force. Previous assignments include Air Staff positions as a program element monitor and deputy division chief in the Directorate of Information Dominance, Assistant Secretary of the Air Force (Acquisitions), Washington, DC; research, development, and program management positions at the National Reconnaissance Office, Chantilly, Virginia, in the Advanced Science and Technology and Signal Intelligence Directorates; and scientific researcher to mitigate space weather impacts on US space systems at the Space Vehicles Directorate, Air Force Research Laboratory, Hanscom AFB, Massachusetts. He holds a BS in physics, University of Washington; an MS in engineering physics, Air Force Institute of Technology; an MA in military operational art and science, Air Command and Staff College, Maxwell AFB, Alabama; and a master of strategic studies, Air War College.

Articulation beyond the Bumper Sticker

Revamping an Incomplete and Confusing Master Tenet

*Col Rolanda Burnett Sr., USAF**

The US Air Force should adjust its time-honored master tenet for the employment of airpower: centralized control and decentralized execution (CC&DE). This Mosaic Law equivalent remains as valid today as when the airpower forefathers divined it amidst their operational context. It is, nonetheless, incomplete.

The United States conducts air operations over a wide spectrum of conflicts producing many varied conditions. Correspondingly, the military has adapted. From counterinsurgency operations to thermo-nuclear deterrence, America's strength has been the ability to create flexibility to effectively respond to the types of wars it may face. Why then should the Air Force assume its master tenet is the right approach to all operational contexts? Many Airmen view the master tenet as the only way to employ air and space power; however, restrictive doctrine and thinking have contributed to the master tenet's unenviable status as a "bumper sticker."

This paper considers why centralized control dominates an Airman's thinking, the doctrinal history of centralized control and current doctrinal concerns, how different operational contexts impact the Air Force's master tenet, key doctrinal strengths and weaknesses, and how the master tenet can be improved upon.

Why Centralized Control Dominates Airmen's Thinking

What is the basis for an Airman's total commitment to this age-old edict? Some may argue that the Airman's allegiance stems from fear—fear of losing the status of an independent service. Centralized control holds a special place in airpower history, underpinning the argument that led to an independent US Air Force in 1947. Therefore, if an Airman compromises—even one iota—on the master tenet, it would be tantamount to undermining the value of an independent US

*Gp Capt Raymond Goodall, Royal Air Force, was the essay advisor for this paper.

Air Force. Most would agree that airpower has come of age in the last 63 years, based on the experiences in World War II, Korea, Vietnam, and Iraq, with the chances of returning the Air Force back to the Army slim to none.¹ Nevertheless, dogged defense of centralized control may, in part, be explained by the fear of losing independence.

Paranoia is not the only explanation for an Airman's loyalty to the master tenet. The origins for such loyalty can be traced back to lessons learned by early airpower practitioners. As a result of the British experience prior to and during World War II and the US experience during that war, Airmen would rightly conclude that centralization (command and control) was the foundation to effective airpower operations.

British Experience

Following the Battle of France in 1940, numerous events shaped Britain's approach to the employment of airpower. The Battle of Britain, lessons learned in North Africa, numerous exercises, and technological advances all contributed to Britain's approach to joint operations. During the fall of 1940, exercises in Northern Ireland resulted in air support controls which embodied the technical and organizational means to enhance support of ground forces. Another development emphasized colocated army-air headquarters and a signals network that linked forward and rear airfields with the joint army-air headquarters and deployed army divisions and brigades. Sorting out the best of the emerging systems led to delays. Even more daunting was introducing these concepts in the crucible of battle against the Germans in North Africa during WWII. However, they proved effective once fully developed. A hybrid of the two systems, developed by Air Marshals Arthur William Tedder and Arthur "Mary" Coningham, gained acceptance in the summer of 1942.²

During Operations Compass's and Crusader's (autumn of 1940 through the winter of 1941–42) offensive operations against Italian forces in Libya, British airmen learned that colocating with army headquarters and leveraging technological advances in communications allowed airpower's flexibility to gain air superiority. This enabled airpower to be effective in the ground-support role by massing airpower at a decisive point. The new doctrine proved far superior to German blitzkrieg.³

"The success achieved is correctly attributed to the system devised by Air Chief Marshal Arthur Tedder and Air Vice Marshal Arthur Coningham, but the system alone was not antecedent to successful operations. . . . Continuous and intimate collaboration between Coningham and [Bernard] Montgomery [Eighth Army commander]

accounts for the triumphant application of airpower" in North Africa's Western Desert in 1942.⁴ The British learned that properly employing airpower in its different roles at the right place and time and in the right amount was far more advantageous than dividing airpower between the land commanders. Airpower's ability to morph during operations would not materialize if shackled by a ground commander who is (1) unable to think outside the ground force limitations; and (2) unable to consider the theater-wide picture—concerned only with one "fight"—and thus does not take advantage of opportunities to influence the fight outside the geographic "box."

To realize these advantages, airmen needed a mechanism to wield airpower to leverage its flexibility. The mechanism was central control, in the form of an airman who commanded air assets and was coequal and preferably colocated with the ground commander. Sadly, the Americans and British did not incorporate the lessons learned and executed by the British during Operation Torch, the massive operation in November 1942 that intended to remove the Axis forces from Northern Africa.

American Experience

An untested American airpower doctrine—Field Manual (FM) 31-35, *Aviation in Support of Ground Operations*—bounded the initial foray into joint and combined operations by the Americans and British. On paper it looked sound, with "a comprehensive tactical air control system: a central air command, a sophisticated network of ASC [air support control] centres and various levels of communications between the ground and air forces."⁵ However, the theory had not been exercised.

The doctrine's emphasis on corps-level support and the ground commander's decision authority for target priority and selection led to dispersion and subordination of air assets to the "narrow close-support interests of the ground commanders."⁶ Despite Britain's successful air operations in the Western Desert, Operation Torch planners did not consult with Tedder and Coningham, the chief architects, for advice. As a result, air assets were spread throughout the close battle, putting up an "air umbrella" (flying artillery) to protect ground units and thus preventing airpower from massing decisively. Strategic targets such as enemy aerodromes and ports, which could have had a more significant long-term effect on overall operations, were not considered high priority and thus were not engaged. Brig Gen Elwood "Pete" Quesada, 12th Fighter Command commander at the time, said that "there was an abundance of ignorance" from US Army Air Corps Airmen during Operation Torch.⁷

In contrast, Erwin Rommel massed Axis air assets and gained air superiority by outnumbering Allied forces at decisive points. With air superiority, Rommel eroded Allied defense in depth of key airfields and supply depots on the Algerian coast. Allied forces used two mountain ranges and their key passes to form defense in depth. By mid-February 1943, Rommel had driven Allied forces from the first mountain range, the Eastern Dorsal, and was advancing toward the Western Dorsal, the second mountain range, and one of its key passes, Kasserine. It was during the Kasserine crisis that a number of things changed.⁸

Allied forces reorganized, based on changes proposed at the Casablanca conference in January 1943. In essence, the British implemented lessons learned. Airpower was controlled centrally by an airman who was coequal with the ground commander. Gen Carl Spaatz established and commanded the Northwest African Air Force and was supported by Marshal Coningham, who commanded a subelement called the Northwest African Tactical Air Force (NATAF). With control of airpower, Coningham halted umbrella missions and concentrated forces against targets, achieving air superiority. With air superiority, the NATAF gained the upper hand as it punished Rommel while he retreated to the Eastern Dorsal after 20 February 1943. Operation Torch tactics changed to fit the British model and eventually resulted in the United States' wholesale embracement of the UK doctrine in the form of FM 100-20, *Command and Employment of Airpower*.⁹ "In short, the Americans adopted the British doctrine in toto," and Axis powers surrendered to US and British commanders two months after Operation Torch adopted these new command relationships.¹⁰

North Africa 1943—A Major Combat Operation

FM 100-20 is a product of its environment, which was unlimited in nature where overwhelming force was required to destroy the enemy to achieve military and strategic objectives.¹¹ Achieving air superiority, establishing airpower as a coequal to land power, and exploiting airpower's inherent flexibility to be concentrated at a decisive point were key advantages enabled by centralized control.¹²

Air superiority was necessary, as in most conflicts involving airpower. However, it is important to point out the context in which air superiority was gained. Air superiority for the Allied forces was not a given; it had to be wrestled from an enemy who possessed a legitimate air threat—one fully capable of gaining and maintaining air superiority for itself. Next, the operational environment allowed combatants to identify decisive points where concentrated combat power meant the

difference between success and failure. The environment favored an approach which leveraged the flexibility of airpower. Air commanders exploited decisive points because the nature of the fight was homogeneous, or consistent across the area of operations. Thus, the air commander was more likely to understand the operational pros and cons of flexibly applying airpower to meet the changing needs across operational areas.

The doctrine of centralized control was essentially formed in a conventional operational environment—force-on-force on a linear battlefield, a type of fight the United States has become very adept in prosecuting. Therefore, centralized control, through a single Airman commander, is rooted in validity. It is understandable why Airmen have created and clung to the master tenet. Given the conditions and operational context, centralized control was a logical and pragmatic approach to fully exploit airpower. The tendency of Airmen to default to centralized control is warranted. Centralized control is still relevant today; however, its relevancy does not necessarily mean it is without shortcomings.

Doctrinal History of Centralized Control and Decentralized Execution, 1954–2010

It is important to establish a background of post-WWII doctrine with regard to CC&DE because it serves as a foundation to evaluate and determine possible improvements. Historically, what does USAF and joint doctrine reveal about CC&DE?

In 1954 the USAF's doctrinal approach to managing air operations was "centralized overall direction and decentralized control of operations."¹³ In 1955 USAF doctrine described control in the context of command: when determining command relationships, "control should always be placed at a level which is fully able to employ the capabilities of the forces."¹⁴ In 1971 it changed to "aerospace forces must be centrally allocated and directed," and "mission control and execution of specific tasks must be decentralized."¹⁵ In 1975 the doctrine first used the terms *centralized control* and *decentralized execution* but added *coordinated effort*, a third pillar deemed fundamental to aerospace operations.¹⁶ In 1984 coordinated effort was not explicitly linked to CC&DE, and the dual-pronged master tenet became gospel for directing and executing aerospace forces.¹⁷ The 2003 version of doctrine continues to state the value of CC&DE. The language describing what has become CC&DE has been far from consistent over the years and has contributed to a culture of confusion concern-

ing the master tenet and its relationship to command. The confusion continues today.

Current Doctrine and Concerns

There is confusion over the relationship between command and control. The terms are mistakenly used interchangeably.¹⁸

Command

An overriding aspect to the debate over CC&DE is command. Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, defines *command* as “the authority that a commander in the Armed Forces lawfully exercises over subordinates by virtue of rank or assignment. Command includes the authority and responsibility for effectively using available resources and for planning the employment . . . , organizing, directing, coordinating, and controlling [of] military forces for the accomplishment of assigned missions. It also includes responsibility for health, welfare, morale, and discipline of assigned personnel.”¹⁹

While control is inherent to command, these terms are not synonymous. Command has to do with organizational issues. For example, should command of air assets be given to a single Airman, or should it be divided among commanders? Control has to do with operational issues, such as whether a single commander should centrally control air assets or “allow decentralized control so that lower echelon commanders can develop and implement plans in accordance with JFACC [joint force air component commander] intent.”²⁰ Command and control are distinct: it is clear from doctrine that control can be delegated, whereas command cannot. Just as the commander can delegate authority but not responsibility, so can a commander delegate control but not command. Command is the ability to give orders. Control is implementing those orders. Even though military terminology has tended to put them together, they are two distinct things. Since control is inherent to command, why does the USAF master tenet focus on centralized control instead of centralized command?

The following excerpt from a proposed revision in USAF doctrine continues the Air Force's long-standing focus on and fascination with control: “Centralized control empowers the JFACC to respond to changes in the operational environment.”²¹ Surely, the JFACC is the commander and does not need control to be empowered. It is the element of command that should be emphasized. This muddled interpretation of the relationship between command and control may be a

major source of confusion and may be why Airmen and the other services struggle to correctly understand the USAF's master tenet. USAF doctrine seems to have placed the emphasis on a part (control) rather than the whole (command).

Control

JP 1-02 defines control in two ways—at the operational and tactical levels. *Operational control* is defined as “organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission.”²² *Tactical control* is defined as “detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned.”²³

Both Air Force and joint air and space operations doctrine define control from a centralized perspective, espousing centralized control as the best way to conduct air operations. Air Force Doctrine Document (AFDD) 1, *Air Force Basic Doctrine*, defines *centralized control* as “the planning, direction, prioritization, synchronization, integration, and deconfliction of air and space capabilities to achieve the objectives of the joint force commander.”²⁴ JP 3-30, *Command and Control for Joint Air Operations*, also offers the virtues of centralized control. For example, it states that centralized control adds “coherence, guidance and organization to the air effort and the ability to focus the tremendous impact of air capabilities wherever needed across the theater of operations.”²⁵

Although doctrine portrays centralized control as beneficial, JP 3-30 implies other ways to control joint air operations: “Joint air operations are normally conducted using centralized control.”²⁶ However, there is no explanation of what “other than normal” might look like in practice. Effectively, doctrine views centralized control as not merely the best way, but the only way, to control air and space forces. Since current doctrine does not go into detail about how to control air operations other than centrally, it can be assumed that the conditions warranting something other than centralized control have never occurred (since doctrine is based on best practices during operations) or have not occurred enough to warrant inclusion into the USAF's codified system of best practices.

It is clear that within US doctrine there are differences in how control is viewed. JP 1-02 makes allowances for effective control of forces at the operational as well as the tactical level. Though not explicitly mentioned, this would include air and space forces. On the other hand, air and space operations doctrine, JP 3-30 and AFDD 1, re-

ports effective control only in the context of the operational (centralized) level.

Decentralized Execution

At first glance, doctrine regarding decentralized execution seems more unified and less confusing than either command or control. AFDD 1, JP 1-02, and JP 3-30 define execution in terms of decentralization. The doctrine explicitly defines decentralized execution but not execution. AFDD 1, JP 1-02, and JP 3-30 characterize decentralized execution as “delegation of execution authority.” However, AFDD 1 and JP 3-30 say that “decentralized execution helps achieve effective span of control and flexibility to deal with changes and uncertainty.”²⁷ Although execution seems straightforward, it is not.

As Daniel Baltrusaitis states in *Centralized Control with Decentralized Execution*, “Current AF doctrine fails to adequately and consistently define the central terms of command, control and execution. This causes major weaknesses in the debate over command, control and execution concepts because there is no agreed upon definition of the terms.”²⁸ This has led to varying interpretations.

In *Command in Air War*, Lt Col Michael Kometer observes that “what control is to one may be execution to another.”²⁹ Likewise, what may be centralized at one echelon of the organization could be viewed as decentralization to another. For example, I asked career-Air Force senior space officers about the nature of space operations with respect to control and execution. One concluded that space operated under decentralized command and centralized execution (notice the word *control* was not used), while another believed that space conformed to centralized control, decentralized execution.³⁰ In another example, the letter “C” in AWACS (Airborne Warning and Control System, a common reference to the E-3 Sentry), stands for *control*. To battle-manager crew members, this is an accurate, functional description of what they do at the tactical level. However, the combined air and space operations center (CAOC) may view those same activities, from the operational level, as decentralized execution.

This doctrinal analysis offers insight into the arguments over CC&DE, but it doesn’t answer all the questions. In fact it raises an important one: can something other than CC&DE be a better option for air and space operations? When we consider this question through the lens of differing operational environments, it adds clarity.

One Size Does Not Fit All

There are weaknesses with the master tenet. It is not the optimal approach for every situation—it is necessary but not sufficient to overcome the vast diversity of challenges posed by airpower employment across the spectrum of operations.

FM 100-20 represented the best way to use airpower—one might say an optimization—based on the operational environment of WWII. However, the conditions which shaped and led to centralized control were not universal. One could reason, then, given different operational circumstances and conditions, that centralized control may not be the optimal approach in conducting air operations. Control is a subset of command; therefore, it is reasonable to conclude that ideas on command could also apply to control. Martin van Creveld writes about varied contexts and the impact these variations have on so-called immutable laws of command. He suggests that since "command [is] so intimately bound up with numerous other factors that shape war, the pronouncement of one or more 'master principles' that should govern its structure and the way it operates is impossible."³¹

What about other operational environments? What are the differences, and how might they affect the conduct of air and space operations? Is CC&DE right for every situation—a counterinsurgency, for instance? Van Creveld also explains that "the fundamentals of command in conventional war may require modification, even inversion, in a counterinsurgency environment where purely military factors are less important than psychological and political ones."³² Gen James N. Mattis, commander, US Joint Forces Command, said of the current counterinsurgency in Afghanistan, "Times are changing. We are having to decentralize, in terms of decision making, decentralize in terms of assets. . . . It's wasteful but highly effective."³³ He characterized the type of war America is in as "not the American way of war. . . . It's outside our comfort zone. We have to overcome this as our reality meets the reality on the ground—not the reality as we want it to be but the reality as it exists."³⁴ So what is the reality of this war? What are the conditions that make it different from the conditions under which centralized control was forged?

The contextual divergence is staggering. First, counterinsurgencies are limited in nature, and the use of overwhelming force can possibly cause negative political fallout that can be detrimental to achieving military and strategic objectives. The United States and its allies had air superiority by default—the enemy posed no significant air capability. Next, the notion of a decisive point or points where massing combat capability decides the outcome is simply not applicable in a

counterinsurgency. If massing airpower is less advantageous, then the mechanism (centralized control) that enables the massing of airpower is also less advantageous.

The current insurgency in Afghanistan is comprised of many varied mini-insurgencies—each with different challenges and requiring tailored approaches. Afghanistan is a nation of ethnic tribes. It becomes difficult for a single commander to understand interrelationships between the mini-insurgencies as capability is moved between local insurgencies, as opposed to the homogeneity of the North Africa operation in WWII. It is reasonable to conclude that this type of operational environment may benefit from an increased level of decentralization. In fact, the land forces have done just that by “pushing” the planning down to the division and, in some cases, to the brigade.

The shift toward decentralization in response to the diverse nature of counterinsurgencies is understandable for land forces but does not apply to air and space power. This view is shortsighted and does not take into account many instances where the Air Force has departed from its master tenet, based on the conditions. For example, “Air Force participation in Operations Northern Watch, Southern Watch, Allied Force, and Deliberate Force emphasize [sic] the use of centralized execution to manage the application of air power [because of political influence and force protection requirements for coalition aircraft]. In each instance, the operation’s small scale [and] limited objectives . . . allowed the C/JFACC to pay individual attention to the execution of the air effort and thereby to achieve the desired political and military objectives.”³⁵

The context and environment influence choices on how to employ airpower. The experiences of Lt Col Clint Hinote, while serving as chief of strategy for the Central Command combined force air component commander responsible for surge operations in Iraq, convinced him that asking five questions can help determine how airpower is best controlled and executed: (1) What is the nature of the operation? (2) Where should flexibility be preserved? (3) How many assets are available? (4) What is the geographical range of effects? and (5) Who has the best situational awareness?³⁶ Properly answering and appropriately responding to the questions are necessary but not sufficient for improved command and control. Trust and cooperation between components are also critical.

Lack of Trust and Cooperation

The AF doctrinal approach to centralized control, coupled with Army trends in further decentralizing planning, has made it more difficult for air and ground planners to cooperate. A key characteristic of

centralized control is the Airman's approach to planning. Significant planning occurs centrally at the CAOC, although detailed planning also occurs at lower levels upon receipt of the air tasking order.³⁷ Historically, the Army's approach has been more decentralized through mission-type orders. This different approach has led to USAF deficiencies in planning entities for the Army at every echelon.³⁸

When critical Army planning occurs at the corps level, the USAF's doctrinal approach is appropriate and works relatively well, heavily impacting and shaping subordinate echelons such as in Operation Desert Storm.³⁹ The counterinsurgencies in Iraq and Afghanistan, however, have caused the Army to change. These insurgencies can be described as made up of differing insurgencies—each with its own specifics requiring its own approach. A senior leader at the Air Command and Control workshop describes the wars in Afghanistan and Iraq as not two conflicts but 12, the implication being that they are so different they should be considered as separate fights.⁴⁰

The components no longer operate in a coordinated fashion as they did during the first phase of Operation Iraqi Freedom. Instead of operating in support of the joint force commander's grand scheme of maneuver, they now operate in "a highly decentralized fight, driven largely by independent actions of lower level tactical commanders."⁴¹ What does all of this mean to the air component?

The absence of robust air planning capability at lower Army echelons results in Airmen not providing air expertise where it matters. Often, ground commanders do not realize all the benefits airpower could provide because air isn't an integral part of the planning. Sometimes this can cause ill-conceived and poorly executed operations. Lt Col William Pinter believes that "the air component needs to commit to developing the necessary resources to allow for the full degree of air-ground integration to occur at the lowest planning levels required for effective combat operations."⁴² Operation Anaconda highlighted operational weaknesses that can occur due to, among other things, a lack of integrated planning between air and ground forces.⁴³

Another negative is missed opportunities for the joint planning that fosters trust between air and ground components. The more the Army decentralizes, the more profound the issue becomes. With planning by land forces occurring at lower levels, it has become even more difficult for the air and land forces to plan together to best leverage what airpower can contribute. This has resulted in a perceived wider divide between air and ground planners.

Colonel Hinote comments that "not being in the mud" with the ground planners limits opportunities to build trust. "There are not many shared experiences between the air and ground. . . . There is no

sense of trust between air planners at the CAOC and ground planners at the many decentralized fights which are going on."⁴⁴ This general sentiment is shared by Colonel Kometer, who also served as chief of strategy in the Al Udeid CAOC.⁴⁵

Conclusions and Recommendations

From the analysis above flow three broad conclusions. The first is that the master tenet is incomplete; it does not address the variety of ways air and space power has been managed. Differing operational contexts have led to different, but valid, ways to conduct air and space power operations. For the most part they are not addressed in USAF doctrine. The second main conclusion is that USAF doctrine, although incomplete, is still relevant. As long as there remains the possibility of the United States engaging in major combat operations, CC&DE is an option. Third, confusion abounds over centralization, decentralization, command, control, and execution. The varied interpretations of these terms and how they relate reflect the profound complexities associated with conducting air and space operations.

Centralized command, flexible control, and flexible execution seem to be a sound basis from which to articulate airpower philosophy. The new and improved master tenet unequivocally places the emphasis on command. It recognizes centralized command as the most likely constant across the spectrum of air and space operations. Control is inherent to command; by emphasizing command, the confusion over how they relate can be lessened if not totally eliminated.

Control and execution, however, need to be flexible. Sometimes it may be best to centrally control and execute (e.g., nuclear deterrence mission); at other times, controlling and executing in a decentralized fashion (e.g., counterinsurgency operations) may be best. And there are times when they may fall somewhere in between this continuum. The issue of centralization and decentralization is a matter of degree when applied to control and execution. In *Command in Air War*, Colonel Kometer states that "control of airpower has varied among different types of wars and even among different missions within the same war."⁴⁶ Lt Gen Michael Short, USAF, retired, said as he recounted operations during Allied Force, "In the same ATO [air tasking order] some missions were centrally controlled and executed, and others were centrally controlled with decentralized execution."⁴⁷ Although useful, this simple tweak to the tenet is not enough.

Doctrine has to address, in detail, what is meant by *flexible*. This could be accomplished in a supplement that presents a contextual analysis by explaining the differing operational circumstances and their

impact in determining the best approach to conducting air operations. Airmen would then be better equipped to understand the centralization issue that dominates control and execution arguments. It would allow Airmen to discern the complex interplay between the pluses and minuses of centralization or decentralization, based on those who have experience. In short, it would add much-needed muscle, bone, and academic rigor to the current straw man of CC&DE.

Airmen have a hard time articulating beyond the bumper sticker, partly because the Air Force has failed to systematically document these complexities and their all-important implications. The Airman's understanding is stifled, lacking in-depth comprehension of command and control of air and space operations. USAF doctrine penetrates only surface deep and leaves much to be learned through trial and error or word of mouth. It is time the Air Force adjusted its master tenet to reflect those complexities. If it continues to allow the doctrine to be what amounts to a caricature of reality, its Airmen's ability to explain the doctrine will also be a caricature. Sadly, that amounts to nothing more than dogma.

Notes

1. Many lessons were learned in North Africa, Europe, and the Pacific theaters.
2. David Ian Hall, *Learning How to Fight Together*, AFRI Paper 2009-2 (Maxwell AFB, AL: Air University Press, 2009), 1-13.
3. *Ibid.*, 14-15.
4. *Ibid.*
5. *Ibid.*, 21.
6. *Ibid.*
7. Lt Gen Elwood R. Quesada, USAF, retired, interview by Col William R. Carter; Lt Col Price Bingham; J. A. Mowbray, PhD; Lt Col David McIsaac, USAF, retired; and Charles Westenhoff, Fall 1990, Maxwell AFB, AL. (Personal collection of J. A. Mowbray).
8. Shawn P. Rife, "Kasserine Pass and the Proper Application of Power," *Joint Force Quarterly*, no. 20 (Fall/Winter 1998-1999): 71-77.
9. *Ibid.*
10. Hall, *Learning How to Fight Together*, 25.
11. Lt Col Daniel F. Baltrusaitis, *Centralized Control with Decentralized Execution: Never Divide the Fleet?* Occasional Paper no. 36 (Maxwell AFB, AL: Center for Strategy and Technology, Air War College, 2004), 16, <http://www.au.af.mil/au/awc/awcgate/cst/cs36.pdf>.
12. Field Manual (FM) 100-20, *Command and Employment of Air Power*, 21 July 1943, 1.
13. Air Force Manual (AFMAN) 1-2, *United States Air Force Basic Doctrine*, 1 April 1954, 4.
14. *Ibid.*, 1 April 1955, 2.
15. AFMAN 1-1, *Basic Aerospace Doctrine of the United States Air Force*, September 1971, 2-2.
16. *Ibid.*, January 1975, 2-2.
17. *Ibid.*, March 1984, 2-20 and 2-21.

18. Baltrusaitis, *Centralized Control with Decentralized Execution*, 6.
19. Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001 as amended through 19 August 2009, http://www.dtic.mil/dod_dictionary/data/c/01087.html (accessed 5 December 2009).
20. Ibid.
21. Air Force Doctrine Document (AFDD) 1, *Air Force Basic Doctrine*, draft revision, 1 April 2010.
22. JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*.
23. Ibid.
24. AFDD 1, *Air Force Basic Doctrine*, November 2003, 28.
25. JP 3-30, *Command and Control of Joint Operations*, 5 June 2003, vii–viii.
26. Ibid., vii.
27. Ibid., 1–3; and AFDD 1, *Air Force Basic Doctrine*, November 2003, 28.
28. Baltrusaitis, *Centralized Control with Decentralized Execution*, 5.
29. Lt Col Michael Kometer, *Command in Air War: Centralized versus Decentralized Control of Combat Airpower* (Maxwell AFB, AL: Air University Press, 2007), 23.
30. Comments by Air Force senior space officers.
31. Martin van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1995), 261.
32. Ibid., 262.
33. Gen James N. Mattis, commander, US Joint Forces Command (speech, Air War College, 15 September 2009).
34. Ibid.
35. Baltrusaitis, *Centralized Control with Decentralized Execution*, 28–29.
36. Lt Col Clint Hinote, *Centralized Control and Decentralized Execution: A Catchphrase in Crisis?* (Maxwell AFB, AL: Air University Press, March 2009), 59–62.
37. The five deployable CAOCs are a direct result of centralized doctrine.
38. The Army's planning echelons include the corps, division, brigade, and company levels.
39. Lt Gen Eugene D Santarelli, USAF, retired (comments, Command and Control of Air and Space Power Forces course, Maxwell AFB, AL, 13 October 2009).
40. Maj Gen Maurice H. Forsyth, commander, Curtis E. LeMay Center for Doctrine Development and Education, and vice-commander, Air University (comments, Air Command and Control workshop, Maxwell AFB, AL, 13 October 2009).
41. Air Force/Marine Corps Tiger Team, *Air Force/Marine Corps Tiger Team Trip Report*, March 2008, 4.
42. Lt Col William E. Pinter, "Air-Ground Integration in the 21st Century: Improving Air Force Combat Capabilities and Theater Command and Control for Major Combat Operations and Irregular Warfare," Research report (Maxwell AFB, AL: Air War College, 2009).
43. HQ USAF/XOL, Office of Air Force Lessons Learned, *Operation Anaconda: An Airpower Perspective* (Washington, DC: DOD, 7 February 2005), 3–10.
44. Lt Col Clint Hinote (comments, Air Command and Control workshop, Maxwell AFB, AL, 13 October 2009).
45. Lt Col Michael Kometer (comments, Air Command and Control workshop, Maxwell AFB, AL, 13 October 2009).
46. Kometer, *Command in Air War*, 17.
47. Lt Gen Michael Short, USAF, retired (comments, Command and Control of Air and Space Power course, Maxwell AFB, AL, 9 December 2009).

Abbreviations

AFDD	Air Force doctrine document
ASC	air support control
ATO	air tasking order
AWCS	Airborne Warning and Control System
CAOC	combined air and space operations center
CC&DE	centralized control and decentralized execution
FM	field manual
JFACC	joint force air component commander
JP	joint publication
NATAF	Northwest African Tactical Air Force

The Dangerous Decline in the US Military's Infectious-Disease Vaccine Program

*Col Kenneth E. Hall, USAF**

For over 230 years, vaccines advanced by the US military research and development (R&D) community have dramatically reduced the impact of naturally acquired infections not only in America's armed forces but in society at large. In recent years, however, the military's infectious-disease vaccine program has lost considerable emphasis, funding, and mission capability. In the 1990s, with the burgeoning concern for weaponized bioagents in Iraq and North Korea, Congress turned its attention to combating biological threats of deliberate origin over those of natural causes. The Department of Defense (DOD) responded by partitioning its biodefense and infectious-disease vaccine acquisition programs, with biodefense vaccines holding a higher acquisition priority and receiving more robust funding than infectious-disease vaccines. The result has been a significant erosion of the DOD's ability to ensure the acquisition and availability of the right vaccines at the right time to optimally protect US forces from established and emerging natural infections now and in the future.¹

In this paper, I argue that the DOD needs to take swift actions to revitalize its infectious-disease vaccine program and enhance the synergy between biodefense and infectious-disease activities to resolve vaccine acquisition and availability shortfalls. Specifically, the DOD must collectively assess and prioritize all biological threats, whether natural, accidental, or deliberate in nature; consolidate redundant vaccine acquisition activities; elevate the priority of infectious-disease vaccines; and provide ample resources to sustain a robust vaccine acquisition capability to protect US military forces against validated and prioritized biological threats.²

In presenting the argument, I first make a case for why vaccines against natural infectious diseases, developed under US military R&D leadership, must remain a vital force health protection (FHP) imperative for safeguarding the war fighter and optimizing US military mission effectiveness. I then establish the historical impact of naturally occurring infectious diseases on military operations, the criticality of FHP in defending the human weapon system, and the superiority of vaccines among medical countermeasures. An analysis of the factors

*Col Gilbert Hansen, USAF, was the essay advisor for this paper.

hindering infectious-disease vaccine acquisition follows, including unbalanced threat assessment and mission focus, ineffective organization, insufficient funding, and inferior priority status. Finally, I recommend ways to enhance FHP vaccine acquisition and availability that will posture the DOD and America's military forces for twenty-first-century national security success.

Why DOD-Led Vaccines against Naturally Acquired Infections Are Vital

Throughout America's wars, naturally acquired infectious diseases—many preventable by vaccine—have eclipsed bombs and bullets as the culprits of morbidity, mortality, disability, and mission degradation. This section investigates the criticality of infectious-disease vaccines in protecting force health and explains why US military R&D leadership is vital to their development.

Historical Impact of Infectious Diseases on US Military Readiness and Effectiveness

"Should the disorder infect the Army, in the natural way . . . we should have more to dread from it than from the sword of the enemy."³ These were the sentiments of Gen George Washington as thousands of troops fell ill—and hundreds died—from smallpox during the first two years of the American Revolution, resulting in campaign losses, poor morale, and sparse recruiting. Via inoculation, the Continental Army dramatically reduced smallpox mortality from 160 to 3.3 per 1,000 cases, all but eliminating the threat.⁴ The US Civil War saw twice as many deaths from disease (65 per 1,000) as from battle (33 per 1,000).⁵ Of the 6 million disease cases among 2.8 million enlistees on both sides, over 95,000 died and roughly 250,000 were discharged for disability.⁶ Typhoid fever, malaria, and yellow fever accounted for 80 percent of US military deaths in the Spanish-American War, forcing a rapid withdrawal from Cuba soon after the end of hostilities.⁷ While World War I saw—for the first time—parity between US deaths from battle (50,510) and disease (51,477), the latter's impact on combat operations was demoralizing.⁸ Various diseases accounted for 95 percent of American battlefield hospital admissions in World War II, 69 percent in Vietnam, 71 percent in the Gulf War, and over 95 percent in Somalia.⁹ Unchecked, natural infections can wreak havoc on military forces.¹⁰

Criticality of Force Health Protection in Defending the Human Weapon System

The DOD's FHP doctrine characterizes every service member as a human weapon system requiring total life-cycle support and health maintenance.¹¹ Protecting the human weapon system, the central element of military power, is pivotal. Absent "craniums at the controls," "boots on the ground," and "hands on deck," wars cannot be won. Strained budgets, emerging technologies, and evolving threats have pressed the United States to transform its military into a lighter, leaner, and more agile force. With fewer people performing more specialized roles, it is critical for each military member to remain healthy, fit, and effective. Such is the challenge, as DOD personnel are often placed in austere locations, on short notice, and under stressful conditions, where naturally acquired infectious threats are abundant, immune systems are naïve, and healthcare support is limited. A vital part of FHP, immunization is effective in mitigating these operational hurdles.¹²

Superiority of Immunization among Medical Countermeasures

In defeating health threats, primary prevention—action prior to exposure—reigns supreme. Immunization affords the lowest risk, highest efficacy, and most cost-effective protection to vaccine recipients. Immunization is superior to therapeutics (e.g., antibiotics and chemoprophylactics) and personal protection (e.g., repellents and bed nets) since it does not require knowledge of exposure; is not contingent upon an accurate and timely diagnosis; protects against severe diseases (e.g., rabies) and those for which treatment is unavailable, ineffective, or prone to cause side-effects; does not require individual compliance (e.g., antimalarials); and neither contributes to nor is fazed by microbial resistance. As well, immunization can notably reduce the medical logistical footprint in theater since, for every casualty, five personnel are required in the evacuation and treatment support chain.¹³ Furthermore, vaccines not only elicit a direct benefit to recipients, they also afford herd immunity to those in the communities with whom they live and work.¹⁴ Finally, despite perceived differences between weaponized and natural pathogens, "vaccines are a unifying technology proven to effectively and efficiently defeat both of these threats."¹⁵

The Case for US Military Leadership in Infectious-Disease Vaccine R&D

Fielding a licensed vaccine is a long, complex, high-risk endeavor. It requires the synergy of expertise and resources from multiple partners spanning government, industry, academia, nonprofits, and international organizations.¹⁶ Cooperation is essential to manage the substantial scientific and financial risks. In general, no partner is capable of developing and producing a vaccine countermeasure alone. The DOD, for instance, must rely on industry for scale-up production, just as industry relies on the DOD to bring its many unique R&D capabilities to the cooperative effort.¹⁷

First is the DOD's unique experience. More than half of the routine vaccines given to service members today were codeveloped by the US military.¹⁸ Beyond protection of its own forces, the military's advances also created solutions to diseases of dire importance to national and international public health. Of 15 adult vaccines licensed in the United States since 1962, the DOD played a significant role in developing eight.¹⁹ Currently used worldwide, these include vaccines for influenza, meningococcal disease, hepatitis A, hepatitis B, rubella, adenovirus, typhoid, and Japanese encephalitis.²⁰ In addition, development of licensed vaccines for yellow fever, mumps, measles, varicella, and oral polio was supervised by investigators who began their careers at US military R&D centers.²¹ In the high-risk business of vaccine production, experience breeds proficiency and efficiency and curbs scientific, regulatory, and financial risk that can stifle product development.

Second are the DOD's unique facilities. The Walter Reed Army Institute of Research (WRAIR) is currently home to one of the nation's three pilot facilities dedicated to the production of a variety of investigational vaccines for use in clinical trials.²² Industry actively seeks the WRAIR's in-house laboratory capabilities to conduct animal modeling studies.

Third is the DOD's unique intellectual property (IP) sharing.²³ Highly sought after by industry, DOD partnerships attract companies by allowing them to retain IP rights for use in lucrative civilian markets.²⁴

Fourth is the DOD's unique R&D networks.²⁵ Because the Food and Drug Administration (FDA) requires pivotal clinical trials of products in people living in areas where infectious diseases are endemic, the DOD's overseas laboratories serve as bases for conducting clinical trials that attract industry partnerships.²⁶ Because of its enduring presence, strong host-nation relationships, and professional development of host-nation scientists, the DOD has been able to successfully execute complex clinical trials with industry and international partners.²⁷

Fifth, and most importantly, is the DOD's focus on the often unique needs of the war fighter. This mission distinguishes its infectious-disease activities from other organizations conducting what may appear to be similar R&D. The global effort to develop antimalarial countermeasures provides one example. Outside of the DOD, this effort is focused on drug therapies to attenuate lethal disease in children and pregnant women in underdeveloped countries. The goal of the DOD's program, on the other hand, is to prevent the war fighter from ever contracting the debilitating illness in the first place. To that end, DOD research has focused on developing prophylactic drugs and, more recently, a malaria vaccine solution. Additionally, any drug or vaccine used to protect US war fighters must be FDA licensed. Because many companies are reluctant to independently take on this costly risk, the DOD's R&D community plays a key role in moving potential military-relevant products through early development, FDA licensure, and eventual use by the US military.²⁸

Also compelling is the potential impact of infectious-disease vaccines on the military's increasing role in stability operations, which the DOD recently designated as "a core US military mission that [it] should be prepared to conduct with proficiency equivalent to combat operations."²⁹ Infectious diseases contribute significantly to social unrest and conflict in these scenarios. Infections not only ravage the local civilian populace, but also can decimate the strength of their national militaries. The prevalence of human immunodeficiency virus (HIV) infection and acquired immunodeficiency syndrome (AIDS) in Africa provides a persuasive example. Of 33 million people living with HIV worldwide, two-thirds reside in sub-Saharan Africa.³⁰ Armed forces in this region experience HIV infection rates two to three times those of the civilian population, further eroding local, national, and regional prospects for stability.³¹ The significance of this US national security concern is well summarized in the following excerpt from a 2002 report by the Center for Strategic and International Studies:

In Africa, HIV/AIDS is spreading fastest in the Horn of Africa, where the US already has deep concerns about lawlessness and extremism. In both Ethiopia and Kenya, potentially important regional hubs in the violent and volatile East African sub-region, adult HIV-prevalence rates are over 10 percent. Nigeria, an essential guarantor of security and economic growth in the West African region, has more than 3 million citizens living with HIV or AIDS. The adult prevalence rate in South Africa, which plays a similar economic and security role in the southern African region, is 20 percent. If these two regional hegemony cannot send peacekeepers, contribute to growth and stability, or guarantee their own internal stability, US security interests in the continent . . . are severely threatened.³²

This situation demonstrates the powerful potential impact that vaccines for endemic diseases could have on geopolitical stability.³³ An

effective HIV vaccine could remarkably strengthen foreign militaries, secure vulnerable families and communities, bolster international public health, and reinforce US national security.³⁴

Natural infections will continue to challenge the US military and its R&D community. With 1,500 known human pathogens continuously lurking and novel agents like H1N1 (influenza A virus or “swine flu”) constantly emerging, infectious diseases will remain a formidable national security threat indefinitely.³⁵ The expeditionary nature of military missions, the effects of climate change, and the interconnectedness of an increasingly globalized planet accentuate the risks. Worldwide, 14.7 million people die each year from known and preventable contagions.³⁶ Even in industrialized nations, 46 percent of all deaths result from infectious causes.³⁷ Emerging infections have been discovered at the rate of one per year since the late 1980s.³⁸ Pathogens adapt, persist, and emerge; this pattern will continue.³⁹

Keeping pace with the evolving threat requires a robust US military infectious-disease vaccine program with the venerable experience, proven track record, and unique attributes that no other agency can bring to bear—one that can continually improve upon its unparalleled protection of America’s warriors and, in the process, her citizens and global neighbors.

The DOD’s Unbalanced Biological-Threat Assessment and Mission Focus

Since the Cold War’s end, the DOD has become fixated on combating biological threats of deliberate origin over those of natural causes. This section examines the DOD’s lopsided focus on notional bio-weapons while natural infections continue to plague military operations.

Weaponized Pathogens: A Matter of National Insecurity

Despite its remarkable history, the US military infectious-disease vaccine program has taken a backseat to countering the bioterrorism threat since the mid-1990s. Beginning with its stand-up of the Joint Program Office for Biological Defense in 1993 and formalized requirements for biodefense vaccines in 1995, the DOD—with a push from Congress—justifiably turned a focused eye to biodefense.⁴⁰ By 1998 the DOD had established the Joint Vaccine Acquisition Program (JVAP) and significantly increased funding for advanced biodefense vaccine development, while core funding for infectious-disease vaccine R&D declined.⁴¹ Because of the post-9/11 anthrax letters, fears of state-sponsored weapons-of-mass-destruction proliferation by Iraq,

and the express interest in bioagents by al-Qaeda, the nation perceived an urgent vulnerability to biological attack.⁴² The DOD responded with wholesale investments in biodefense as infectious-disease R&D funding remained level.⁴³

Reportedly, about a dozen states and multiple nonstate actors possess or are pursuing biological weapons.⁴⁴ Their potential use clearly poses a level of danger to US forces in the contemporary battlespace, as do established and emerging natural infections. To date, the DOD has yet to incur a single case of weaponized disease, while some 3,400 cases of natural-origin and vaccine-preventable infectious diseases have been reported in deployed US forces since 1998.⁴⁵ While the potential threat is duly noted, bioterrorism against US interests has been limited to 22 American citizens sickened by anthrax-tainted letters in 2001, of whom five tragically died. Allegedly, this may have been the work of a lone American researcher, with no link to either state sponsors or nonstate actors.⁴⁶

In contrast, by 2008 West Nile virus had sickened 28,961 Americans—claiming 1,131 lives—since its arrival on US soil in 1999.⁴⁷ The emergence of severe acute respiratory syndrome (SARS) in 2003, H5N1 (influenza A virus or “bird flu”) in 2006, and H1N1 in 2009 further underscores the clear and present danger posed by natural infectious diseases. Also, to some experts, the emergence of a novel strain of adenovirus among military recruits in 2007 served to “remind us that we are at least equally likely . . . to soon experience large-scale morbidity through epidemics of emergent pathogens’ as we are to experience a biological weapons attack.”⁴⁸

Although it is undoubtedly a national security imperative for the United States to prepare its public and military against the intentional use of biological agents, vigilance for natural infections warrants at least the same level of emphasis.

Natural Pathogens: An Operational Reality Check

All the while, natural-origin infectious diseases have continued to pose real challenges to US military commanders in lost manpower-days, reduced effectiveness, increased medical visits, and frequent medical evacuations.⁴⁹ In one tri-service study, of 15,459 Operation Iraqi Freedom (OIF) and Operation Enduring Freedom (OEF) deployers surveyed, 75 percent reported having at least one bout of diarrhea, 69 percent suffered one or more episodes of acute respiratory illness, and “one-quarter believed that combat unit effectiveness had been negatively affected by these common illnesses.”⁵⁰ Roughly 13 percent of ground forces missed at least one patrol, 12 percent of air forces

were grounded, 25 percent required intravenous fluids, and over 10 percent were hospitalized.⁵¹

Table 1 summarizes the incidence of the four leading—and potentially vaccine-preventable—infectious diseases in deployed US forces between 1998 and 2009.⁵² Of 3,386 total cases, leishmaniasis, malaria, and Lyme disease accounted for 95.8 percent of the disease burden. Through 2004, leishmaniasis prompted 4.4 percent of the monthly medical evacuations during OIF.⁵³ The occurrence of 126 cases of meningococcal disease reflects the absence of an effective vaccine for subtype B of this potentially lethal pathogen. Each of these operational experiences emphasizes the current threat from naturally acquired pathogens and urges continued development of vaccine solutions for the mission-crippling diseases they cause.

Table 1. Summary of the major potentially vaccine-preventable infectious diseases incurred by deployed US military forces, 1998–2009

	<i>Leishmaniasis</i>	<i>Malaria</i>	<i>Lyme Disease</i>	<i>Meningococcal Disease</i>
Active	771	990	551	106
Reserve	420	68	445	20
TOTAL	1,191	1,058	996	126

Data from Armed Forces Health Surveillance Center (AFHSC), "Defense Medical Surveillance System," 10 December 2009.

**Signs of a Program in Serious Decline:
Loss of Adenovirus Vaccine**

While its emphasis was shifting to biodefense, the DOD was losing ground in its portfolio of infectious-disease vaccines. Table 2 depicts the major vaccine shortfalls which resulted from a variety of economic, regulatory, scientific, and legal pressures the existing DOD vaccine-acquisition apparatus was unable to mitigate.⁵⁴ Previously licensed vaccines for Lyme disease, cholera, and plague are currently unavailable. Ten investigational new drug (IND) vaccines are no longer produced and have limited availability.

The most instructive example is the DOD's loss of adenovirus vaccine. Because of crowding and various stressors, adenovirus is a frequent cause of acute respiratory disease in unvaccinated military recruits.⁵⁵ Prior to routine immunization in 1971, adenoviral outbreaks in DOD basic-training units were common. Infection rates approached 50 percent, hospitalizations reached 10 percent, and occasionally trainees died.⁵⁶ Outbreaks stressed medical services, eroded

Table 2. Previously licensed and IND-only infectious-disease vaccine shortfalls

	Vaccine
Previously licensed but unavailable	Adenovirus, types 4 and 7
	Lyme disease
	Cholera
	Plague
IND product no longer produced and of limited availability	Argentine hemorrhagic fever
	Chikungunya virus
	Eastern equine encephalitis
	Q fever
	Rift Valley fever
	Tularemia
	Venezuelan equine encephalitis
	Western equine encephalitis
	Botulinum toxoid
	Tickborne encephalitis

Data from Stanley M. Lemon, Susan Thaul, Salem Fisseha, and Heather C. O'Maonaigh, eds., *Protecting Our Forces: Improving Vaccine Acquisition and Availability in the US Military* (Washington, DC: Institute of Medicine of the National Academies, National Academies Press, 2002).

training effectiveness, and sometimes stalled the training pipeline altogether.⁵⁷ During 25 years of use, the adenovirus vaccine provided to recruits on day one of training virtually eliminated the disease.⁵⁸ In the mid-1990s, however, negotiations between the DOD and the sole adenovirus vaccine manufacturer failed to produce a financial agreement concerning upgrades to the production facility required by the FDA. In 1996 the manufacturer could no longer afford to produce the vaccine. As supplies waned across the DOD, prevaccination program morbidity returned, with unvaccinated trainees 28 times more likely than vaccinated trainees to be positive for the types of adenovirus covered by the vaccine.⁵⁹ All stocks were depleted by 1999, and by the end of 2000, seven basic military training centers had experienced adenoviral epidemics.

Today the DOD remains without an adenovirus vaccine, and the disease continues to sicken trainees, burden medical systems, and disrupt training.⁶⁰ For the 12 months prior to December 2009, over 4,400 military recruits with febrile respiratory illness tested positive for adenovirus.⁶¹ Not all who became ill were tested; the actual number of cases was higher.⁶² One DOD study estimated the loss of adenovirus vaccine to be responsible for 10,650 preventable infections, 4,260 medical clinic visits, and 852 hospitalizations among the roughly 213,000 active duty and reserve trainees enrolled in basic

training each year.⁶³ Another study projected the related annual medical and training costs at \$26.4 million for the US Army alone.⁶⁴

The loss of the adenovirus vaccine “sounds a warning for the fragile system supporting other vaccines of military and public health importance.”⁶⁵ To stay in business, vaccine manufacturers need to realize a profit. To do so, they must weigh what it costs to manufacture a product, how much of it they can sell at what price, and what they could be making if they used their production capacity on a different product. The economic pressures brought on by evolving regulatory requirements caused this sole-source manufacturer to abandon its production of a limited-market, mainly military-use vaccine. Competing priorities and the lack of a single agent with the authority and budget to preserve adenovirus vaccine availability were significant DOD shortcomings.

Disparate Organizations, Disproportionate Funding, Dissimilar Priority

Despite overlapping missions, the DOD maintains separate organizations for infectious-disease and biodefense vaccine development, procurement, and product management. Each has exclusive budgetary authority and product-line responsibility. This section investigates the negative impacts from the DOD's decision to decouple its vaccine programs while granting preferential funding and priority to its biodefense efforts.

Disparate Organizations

The Military Infectious Diseases Research Program (MIDRP) mission is to “protect the US military against naturally-occurring infectious diseases via the development of FDA-approved vaccines” and other protection systems.⁶⁶ The JVAP exists to “develop, produce and stockpile FDA-licensed vaccine systems to protect the warfighter from biological agents.”⁶⁷ Figure 1, a simplified organizational chart, highlights these agencies' disparate command and control relationships.⁶⁸ In reality, the number of players and interactions is much more complex, indicative of the fragmented and diffuse organization that encumbers acquisition. Congress directed the split management scheme to raise the visibility of biodefense and streamline acquisition procedures.⁶⁹ In retrospect, however, separating the acquisition of infectious-disease and biodefense vaccines was ill-advised for multiple reasons.

First, separate acquisition precludes a unified approach to the identification and prioritization of vaccine solutions based primarily

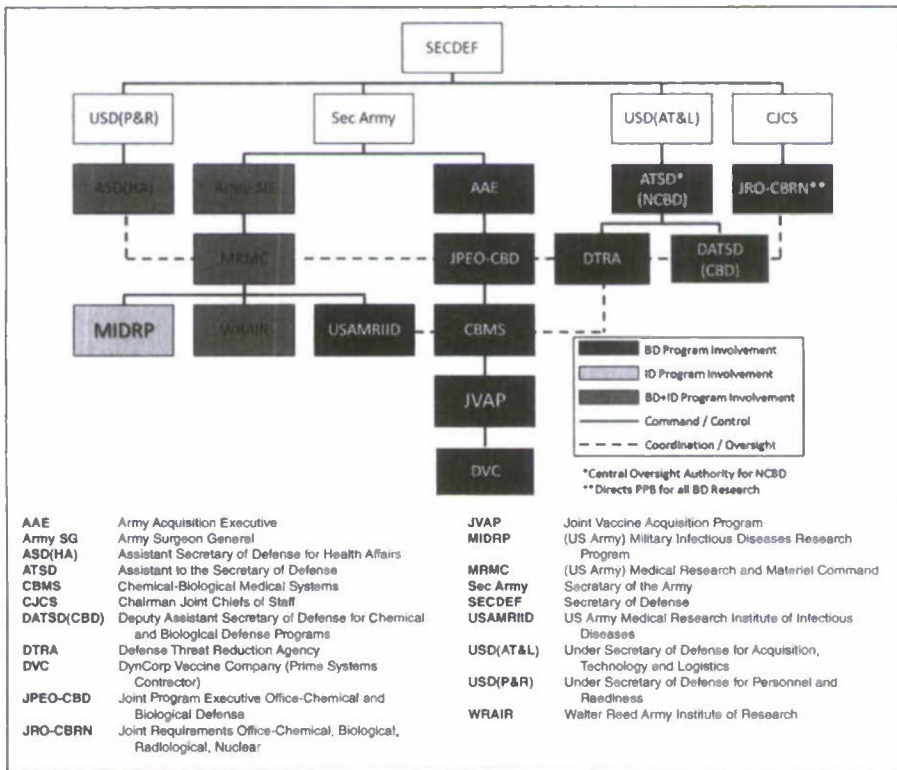


Figure 1. Simplified organizational chart depicting DOD infectious-disease and biodefense vaccine programs. (Adapted from LTC Coleen K. Martinez, "Biodefense Research Supporting the DOD: A New Strategic Vision," Research Report no. 1-58487-288-8 [Carlisle Barracks, PA: US Army War College, 2007]; Rudolph Kuppers, USMRMC/MIDRP, to the author, 11 December 2009; and COL Charles Hoke, retired, MD, USAMRIID, to the author, e-mail, 24 January 2010.)

on operational risk rather than the nature of the threat. Similarly, it impedes a united approach to the acquisition of "dual-use" vaccines, those which could counter both a natural and a weaponized threat to military personnel.⁷⁰ The National Select Agent Registry (NSAR), utilized for monitoring the possession and use of 48 pathogens and toxins that pose a severe threat to human health, contains 13 bioweapons that are also natural infections for which vaccines have been, or currently are, in some stage of development by the MIDRP.⁷¹

Second, separate acquisition fosters programmatic redundancy. There are many more similarities than differences between the pathogens, science, technology, and business processes for vaccines against natural and weaponized agents. Their development and pro-

duction follow like pathways, encounter similar difficulties, and present comparable developmental and financial risks.

Third, separate acquisition dilutes limited expertise and splits budgetary power. Because vaccine development is so complex, highly skilled and experienced professionals are required in all facets, from scientists to administrators. Also, the industry average cost to bring a new vaccine through the development process from concept to licensure ranges from \$800 million to \$1.6 billion over 14 years; to sustain a fielded product costs millions more. Separation curbs professional and budgetary synergy.⁷²

Fourth, separate acquisition hinders the Total Life-Cycle Systems Management (TLCSM) of vaccine products—"the implementation, management, and oversight, by a single accountable authority, of all activities associated with the acquisition, development, production, fielding and sustainment of a DOD system across its life cycle."⁷³ The Joint Program Executive Office for Chemical and Biological Defense (JPEO-CBD) leads the TLCSM of biodefense vaccines.⁷⁴ To date, no single locus of TLCSM authority, responsibility, and accountability exists for infectious-disease vaccine products.⁷⁵ Separation under-serves infectious-disease vaccine acquisition and precludes enterprise-wide vaccine TLCSM collaboration.

These issues have contributed to significant vaccine availability problems, such as the loss of the adenovirus vaccine as previously described. They also signify the level of commitment required by the DOD not only to bring militarily important vaccines on line but to keep them available.⁷⁶ In its 2002 report to the DOD, the Institute of Medicine was "convinced that disjointed authority . . . within DOD contributed significantly to the lack of additional investment required for continued production of [adenovirus] vaccine."⁷⁷

Disproportionate Funding

While discrete programs with no single oversight authority are problematic, the pivotal issue in separating the acquisition of infectious-disease and biodefense vaccines is budgetary. In 1993 the DOD's annual budget for the advanced development of biodefense vaccines was \$1 million.⁷⁸ By 1998 funding levels rose to \$25 million per year.⁷⁹ Between fiscal year (FY) 2001 and FY 2008, the US government annually allocated \$57 billion to biodefense, with the DOD receiving nearly \$12 billion.⁸⁰ In FY 2009 government-wide allocations jumped by 39 percent to \$8.97 billion; the DOD share was \$1.72 billion.⁸¹ Billions were allocated to the Department of Health and Human Services and the DOD to develop, produce, procure, and stock-

pile vaccine countermeasures against weaponized pathogens.⁸² Since FY 1997 the annual US budget for biological defense has increased over 47-fold, from \$137 million to \$6.5 billion by FY 2008.⁸³

Figure 2 shows MIDRP funding for its core research over the past 15 years, with projections to FY 2011.⁸⁴ Several points must be made. First, biodefense vaccine management transitioned from the MIDRP to the JVAP in 1998, accounting for the associated funding spike and then dip. Second, there is a relative budget flatline in actual-year dollars over the period. In FY 1994 the MIDRP's annual budget was \$42 million. By FY 2009 it had increased only to \$47 million. Third, when adjusted for inflation to FY 2005 dollars, the buying power of the FY 2009 budget was only \$41 million, less than that of 15 years earlier. Fourth, the inflationary gap is widening. By FY 2011 the MIDRP's \$46 million annual budget will be worth, in effect, only \$37 million in FY 2005 dollars.

Figure 3 depicts the mounting impact of inflation on the MIDRP budget through FY 2015.⁸⁵ With projected funding levels, the MIDRP cannot keep pace with inflation. This dismal scenario is exacerbated by the rising cost of advanced product development and clinical trials, which accounts for roughly 75 percent of total development outlays.⁸⁶ Also, clinical trials to assess a vaccine's safety and efficacy in human subjects are very expensive. In the past five years, these costs have

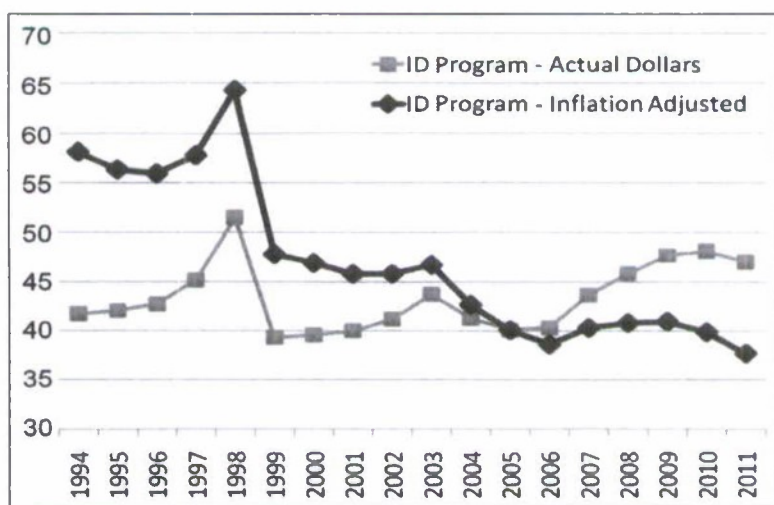


Figure 2. US Army MIDRP funding for infectious diseases core research with inflation adjusted to FY 2005, in millions of dollars (does not include HIV program). (Adapted from Rudolph Kuppers, USMRMC/MIDRP, to the author, e-mail, 11 December 2009.)

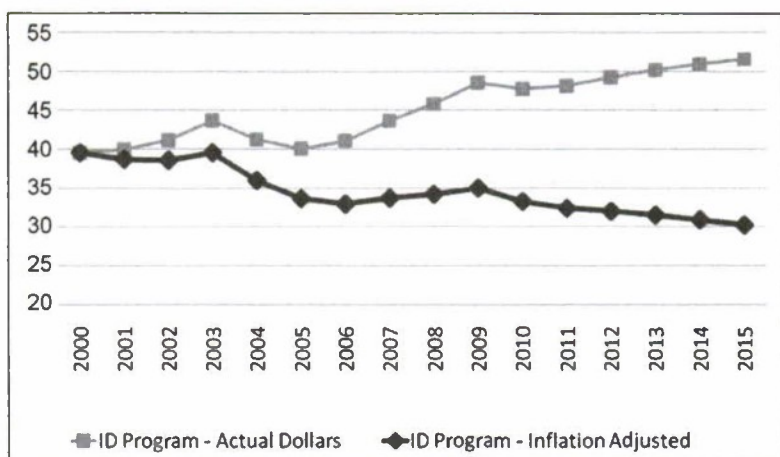


Figure 3. US Army MIDRP budget, FY 2000–15, in millions of dollars (does not include HIV program). (Adapted from Rudolph Kuppers, USMRMC/MIDRP, to the author, e-mail, 11 December 2009.)

risen from \$15,000 to as much as \$26,000 per enrollee.⁸⁷ With static funding and less buying power, the MIDRP's ability to develop vaccine products is, and will remain, seriously constrained.

Dissimilar Priority

To make the best use of limited resources, the rules of the Defense Acquisition Management System govern the acquisition of military vaccines. Acquisition categories (ACAT I, II, and III) are used to assign priority and determine the level of DOD review, decision authority, and milestones that apply to a given project.⁸⁸ The MIDRP's infectious-disease vaccines are now managed as an ACAT III "less than major" program, the lowest priority level, with each vaccine managed as a separate acquisition project.⁸⁹ Biodefense vaccines, on the other hand, are developed by the JVAP as an ACAT II "major system" program under the JPEO-CBD.⁹⁰ The ACAT II designation affords biodefense vaccines not only a higher priority for acquisition funding but also higher visibility than vaccines against infections of natural origin. The lack of emphasis on these natural infectious-disease countermeasures has contributed to the loss of licensed vaccines (e.g., adenovirus, plague, and cholera) and the inability to advance IND products (e.g., tick-borne encephalitis, Rift Valley fever, and eastern equine encephalitis vaccines) to full licensure. Additionally, the inferior priority of infectious-disease vaccines makes their funding vulnerable to becoming offsets for higher ACAT programs.

Recommendations and Conclusion

This section recommends four imperatives for ensuring the DOD's ongoing ability to produce vaccines against natural infections and provides final thoughts on reversing the dangerous decline in US military infectious-disease R&D capability. While the challenges are formidable, the DOD can return its ailing infectious-disease vaccine program to its former status as the world's premier force health defender. Here is what needs to be done.

Redesign the Biological-Threat Assessment Process

Concurrently consider all biotreats regardless of origin. Then prioritize them based on a balanced assessment of notional and experiential risks to war fighters independent of the nature of the threat.⁹¹ To facilitate this process, a standardized cost-benefit computation should be instituted for candidate vaccines and strategies, where solutions to natural or weaponized biotreats with the most compelling calculations garner the highest priority for funding.⁹²

Merge Infectious-Disease and Biodefense Vaccine Management

A single DOD program is required to unify needs identification, prioritization, basic and advanced research, production, procurement, and ongoing product management.⁹³ Program leadership must be vested in a single agent with the authority, responsibility, and accountability for ensuring effective TLCSM of all vaccines that protect war fighters against natural and weaponized pathogens. Combining programs will facilitate the synergistic sharing of ideas, expertise, and resources; incentivize cohesive thinking on vaccine solutions of mutual benefit to infectious-disease prevention, biodefense, and public health; and underpin the maintenance of a robust, adaptable technology base that can flex to conduct timely research on the moving target of natural and weaponized biotreats. In addition, a unified program champion will provide the strongest advocacy for infectious-disease vaccines to balance against the government's proclivity for biodefense countermeasures.

Elevate the Acquisition Priority of Infectious-Disease Vaccines

Like those intended for biodefense, vaccines to counter natural infections should be managed at the ACAT II major-system level (or higher). This is in alignment with the first recommendation above to

consider all biological threats—regardless of origin—of equal threat potential to war fighters. This will ensure appropriate visibility and emphasis of both infectious-disease and biodefense vaccine acquisition within the DOD.

Increase Funding for Infectious-Disease Vaccine Research, Development, and Procurement

In addition to raising overall program funding, each infectious-disease vaccine should be funded as a separate line item in the Future Years Defense Program to ensure TLCSM.⁹⁴ These are the most important actions the DOD must take. To be clear, what is needed is not a zero-sum realignment of biodefense and infectious-disease vaccine resources. Biodefense vaccines should remain fully funded, with relative parity achieved for infectious-disease vaccine development. Currently, at least half of national biodefense funding serves both biodefense and public health ends.⁹⁵ This kind of overlap should become the rallying cry of DOD vaccine prioritization and resource allocation. A successful biothreat vaccine program is about cooperation, not competition.

Conclusion

The president's 2009 *National Strategy for Countering Biological Threats* calls for "a comprehensive and integrated approach to prevent the full spectrum of biological threats . . . whether natural, accidental or deliberate in nature."⁹⁶ To meet his intent, the DOD needs to reorganize its current infectious-disease and biodefense vaccine acquisition stovepipes and establish a unified program to effectively assess, prioritize, develop, and procure vaccines to protect war fighters against threats from all causes.

Staying ahead of the changing threat requires the DOD to refocus on the full range of biothreats and commit ample resources for the sustained development of infectious-disease—as well as biodefense—vaccines. Anything less places force health, combat readiness, and operational effectiveness at serious risk.

Notes

1. In this paper, *acquisition* is defined as the DOD's process for ensuring that vaccines are acquired and maintained for the protection of its forces, from needs identification, prioritization, and basic research to advanced development, testing, production, and procurement. *Availability* is having on hand the right vaccine for the right threat at the right time.

2. National Security Council, *National Strategy for Countering Biological Threats*, November 2009, http://www.whitehouse.gov/sites/default/files/National_Strategy_for_Countering_BioThreats.pdf (accessed 15 January 2010).
3. Stanhope Bayne-Jones, *The Evolution of Preventive Medicine in the United States Army, 1607-1939* (Washington, DC: Office of the Surgeon General, Department of the Army, 1968), 52, <http://history.amedd.army.mil/booksdocs/misc/evprev/default.html> (accessed 28 October 2009).
4. Specifically, this was *variolation*, an "obsolete process of inoculating a susceptible person with material taken from a vesicle of a person who has smallpox." Princeton University, WordNet, <http://wordnetweb.princeton.edu/perl/webwn?s=variolation>.
5. Bayne-Jones, *Evolution of Preventive Medicine in the US Army*, 99.
6. *Ibid.*
7. *Ibid.*, 124.
8. *Ibid.*, 151.
9. Mark S. Riddle et al., "Past Trends and Current Status of Self-Reported Incidence and Impact of Disease and Nonbattle Injury in Military Operations in Southwest Asia and the Middle East," *American Journal of Public Health* 98, no. 12 (2008): 2199; and Stanley M. Lemon et al., *Protecting Our Forces: Improving Vaccine Acquisition and Availability in the US Military* (Washington, DC: Institute of Medicine of the National Academies, National Academies Press, 2002), 10.
10. John W. Sanders et al., "Impact of Illness and Non-Combat Injury during Operations Iraqi Freedom and Enduring Freedom (Afghanistan)," *American Journal of Tropical Medicine and Hygiene* 73, no. 4 (2005): 713-19.
11. Joint Publication (JP) 4-02, *Doctrine for Health Services Support in Joint Operations*, 31 October 2006, GL-14; Anthony P. Tvaryanas, Lex Brown, and Nita L. Miller, "Managing the Human Weapon System: A Vision for an Air Force Human-Performance Doctrine," *Air and Space Power Journal* 23, no. 2 (Summer 2009): 34-41; and Joint Chiefs of Staff (JCS), *Force Health Protection Capstone Document* (Washington, DC: JCS, 2000), 2.
12. JP 4-02, *Doctrine for Health Services Support*, IV-5.
13. Richard D. Nidel, JVAP Office Video, <http://www.jpeocbd.osd.mil/packs/DocHandler.ashx?DocId=4711> (accessed 5 December 2009).
14. John D. Grabenstein, "Immunization to Protect the US Armed Forces: Heritage, Current Practice, Prospects," *Epidemiologic Reviews* 28, no. 1 (2006): 10.
15. DOD, *Report on Biological Warfare Defense Vaccine Research & Development Programs* (Washington, DC: DOD, July 2001), 7.
16. Rudolph Kupperts, USMRMC/MIDRP, to the author, e-mail, 11 December 2009.
17. *Ibid.*
18. *Ibid.*
19. Military Infectious Diseases Research Program (MIDRP). "History and Achievements," <https://midrp.amedd.army.mil/info/HAchieve.html> (accessed 5 January 2010).
20. *Ibid.*
21. *Ibid.*
22. The Quantic Group, "CBRN Medical Countermeasures (MCM) Manufacturing Capabilities Analysis of Alternatives Report," 15 June 2009, 10.
23. Intellectual property is "the group of legal rights to things people create or invent. Intellectual property rights typically include patent, copyright, trademark and trade secret rights." Sitepoint, <http://www.sitepoint.com/glossary.php>.
24. Kupperts to the author, e-mail; and Lemon, *Protecting Our Forces*, 87.
25. COL Charles Hoke, retired, MD, USAMRIID, to the author, e-mail, 24 January 2010.

26. A pivotal clinical trial must be controlled, have a double-blinded design when practical and ethical, be randomized, and be of adequate size. AdisInsight, <http://www.adisinsight.com/aClientServiceinfo/CTI%20Appendix.pdf>. DOD overseas labs are located in Thailand, Peru, Kenya, Egypt, and Indonesia. Hoke to the author, e-mail.

27. COL Julia Lynch, USMRMC/MIDRP, to the author, e-mail, 18 January 2010.

28. Kupperts to the author, e-mail.

29. Department of Defense Instruction (DODI) 3000.05, *Stability Operations*, 16 September 2009, 2.

30. World Health Organization (WHO), *Towards Universal Access: Scaling Up Priority HIV/AIDS Interventions in the Health Sector, Progress Report 2009* (Geneva, Switzerland: WHO Press, 2009), 7, http://whqlibdoc.who.int/publications/2009/9789241598750_eng.pdf (accessed 9 January 2010).

31. Mark Schneider and Michael Moodie, *The Destabilizing Impacts of HIV/AIDS* (Washington, DC: Center for Strategic and International Studies, May 2002), 2.

32. *Ibid.*, 4.

33. Kupperts to the author, e-mail.

34. In June 2009 a US Army-led Phase III community-based trial of a candidate HIV vaccine was completed, yielding encouraging preliminary results but requiring further research. Hoke to the author, e-mail.

35. Lynch to the author, e-mail; and W. Neal Burnette et al., "Infectious Diseases Investment Decision Evaluation Algorithm: A Quantitative Algorithm for Prioritization of Naturally Occurring Infectious Disease Threats to the US Military," *Military Medicine* 173 (February 2008): 174–81.

36. Arguably, climate change is resulting in significant changes in weather patterns and disruptions in ecosystems leading to the emergence of new niches for infectious disease pathogens and vectors. Lynch to the author, e-mail. On the death rate from contagions, see Sara E. Davies, "Securitizing Infectious Disease," *International Affairs* 84, no. 2 (2008): 295–313; and WHO, "The Top Ten Causes of Death," fact sheet, February 2007, <http://www.who.int/mediacentre/factsheets/fs310.pdf> (accessed 15 January 2010). The top five infectious disease killers include HIV/AIDS, pneumonia, diarrhea, malaria, and tuberculosis.

37. Burnette et al., "Infectious Diseases Investment," 174.

38. Davies, "Securitizing Infectious Disease," 298.

39. Hoke to the author, e-mail.

40. Edward T. Clayson, JVPAP Product Management Office, JVPAP overview presentation slides, 30 May 2003, slide 5.

41. *Ibid.*; and Kupperts to the author, e-mail (compares 1997 and 1999 MIDRP funding).

42. US Senate, *Testimony for the Senate Foreign Relations Committee by Amy Sands, PhD, Deputy Director, Center for Non-Proliferation Studies, Monterey Institute of International Studies, before the US Senate Foreign Relations Committee*, 19 March 2002, <http://cns.mils.edu/pubs/reports/asands.htm> (accessed 7 January 2010); and LTC Coleen K. Martinez, "Biodefense Research Supporting the DOD: A New Strategic Vision," Research Report no. 1-58487-288-8 (Carlisle Barracks, PA: US Army War College, 2007), 23.

43. Kupperts to the author, e-mail.

44. US Senate, *Statement by Assistant Secretary of State for Intelligence and Research Carl W. Ford, Jr. before the US Senate Committee on Foreign Relations Hearing on Reducing the Threat of Chemical and Biological Weapons*, 19 March 2002, <http://www.fas.org/bwc/news/testimony/CT2002March19Ford.htm> (accessed 7 January 2010); and US Senate, *Testimony by Amy Sands*.

45. Armed Forces Health Surveillance Center (AFHSC), "Defense Medical Surveillance System," <http://www.afhsc.mil/dmss> (accessed 10 December 2009).
46. Federal Bureau of Investigation, "Amerithrax Investigation," <http://www.fbi.gov/anthrax/amerithraxlinks.htm> (accessed 28 January 2010).
47. Centers for Disease Control and Prevention (CDC), "West Nile Virus: Statistics, Surveillance, and Control," http://www.cdc.gov/ncidod/dvbid/westnile/surv&controlCaseCount99_detailed.htm (accessed 22 December 2009).
48. Amesh A. Adalja, "Adenovirus 14," quoting Gregory C. Gray and Margaret L. Chorazy, "Human Adenovirus 14a: A New Epidemic Threat," *Journal of Infectious Disease* 199 (2009): 1413, <http://www.journals.uchicago.edu/doi/full/10.1086/598522> (accessed 5 November 2009). In 2007, 23 trainees at Lackland AFB, Texas, hospitalized for pneumonia, were found to be infected with a variant strain (type 14) of adenovirus; one of the trainees died. Amesh A. Adalja, "Adenovirus 14: An Emerging Threat," 17 April 2009, Clinician's Biosecurity Network, http://www.upmc-cbn.org/report_archive/2009/04_April_2009/cbnreport_04172009.html (accessed 27 November 2009).
49. Sanders et al., "Impact of Illness and Non-Combat Injury."
50. Ibid., 714. *Campylobacter*, *Shigella*, *Escherichia coli* and norovirus have been the most commonly reported diarrheal infections in deployed forces. *Rhinovirus*, *Coronavirus*, parainfluenza virus, and adenovirus have been the most commonly reported causes of acute respiratory infections in deployed forces. AFHSC, "Defense Medical Surveillance System."
51. Sanders et al., "Impact of Illness and Non-Combat Injury," 716.
52. AFHSC, "Defense Medical Surveillance System."
53. C. G. Hawley-Bowland, *Casualty Analysis: Health Policy and Services* (Washington, DC: US Army Medical Command, 2004).
54. Lemon et al., *Protecting Our Forces*, 44–45.
55. James Chin, ed. *Control of Communicable Diseases Manual*, 17th ed. (Washington, DC: American Public Health Association, 2000), 428.
56. Grabenstein, "Immunization to Protect the US Armed Forces," 13.
57. Gregory C. Gray et al., "Adult Adenovirus Infections: Loss of Orphaned Vaccines Precipitates Military Respiratory Disease Epidemics," *Clinical Infectious Disease* 31, no. 3 (September 2000): 663–70.
58. Although referred to as a single entity in this paper, two adenovirus vaccines were actually lost, types 4 and 7.
59. Sanders et al., "Impact of Illness and Non-Combat Injury," 663.
60. Lynch to the author, e-mail. The DOD is pursuing an adenovirus vaccine from a new manufacturer with the assistance of the WRAIR. That product was successfully tested in a phase III efficacy study conducted by military investigators in 2008. License is currently pending FDA review, with a response expected in summer 2010.
61. Naval Health Research Center, Department of Respiratory Diseases Research, "Febrile Respiratory Illness (FRI) Surveillance Update," week ending 16 January 2010, <http://www.med.navy.mil/sites/nhrc/geis/Documents/FRIUpdate.pdf> (accessed 25 January 2010).
62. Ibid.
63. Gray et al., "Adult Adenovirus Infections," 668.
64. M. René Howell et al., "Prevention of Adenoviral Acute Respiratory Disease in Army Recruits: Cost-Effectiveness of a Military Vaccination Policy," *American Journal of Preventive Medicine* 14, no. 3 (April 1998): 168.
65. Gray and Chorazy, "Human Adenovirus 14a," 1414.
66. MIDRP, "MIDRP Overview," <https://midrp.amedd.army.mil/login.jsp> (accessed 27 December 2009).

67. David Williams and Calvin Carpenter, "Medical Systems: Advanced Planning Briefing to Industry," briefing slides, Joint Program Management-Chemical Biological Medical Systems (JPM-CBMS), 7 May 2009, slide 8.

68. Martinez, "Biodefense Research Supporting the DOD," 11; Kupperts to the author, e-mail; and Hoke to the author, e-mail.

69. Lemon et al., *Protecting Our Forces*, 64.

70. Ibid.

71. Possession, Use, and Transfer of Select Agents and Toxins, Interim Final Rule. Code of Federal Regulations, title 42, pt. 73, <http://www.cdc.gov/od/sap/docs/42cfr73.pdf> (accessed 4 November 2009); and Lemon et al., *Protecting Our Forces*, 40–41. The NSAR "currently requires registration of facilities, including government agencies, universities, research institutions, and commercial entities, that possess, use, or transfer biological agents and toxins." See the NSAR Web site, "Overview," <http://www.selectagents.gov> (accessed 19 July 2010).

72. Joseph A. DiMasi, Ronald W. Hansen, and Henry G. Grabowski, "The Price of Innovation: New Estimates of Drug Development Costs," *Journal of Health Economics* 22, no. 2 (2003): 180.

73. Office of the Assistant Deputy Undersecretary of Defense for Logistics Plans and Programs, *Total Life Cycle System Management: Plan of Action and Milestones*, http://www.acq.osd.mil/log/sci/exec_info/sm_milestone_plan010603.pdf (accessed 31 January 2010), 2.

74. Government Contract & Bid, "Joint Vaccine Acquisition Program (JVAP) Storage, Distribution, and Testing of Government Owned/Regulated Chemical Biological Defense," <http://www.govcb.com/H-Joint-Vaccine-Acquisition-Program-ADP11981138560001613.htm> (accessed 31 January 2010).

75. Hoke to the author, e-mail.

76. Ibid.

77. Lemon et al., *Protecting Our Forces*, 59.

78. Clayson, JVAP Overview, slide 5.

79. Ibid.

80. Center for Arms Control and Non-Proliferation, *Federal Funding for Biological Weapons Prevention and Defense, Fiscal Years 2001 to 2009*, 15 April 2008, http://www.armscontrolcenter.org/media/fy2009_bw_budgetv2.pdf.

81. Ibid.

82. Ibid.

83. D. R. Franz, "Ways Ahead: USG Biodefense Program from 2010 to 2020," Bio-defense Way Ahead Project Workshop, Defense Threat Reduction Agency, Washington, DC, 16 September 2009, 2; and Center for Arms Control and Non-Proliferation, *Federal Funding for Biological Weapons Prevention*.

84. Kupperts to the author, e-mail.

85. Ibid.

86. Lemon et al., *Protecting Our Forces*, 52.

87. Kupperts to the author, e-mail; and LifeSciencesWorld, "Phase 3 Clinical Trial Costs Exceed \$26,000 per Patient," 13 October 2006, <http://www.lifesciencesworld.com/news/view/11080> (accessed 31 January 2010).

88. DODI 5000.02, *Operation of the Defense Acquisition System*, 8 December 2008.

89. Lemon et al., *Protecting Our Forces*, 33.

90. The DOD estimates that major systems will require an eventual total expenditure for research, development, test, and evaluation of more than 140 million in FY 2000 constant dollars or for procurement more than 600 million dollars. Department of the Army, *US Army Weapon Systems 2010*, 2009; and Office of the Deputy Assistant Secretary of Defense for Chemical and Biological Defense, *Department of Defense*

Chemical and Biological Defense Program Annual Report to Congress, March 2005, E-38, <http://handle.dtic.mil/100.2/ADA435936> (accessed 14 July 2010).

91. Burnette et al., "Infectious Diseases Investment Decision Evaluation Algorithm," 174.

92. Hoke to the author, e-mail. Burnette et al. provide a viable algorithm for conducting this type of (annually recurring) prioritization.

93. No fewer than five separate studies have previously made this recommendation: DOD, *Report on Biological Warfare Defense Vaccine*, ii; DOD, *Quadrennial Defense Review Report*, 30 September 2001, 52; General Accounting Office (GAO), *Defense Acquisitions: DOD Faces Challenges in Implementing Best Practices*, Testimony before the Subcommittee on Readiness and Management Support, Committee on Armed Services, US Senate, GAO-02-469T (Washington, DC: GAO, 27 February 2002), 3; Lemon et al., *Protecting Our Forces*, 58; and University of Pittsburgh Medical Center, *Ensuring Biologics Advanced Development and Manufacturing Capability for the United States Government: A Summary of Key Findings and Conclusions*, final report for cooperative agreement research study with Defense Advanced Research Projects Agency, 6 October 2009, 66.

94. Ibid.

95. Franz, "Ways Ahead," 2.

96. National Security Council, *National Strategy for Countering Biological Threats*, 3.

Abbreviations

ACAT	acquisition category
AIDS	acquired immune deficiency syndrome
AWC	Air War College
CBRN	chemical, biological, radiological, and nuclear
CDC	Centers for Disease Control and Prevention
DOD	Department of Defense
FDA	Food and Drug Administration
FHP	force health protection
FY	fiscal year
H1N1	influenza A virus or "swine flu"
H5N1	influenza A virus or "bird flu"
HIV	human immunodeficiency virus
IND	investigational new drug
IP	intellectual property
JCS	Joint Chiefs of Staff
JPEO-CBD	Joint Program Executive Office for Chemical and Biological Defense
JVAP	Joint Vaccine Acquisition Program
MIDRP	Military Infectious Diseases Research Program
NSAR	National Select Agent Registry
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
R&D	research and development
SARS	severe acute respiratory syndrome
TLCSM	Total Life-Cycle Systems Management
WHO	World Health Organization
WRAIR	Walter Reed Army Institute of Research

Legal and Ethical Aspects of the Decision for War

A Case Study

*Lt Col Michael Rafter, Canadian Forces**

Throughout its history, the United States rarely shied away from using military force to confront perceived threats to its security and to support its interests abroad. The one element which sets the United States apart from virtually all other states maintaining an expeditionary military capability, particularly in the post-Cold War environment, is the scope and size of the missions and military engagements that it is capable of undertaking. This fact, combined with the reality that it must provide transparency and remain accountable, means that its actions are far more open to scrutiny and criticism from both within and without. Despite its status as the sole remaining superpower, the US government must garner the support of allies, like-minded states, and nations with which it does not traditionally align itself if its military actions are to be considered reasonable and justifiable. The key to ensuring this support is a timely provision of legitimate legal and moral justifications for war.

While it is true the executive and legislative branches of the American government have an important role to play in the approval mechanism to launch military operations, the president, as commander in chief, has the greatest overall influence on the decision-making process. This is not entirely surprising, as the president will normally be criticized when the decision to go to war is questioned. The war-making powers assigned to the president are enshrined in the US Constitution, largely "as a result of the unity of the office of the presidency . . . [where] speedy and purposeful action is often requisite to counter moves from abroad and to deal with rapidly changing international events [and because] Congress, it is claimed, is too cumbersome and ponderous a body to meet and deal with foreign policy and foreign military complexities."¹

When hostilities involving US military assets are initiated, the American populace, foreign governments, national and international media, and any other parties who have an interest in understanding

*COL Eric Smith, USA, was the essay advisor for this paper.

the motivations for going to war will turn to the president for an explanation or a clarification. The ability or inability to convincingly validate the military action taken—particularly to those whose ongoing support is vital to the United States—will have an important impact on American economic, foreign, and military relations, as well as national interests. In situations where use of military force is in direct response to an attack or a verifiable and imminent threat to the United States, the case for war is often quite obvious and understandable.

When the recourse to military action is both legally and morally defensible, the likelihood of negative repercussions will be lessened. In fact, it can be argued that this capability to frame the decision in legal and ethical terms best serves the president in substantiating a military reaction to a particular situation.

Over the past century, which constitutes the period of time when the majority of US expeditionary military operations have taken place, American presidents have effectively explained the rationale for war or military activities in terms of legal and ethical considerations. In instances where the substantiation has been less credible, presidents contended with domestic and international condemnation and opposition to the use of armed force. Given the existence of established laws of armed conflict (LOAC), determinations regarding the legality of military action have proven far easier than confirming the morality of these interventions. Many presidential explanations have been more compelling when evidence confirmed that moral principles were present and played an important role in the war decision. The fact that a particular president truly believed that a moral imperative existed for war has gone a long way in deflecting criticism in the past.

Although the end of the Cold War brought an expectation that a new era of worldwide peace and cooperation would emerge, the ensuing two decades have been fraught with conflict and strife which ultimately resulted in war or warlike confrontations—many involving the US military. Though the need to defend the use of armed forces has always existed, a growing political awareness among the general population, combined with improved media coverage and near real-time communications in recent years, has made the need for legal and moral justification for military action by the commander in chief all the more important.

Examples of specific instances where presidents articulated why compelling arguments existed for international military engagements are relatively straightforward. During the 1999 air war in Kosovo, Pres. Bill Clinton clearly explained that US participation in the operation was legally justified since it equated to an intervention in an escalating humanitarian crisis and that the United States was “acting

out of a 'moral imperative' to help the people of Kosovo."² When the United States and its coalition allies undertook operations in Afghanistan in late 2001, they did so with the legal backing of a United Nations (UN) resolution, as well as an undeniable belief that they were morally obliged to root out those responsible for the reprehensible terrorist attacks of 9/11.

Pres. George W. Bush enjoyed widespread support for his decision to authorize the Southwest Asia mission, principally due to the solid legal and moral arguments in favor of the operation. Conversely, the president's failure to credibly highlight the legal and moral justifications for the war in Iraq, despite his genuine belief the United States was morally bound to redress Saddam's mistreatment of Iraqi citizens, resulted in an unprecedented erosion of confidence in the office of the president and a suspicion of American intentions.³

Not all US military operations achieved success or accomplished the political goals enunciated prior to the start of hostilities. At times, military interventions that appeared to be legally and morally justifiable at their start ended badly because the forces suffered from poor politico-military leadership and vision, among other problems. Having a sound legal and ethical basis for military action is no guarantee that the mission will end favorably. Legal and ethical validation for warfare simply provides a greater probability that the action will be seen as a valid response to an existing threat, the reason for the decision will be understood and supported, and, in the long term, domestic, political, and diplomatic relations will not be negatively impacted.

To validate the premises proposed, a case study from the Vietnam era is elaborated upon. While both legal and moral justifications have been offered for more recent operations, they are ongoing to this day. The long-term consequences and final outcomes of the wars in both Afghanistan and Iraq have yet to be determined, making a final conclusion difficult. For this reason, this paper considers the decision by Pres. Richard Nixon to authorize the 1970 Cambodian incursion. The results of actions taken almost 40 years ago are well known and unlikely to change.

From the day the Cambodian incursion was announced, and through the intervening decades, historians, political scientists, and armchair generals have sought to rationalize and criticize Nixon's decision to authorize this operation. Few, however, have been able to place themselves in the shoes of the target of their criticisms; even fewer truly understand the context and situation at the time the decision was made. With these facts in mind and by using recognized ethical models as well as precepts related to LOAC, this paper demonstrates that from both legal and ethical perspectives, the president's actions were justi-

fied. Politicians or military leaders finding themselves in comparable circumstances would approve of the president's judgment and choices, however unpopular they may have been. The paper also shows that the final findings can thereafter be applied to more contemporary situations, whether ongoing or in the future.

The Cambodian Incursion

At the end of April 1970, American and Republic of Vietnam (RVN) forces launched a series of attacks into the territory of the officially neutral state of Cambodia. This operation—which came to be known as the Cambodian incursion—involved approximately 50,000 ground troops from the Army of the Republic of Vietnam (ARVN) as well as 30,000 US Army personnel.⁴ The incursion was accompanied and supported by an aerial bombardment campaign undertaken by American aircraft from both the Air Force and the Navy.⁵ Ordered by Nixon, the stated purpose of the raids was to destroy established Vietcong (VC) and People's Army of Vietnam (PAVN) sanctuaries and strongholds in Cambodia, from which numerous attacks had been launched against the RVN. The president and his closest supporters, in particular his national security advisor, Henry Kissinger, ultimately hoped to "undercut the North Vietnamese invasion of that country so that Vietnamization and plans for the withdrawal of American troops could continue in South Vietnam."⁶ Prior to the deployment, there was no formal consultation with the US Congress or the Senate Foreign Relations Committee.⁷

In a televised speech on 30 April 1970, Nixon officially advised the American public about the operation, enflaming growing antiwar sentiment in the United States and resulting in condemnation and outrage from sources ranging from ordinary citizens to journalists, academics, and members of the Congress. Critics of the decision accused Nixon and his advisors of blatantly violating the US Constitution and ignoring international law, as well as showing a disconcerting lack of moral and ethical judgement. Despite the backlash in public opinion, the operation carried on as planned for almost two months, with American forces withdrawing to their bases in South Vietnam by the end of June.

From a purely military standpoint, the Cambodian incursion, dubbed Operation Toan Thang 43,⁸ was deemed a moderate success in that it "set the NVA [North Vietnamese Army] offensive timetable back at least a year, probably 18 months, and possibly two years."⁹ Few could argue that the operation dealt the North Vietnamese forces a significant blow, with vast quantities of vital materiel and equip-

ment destroyed or captured.¹⁰ Notwithstanding the widely reported successes, Nixon was nevertheless vilified for expanding the war, unleashing a humanitarian disaster in Cambodia, and abusing his powers as president and commander in chief. Those who supported his decision at the time were definitely a minority of the population, especially in the United States.

Legal Issues

The legal aspects of conflicts of an international nature are unarguably complex, numerous, and multifaceted—the 1970 Cambodian incursion is no exception. Nevertheless, those who have embarked on a detailed study of Operation Toan Thang 43 have usually limited their focus to three central themes relating to the legality of the operation: the neutrality of Cambodia, the right to collective self-defense, and the constitutional powers of the US president. That many disparate experts have singled out these three facets of LOAC and American constitutional law in their examinations is no coincidence, given that they were repeatedly trumpeted by both Nixon and members of his administration as the sources from which the legitimacy of the incursion was derived.

Customary international law and LOAC are very clear regarding the concept of neutral states as well as the responsibilities of these states in ensuring neutrality is maintained in times of conflict. Specifically, duties of a neutral state include “obligations to prevent belligerents from transporting troops or supplies across neutral territory and to prevent neutral territory from being used for base camps, munitions factories, supply depots, training facilities, communications networks, or staging areas for attacks.”¹¹

Prior to the attack, the Cambodian government made some very public diplomatic representations to Hanoi to prevent violations of the country's neutrality by the NVA and the VC; however, the efforts were largely symbolic. In an address given in New York City in late May 1970, the legal adviser of the US State Department, John R. Stevenson, pointedly accused Cambodian officials of failing to do all that they should to safeguard neutrality under the requirements of the LOAC. He even confirmed that the previous Cambodian government under Prince Sihanouk had tacitly allowed and even condoned the shipment of communist arms and munitions through the Port of Sihanoukville.¹² As a result of this inaction and apparent deception on the part of the Cambodians, the United States determined that Cambodia had surrendered its standing as a neutral state and no longer enjoyed protection under the LOAC. Thus, the prohibition

against attacking a neutral state was invalidated in this case, given the actions of the Cambodian government.

Not surprisingly, the decision to question Cambodia's neutrality as a pretext to launching the operation met with some resistance by experts opposed to the incursion. Many in the media and the antiwar movement questioned the US and RVN authorities' assessment that Cambodia had forfeited its neutrality. They explained that the apparent inaction was largely due to that nation's physical inability to repel the PAVN forces rather than a conscious decision by the Sihanouk and Lon Nol governments to allow the unrestricted use of their territory.¹³ Though not disputing the possibility that this view may be valid in some respects, John Norton Moore, director of the Center for National Security Law, provided additional legitimacy to the arguments in favor of the action in an opinion piece published in January 1971. He emphasized the following aspect of customary international law: "It is well established . . . that a belligerent Power may take action to end serious violations of neutral territory by an opposing belligerent when the neutral Power is unable to prevent belligerent use of its territory and when the action is necessary and proportional to lawful defensive objectives."¹⁴ This legal opinion presented further justification for a neutral country conducting cross-border operations: the right of self-defense.

The second legal argument on which American officials based their decision to undertake the incursion related to the inherent right of nations, in this case the United States and the Republic of Vietnam, to practice collective self-defense. To a lesser extent, the stated principle of collective defense was also meant to include Cambodia itself, regardless of the fact that its government had not formally or directly approached the American government for military assistance. As communist forces continued to flood into Cambodia in the spring of 1970, the Lon Nol government put out a general plea for aid, and the United States answered with the incursion. Nixon argued that this indirect request further reinforced the rationale for the operation.¹⁵

PAVN troops had, for nearly five years, launched deadly strikes on American and RVN forces in South Vietnam from the relative safety of their Cambodian sanctuaries. These attacks intensified significantly in the weeks leading up to the incursion.¹⁶ Nixon feared that without an armed intervention aimed at unseating the PAVN and the VC, Cambodia would become "an open-ended staging area from which to mount attacks on South Vietnam that would jeopardize . . . US troop safety, and US troop withdrawal."¹⁷ NVA attacks also posed an important threat to the process of Vietnamization, which could endanger the very survival of the Republic of Vietnam in the long term.¹⁸ Since

less drastic military and political measures had proven inadequate in evicting the North Vietnamese in the past, Nixon authorized the military operation in late April 1970.

In addition to the LOAC, the Nixon administration relied on UN agreements in justifying its actions. John Lawrence Hargrove, director of studies at the American Society of International Law, explained that Article 51 of the UN Charter did not exclude, in the case of a military attack, "an exercise of the right of self-defense on the territory of a foreign state which is not itself the attacker, even without the consent of this state."¹⁹ Given that the United States and the Republic of Vietnam had already been engaged in collective measures of self-defense since 1965, Hargrove therefore extrapolated that the recourse to military action in such a case could be justified.

The Nixon administration further tied its rationale for the incursion to the premise of collective self-defense by relying on other key aspects of the UN Charter. In particular, legal advisors cited the passages which confirmed that the "use of armed force is prohibited except . . . where the Security Council has not acted, in individual or collective self-defense against an armed attack."²⁰ Since the Cambodian government's 22 April 1970 appeal to the UN for assistance in fighting the invaders had been ignored, the legality of the incursion was reinforced when the United States took the action that it deemed necessary to ensure that collective self-defense was assured.²¹

The final legal argument Nixon relied on in framing the rationale for the incursion is based largely in American constitutional law but is also tied to the LOAC. Regardless of one's opinion regarding the US involvement in the Vietnam war itself, the buildup of PAVN forces in Cambodia unquestionably posed a real threat to US national security interests of the day. Some critics argued that the framers of the US Constitution had specifically intended to have Congress decide which threats imperiled national security, thereby limiting the president's power to do so. In response, Congress unilaterally choose to utilize a military solution.²²

Conversely, political scientist and author Eugene Rostow, in quoting from Alexander Hamilton's well-known Federalist Paper No. 23, aptly described that since "the circumstances that endanger the safety of nations are infinite . . . no constitutional shackles can wisely be imposed on the [executive] power to which the care of it is committed."²³ In essence, "[Nixon] maintained that as Commander-in-Chief he had the constitutional authority to order the Cambodian operation to protect US troops . . . [and] he did not have to consult Congress first."²⁴ This interpretation is in line with certain tenets of the US Constitution which confirm that the president's power "includes

broad authority to make strategic and tactical decisions incident to the conduct of a Constitutionally authorized conflict.”²⁵ Since the Gulf of Tonkin Resolution of 1964 had granted Pres. Lyndon B. Johnson the authority to approve the use of force in the entire Southeast Asia region without a formal declaration of war by Congress, Nixon and his advisors considered the Cambodian incursion as being incidental to the conduct of the Vietnam War and, thereby, by extension, a constitutionally approved conflict.

Moral and Ethical Issues

Just as Nixon was accused by many of initiating an illegal military operation and overstepping his constitutional authority, so too was he criticized regarding the morality of his decision. Following his 30 April address to the nation, widespread protests and civil disobedience ensued throughout the United States. He was lambasted in the press, and the US Senate Foreign Relations Committee convened hearings where prominent American religious leaders questioned the moral leadership of the executive branch.²⁶ The choices that he made with respect to potentially escalating the conflict in Southeast Asia may have been unpopular, but this does not mean that they were ethically unsound.

In considering the morality of Nixon's order for US and ARVN forces to embark on Operation Toan Thang 43, a number of moral philosophies or doctrines, including variations of each, may be considered. Two of these moral theories, utilitarianism and Kantianism (or Immanuel Kant's moral theory), prove relevant in demonstrating that Nixon did act in an ethical manner by authorizing this military action.

The most logical method of determining whether the actions were ethical is to apply the principles of utilitarianism or, more precisely, a more modern form known as preference utilitarianism. The basic premise of this theory states that “the action that is best is the one that satisfies the most preferences [of individuals], either in themselves, or according to [the action's] strength or . . . order of importance.”²⁷ By the time the operation began, the American public had lost its appetite for the war in Vietnam, and widespread calls for a withdrawal of US troops were commonplace. In response, Nixon had already announced a large-scale downsizing of the number of troops in Southeast Asia, with the ultimate aim of a complete withdrawal. This plan was tied closely to the program of Vietnamization. However, the increasing NVA attacks on US forces in South Vietnam in the spring of 1970, most of which originated in Cambodia, threatened this plan.

Thus, Nixon's decision to authorize the incursion was taken in large part to ensure that the desire, or preference, voiced by Americans to pull out of the war remained viable. Nixon and his advisors believed that because this operation would deal a significant blow to the NVA and VC forces, they would no longer pose a serious threat to American troops and, thus, the process of handing over responsibility to the ARVN for its own security would continue unimpeded. The president also hoped that any military successes resulting from the operation would compel the North Vietnamese to return to the negotiating table and accept a cease-fire under terms favorable to the United States. In the eyes of the Nixon administration, such a peaceful resolution to the conflict would not only ensure the viability of a free South Vietnam but would also be a victory in the larger battle between good and evil.

Since the beginning of the Cold War, successive American governments emphasized that the struggle against communism was a worthy moral crusade, based largely on protecting the values of democracy and freedom throughout the world. Preference utilitarianism helped validate the US predilection for a world order based on the concept of self-determination and devoid of political and military oppression. This corroboration drove many of the American leaders' decisions regarding the conduct of the war in Southeast Asia. It was therefore believed that a firm stand in Vietnam would counter "the much wider scheme of world domination by the Soviet Union and contribute to [the] larger global struggle against this new form of imperialism."²⁸

In addition to the anticommunist element of the president's thinking in authorizing the incursion, there also existed a larger view that failure in Vietnam would have wider repercussions on the cause of peace in the world. In his book *No More Vietnams*, Nixon wrote that "our acquiescence in aggression would encourage further aggression; our defeat and humiliation in South Vietnam without question would promote recklessness in the councils of those great powers who have not yet abandoned their goals of world conquest."²⁹ Though he did not relish escalating violence amidst an ongoing troop withdrawal, he saw the incursion as a morally necessary action to meet the preferred option of a lasting peace.

The morality of the decision to order the incursion can also be assessed by utilizing Kant's moral theory, which posits that "an act has moral worth only if it is done with right intention or motive."³⁰ In this case, it is not the final outcome of a choice that matters—be it positive or negative—but the reason the action was taken in the first place. The theory also assumes that any rational person, placed in the same position, would make the same decision. As described above, Nixon's ob-

jective in instigating the operation was to neutralize the enemy's ability to engage US forces in South Vietnam and to induce the North Vietnamese to accept a diplomatic resolution to the war. This was also closely linked to what he, as commander in chief, believed was his legal and moral duty to safeguard American personnel.³¹

Considerations regarding communism and the US ability to contain its spread also had a role to play in the president's intentions with respect to the operation in Cambodia. Nixon emphasized this aspect of this decision when he said, "I would rather be a one-term president and do what I believe was right, than be a two-term president at the cost of seeing America become a second-rate power."³² That the desired outcome of the incursion was not wholly achieved in the long term is immaterial in this instance—Nixon can be considered to have acted ethically because his overall intentions were honorable.³³

Conclusion

Nixon's decision to authorize the 1970 military incursion into Cambodia was unquestionably controversial. Much of the literature written about this operation, especially in the years immediately following its completion, is critical of the rationale and explanations that Nixon and the administration provided in justifying their actions. More recent studies, however, tainted far less by the widespread antiwar sentiment that existed in the United States in the early 1970s, have provided more balanced and objective scrutiny.

Undoubtably, many will continue to believe that Nixon made the wrong decision with respect to the Cambodian problem. As is normally the case, the voices and views of the vocal minority often eclipse those of the silent majority. The final assessment about whether the Cambodian incursion, regardless of its long-term impact, was the right thing to do at the time is best summarized in a letter to the *New York Times* from the father of a US soldier killed in Vietnam:

Had the fathers of these young men known that this nation would countenance a sanctuary a scant 50 miles from Saigon, we would have counseled them against induction. That we did not is a burden we will always bear. A great percentage of our ground [troops] dead from 1965 to 1970 came from an enemy who with impunity was staged, trained and equipped in the Parrot's Beak of Cambodia. The perfidy . . . is anything but the US bombing of the sanctuary itself. The perfidy lies in the fact that for more than four years the United States of America, without serious recorded concern, allowed her fighting men to be attacked, maimed and killed from a position which was itself privileged from either ground or air retaliation.³⁴

With the above statement in mind, it becomes easier to support the decision made by the president. Few individuals have had to shoulder

the burden of making such monumental decisions, needing to take into account public opinion and security as well as political and military factors. From a legal perspective, Nixon and his advisors correctly questioned Cambodia's neutrality, championed the right of collective self-defense, and referred to the constitutional role and responsibilities of the commander in chief in explaining their actions, fully believing they were legally permitted and required to launch the operation. This legal point of view has since been supported by a growing number of experts. From an ethical perspective, the president truly felt that his actions were ethical and would "end the war in Vietnam, and win the just peace desired [by Americans]."³⁵ Thus, contrary to the charges of many of Nixon's detractors, [his] decision to authorize the operation "was taken carefully, with much hesitation . . . and [with assumption of] full responsibility."³⁶

Nixon's decision to approve the Cambodian incursion added fuel to the fire being stoked by antiwar activists in the 1970s and also drew condemnation from opponents of the United States, especially in the Soviet Union. His determination to focus on the legal and moral aspects of the decision served as a valuable example for his successors and remains a valid approach to this day. Though the voices of the silent majority were often drowned out by protests of a vocal minority and accounts of the subsequent demonstrations and clashes continue to fill the history books, the reality is that the incursion was widely supported, both at home and abroad.³⁷ A CBS telephone survey taken immediately after Nixon's 30 April speech announcing the operation found respondents two-to-one in favor of the president's position. Opinion polls confirmed that Nixon's overall approval rating rose from 51 percent at the end of March to 57 percent at the beginning of May 1970.³⁸ Outside the United States, as least among allies, open criticism by sitting governments was rare.³⁹ Through it all, it was Nixon's continued assurances that the operation was legally and morally sound that strengthened his position and helped deflect criticism of the United States. It is this strategy that bears emulation if the interests and relations of the United States are to continue to be safeguarded.

The actions taken by Nixon justifying the 1970 Cambodian incursion were rooted in the legal and ethical aspects of decision making. In doing so, particularly in his capacity as commander in chief, he was by no means unique. Previous presidents, as well as those following Nixon, also understood this important fact: while a decision by an American president to use military force may be permissible under international and constitutional law, that does not necessarily make it right. Equally, even if recourse to war may appear to be the right

thing to do from an ethical perspective, it may not be supportable under the law. Only when a president effectively shows that he is both legally and morally justified in turning to war to address a threat to national security and national interests is he thereby more likely to avoid a tempest of criticism and a degradation in internal and external relations. Despite all of his own personal foibles and character shortcomings, Nixon understood this fact clearly and took the steps necessary to safeguard his position and reputation. Had others followed his example in more recent years, some of the criticisms aimed at certain commanders in chief and their administrations could have been avoided.

Notes

1. Ann Van Wynen Thomas and A. J. Thomas, Jr., *The War-Making Powers of the President: Constitutional and International Law Aspects* (Dallas: SMU Press, 1982), xi.
2. James M. McCormick, "Clinton and Foreign Policy: Some Legacies for a New Century," in *The Postmodern Presidency: Bill Clinton's Legacy in U.S. Politics*, ed. Steven E. Schier (Pittsburgh, PA: University of Pittsburgh Press, 2000), 60.
3. Gary C. Jacobson, *A Divider, Not a Uniter: George W. Bush and the American People* (San Diego, CA: Pearson Education, 2007), 99.
4. Spencer C. Tucker, ed., *Encyclopedia of the Vietnam War: A Social, Political and Military History* (Santa Barbara, CA: ABC-CLIO, Inc., 1998), 95.
5. Edward R. Drachman and Alan Shank, *Presidents and Foreign Policy: Countdown to Ten Controversial Decisions* (New York: State University of New York Press, 1997), 151. In fact, the aerial bombardment which took place during the Cambodian incursion was a continuation of a secret bombing campaign which had begun in March 1969, without the knowledge of the US Congress or the American public.
6. James M. Griffiths, *Vietnam Insights: Logic of Involvement and Unconventional Perspectives* (New York: Vantage Press, 2000), 72.
7. William Bundy, *A Tangled Web: The Making of Foreign Policy in the Nixon Presidency* (New York: Hill and Wang, 1998), 153. The decision by the notoriously secretive Nixon was not taken in an attempt to deceive Congress but instead to ensure security and deflect criticism that could delay start of the operation.
8. Joseph R. Cerami, "Presidential Decisionmaking and Vietnam: Lessons for Strategists," *Parameters* 26 (Winter 1996-97): 69.
9. Philip B. Davidson, *Vietnam at War: The History, 1946-1975* (New York: Oxford University Press, 1988), 628; and Shelby L. Stanton, *The Rise and Fall of an American Army* (New York: Presidio Press, 1985), 341.
10. J. D. Coleman, *Incurtion: From America's Chokehold on the NVA Lifelines to the Sacking of the Cambodian Sanctuaries* (New York: St. Martin's, 1991), 265; and Tucker, *Encyclopedia of the Vietnam War*, 97. The operation resulted in the capture or destruction of 16 million rounds of ammunition, 14 million pounds of rice, and 23,000 weapons; additionally, 11,369 communist troops were killed, 4,534 wounded, and 2,328 captured.
11. John Norton Moore, "Legal Dimensions of the Decision to Intercede in Cambodia," *American Journal of International Law* 65, no. 1 (January 1971): 65.

12. John R. Stevenson, "United States Military Action in Cambodia: Questions of International Law," in *The Vietnam War and International Law: The Widening Context*, ed. Richard A. Falk (Princeton, NJ: Princeton University Press, 1972), 27.

13. Coleman, *IncurSION*, 214-16. Lon Nol, who had been Cambodia's prime minister since 1966, was named president of the Khmer Republic on 18 March 1970, after a bloodless coup deposed Prince Sihanouk. An avid anticommunist, Lon Nol had been far more vocal than his predecessor in calling for the withdrawal of NVA and VC troops; however, he lacked the wherewithal to back up his demands with action.

14. Moore, "Legal Dimensions of the Decision," 47.

15. Robert H. Johnson, "Vietnamization: Can It Work?" *Foreign Affairs* 48, no. 4 (July 1970): 637.

16. NVA forces had also stepped up attacks on Cambodian towns in that same time period, signaling their intention to move on the capital of Phnom Penh.

17. Griffiths, *Vietnam Insights*, 149.

18. William Shawcross, *Sideshow: Kissinger, Nixon and the Destruction of Cambodia* (New York: Simon and Shuster, 1979), 89-90. Vietnamization was a military-economic program of South Vietnamese development which would permit rapid but phased withdrawal of US forces without radically upsetting the power balance in Southeast Asia and the handover of responsibilities to the RVN forces.

19. John Lawrence Hargrove, "Comments on the Articles of the Legality of the United States Action in Cambodia," *American Journal of International Law* 65, no. 1 (January 1971): 81-82.

20. Stevenson, "United States Military Action in Cambodia," 31.

21. Henry Kissinger, *White House Years* (Boston: Little, Brown and Co., 1979), 489.

22. Francis Wormuth, "The Nixon Theory of the War Power: A Critique," *California Law Review* 60, no. 3 (May 1972): 628.

23. Eugene V. Rostow, "The 'Lessons' of Vietnam and Presidential Powers," *Strategic Review* 12, no. 4 (Fall 1984): 36.

24. Drachman and Shank, *Presidents and Foreign Policy*, 166.

25. Moore, "Legal Dimensions of the Decision," 83.

26. Senate, *Moral and Military Aspects of the War in Southeast Asia: Hearings before the Committee on Foreign Relations*, 91st Cong., 2nd sess., 1970, 15.

27. Barbara MacKinnon, *Ethics: Theory and Contemporary Issues*, 2nd ed. (Belmont, CA: Wadsworth Publishing, 1998), 41.

28. David Armstrong, "No End of a Lesson: Vietnam and the Nature of Moral Choice in Foreign Policy," in *Ethics and Statecraft: The Moral Dimension of International Affairs*, ed. Cathal J. Nolan (London: Praeger Publishers, 2004), 84.

29. Richard M. Nixon, *No More Vietnams* (New York: Arbor House Publishing, 1985), 114.

30. MacKinnon, *Ethics: Theory and Contemporary Issues*, 53.

31. Peter A. French, *Ethics in Government* (Englewood Cliffs, NJ: Prentice-Hall, Inc., 1983), 41.

32. Stephen Graubard, *Command of Office: How War, Secrecy and Deception Transformed the Presidency from Theodore Roosevelt to George W. Bush* (New York: Basic Books, 2004), 394.

33. Nixon was repeatedly accused of misleading Americans regarding his intentions with respect to this operation. Some theorized that his actions were intended only as a face-saving measure against the bellicose North Vietnamese, who refused to consider a diplomatic settlement on US terms, and as a way of containing the feared spread of communism. It would be naïve to believe that Nixon did not consider the favorable political impact that would result from an orderly withdrawal from South Vietnam in

the shortest time possible and with the fewest casualties. However, these considerations were secondary to his belief that he was doing the right thing for the country.

34. Richard M. Nixon, *The Real War* (New York: Warner Books, 1980), 110.

35. Richard M. Nixon, "Cambodian Incursion Address" (speech, Washington, DC, 30 April 1970), <http://inspirationalspeakers.wordpress.com/2007/12/07/richard-m-nixon-cambodian-incursion-address> (accessed 29 September 2009).

36. Kissinger, *White House Years*, 502.

37. Melvin Small, *Johnson, Nixon, and the Doves* (London: Rutgers University Press, 1988), 100, 163. The term *silent majority* was first used by Nixon in a November 1969 speech in an attempt to attract inactive moderates to support the policies surrounding Vietnamization.

38. Hal W. Bochín, *Richard Nixon: Rhetorical Strategist* (New York: Greenwood Press, 1990), 66.

39. Alexander J. Banks, "Britain and the Cambodian Crisis of Spring 1970," *Cold War History* 5, no. 1 (February 2005): 100–101.

Abbreviations

ARVN	Army of the Republic of Vietnam
LOAC	law of armed conflict
NVA	North Vietnamese Army
PAVN	People's Army of Vietnam
RVN	Republic of Vietnam
UN	United Nations
VC	Vietcong

Developing a US European Command Intelligence, Surveillance, and Reconnaissance Strategy for FY 2010-15

*Lt Col Kevin M. Coyne, USAF**

Intelligence analysts . . . must open their doors to anyone who is willing to exchange information, and this includes Afghans and non-governmental organizations as well as the US military and its allies.

—Maj Gen Michael T. Flynn, US Army

"Our number one priority is the current fight, which means the fight in Central Command," said Gen Roger Brady, commander of the US Air Forces in Europe (USAFE), highlighting a major challenge facing most of today's theater component and combatant commanders.¹ As the United States continues to fight overseas contingency operations (OCO) in Afghanistan and Iraq, the nation's war-fighting resources remain dedicated to prevailing in today's wars.² This study examines how America's OCO focus in the US Central Command (USCENTCOM) impacts the operations of other commands by analyzing US European Command's (USEUCOM) ability to execute an effective intelligence, surveillance, and reconnaissance (ISR) strategy in pursuit of its intelligence requirements.

To begin this discussion, the impact of ISR operations in USEUCOM during the 1990s is introduced, followed by national and Air Force-specific strategies and their impact on USEUCOM's strategy of active security. The topics then turn to specific threats to US national security interests in the USEUCOM area of responsibility (AOR), the command's responsibilities versus these threats, and USEUCOM's ability to meet its responsibilities and requirements with allocated ISR resources.

I propose a three-tiered mitigation strategy based on this information. For a long-term solution, USEUCOM ISR planners can mitigate command collection gaps through the use of the North Atlantic Treaty Organization's (NATO) alliance ground surveillance (AGS) system, scheduled for delivery in 2014. As a mid-term solution, the United States would team with the Royal Air Force (RAF) to begin planning the integration of US-purchased RC-135 Rivet Joint aircraft into

*Mr. Michael Ivanovsky, USAF civilian, was the essay advisor for this paper.

USEUCOM ISR collection profiles. Finally, in the near term, USEUCOM can engage with the German Air Force (GAF) to develop tactics, techniques, and procedures (TTP) for combined postmission processing of EuroHawk-derived signals intelligence (SIGINT) to meet command collection requirements. With most ISR assets still dedicated to supporting OCO in USCENTCOM, I contend that other theaters competing for remaining scarce ISR resources—such as USEUCOM—should develop requirements-based collection strategies that better integrate current and planned allied capabilities to offset collection shortfalls.

ISR in USEUCOM—The 1990s

USEUCOM witnessed a high point of theater ISR collection operations in the 1990s due to the Balkan crises in Croatia, Bosnia-Herzegovina, and Kosovo. In 1995 the Bosnian civil war was in its third year; by that summer, the international community coalesced to put an end to the conflict by attempting to coerce the Bosnian Serbs to the negotiating table through an air campaign primarily targeting their heavy weapons. Operation Deliberate Force lasted from 30 August to 14 September 1995, with airborne ISR sensors playing a critical role in verifying Bosnian Serb compliance “by obtaining needed combat information in the planning, execution and combat assessment phase” of the operation.³ The U-2 and Predator played key roles in monitoring Bosnian Serb heavy weapons sites and assessing “whether the Serbs were withdrawing, or at least demonstrating an intention to withdraw.”⁴

ISR contributions to the success of Deliberate Force were significant not only in making real-time strike decisions but also in highlighting the contributions of allied ISR capabilities. In fact, “five nations employed 13 different manned or unmanned recce [reconnaissance] platforms for purposes that included monitoring heavy weapons as well as making assessments.”⁵ British, French, German, and Dutch tactical and select strategic reconnaissance aircraft were integrated with US ISR assets in a combined air tasking order (ATO) to add “to the total information available to the combined air and space operations center.”⁶ In sum, while Deliberate Force validated both the criticality of US and allied ISR assets to the joint/combined fight, it also demonstrated how allied ISR capabilities could be seamlessly integrated with US operations.

Renewed violence in the Balkans from March to June 1999 due to the Kosovo crisis affected US ISR programs, had an impact on future ISR asset availability, and highlighted shortfalls in connecting allied ISR capabilities to the US federated intelligence architecture. In an after-action lessons learned report to Congress on Operation Allied

Force, the chairman of the Joint Chiefs of Staff (CJCS), Gen William L. Shelton, and Secretary of Defense (SecDef) William S. Cohen, notified Congress of the Department of Defense's (DOD) increased investments in ISR programs by approximately \$2.5 billion for sensors; aircraft; and tasking, production, exploitation, and dissemination (TPED) capabilities.⁷ In their view, "better sensors with improved dissemination capabilities are needed to provide a capability to counter any future adversary."⁸ The critical need for more remotely piloted aircraft and greater TPED capacity was especially compelling because of the low density and high demand (LD/HD) of manned ISR aircraft, such as the U-2 and the RC-135. These aircraft were "especially critical since they also support multiple intelligence activities in other areas around the world."⁹ Thus, DOD leaders were aware of how competing intelligence requirements impeded their ability to provide combat-mission-ready ISR forces in sufficient numbers. LD/HD assets needed to be more carefully managed; even then, their availability could not be guaranteed.

Finally, the CJCS and SecDef stressed that "the Department must develop a clear policy and implementation plan to explain when and how coalition partners can be connected to US networks and how data can be shared with those partners."¹⁰ In their view, one solution to the US TPED challenge was through increased reach-back to US-based processing capacity. In addition, they believed that allied partners who were contributing ISR assets to a joint/combined campaign should be able to benefit from and share in the intelligence output. This study takes the Kosovo lessons-learned recommendation one step further and argues that our allies should integrate their sensor and TPED capacities into the US intelligence community's (IC) federated architecture and assist in the production process. This simple step of creating seamless US and allied intelligence production and information sharing, still not a reality 10 years after the Kosovo after-action report, could readily help the USEUCOM combatant commander begin to meet unfulfilled collection requirements due to limited ISR resources.

Unfortunately, the DOD calls for greater ISR investments, and process overhauls did not come in time to meet the challenges caused by the terror attacks of 9/11. Still reconstituting after Operation Allied Force, US ISR assets and personnel surged to meet USCENTCOM requirements during Operation Enduring Freedom in October 2001. The surge in ISR operations exceeded steady-state operating levels for service ISR assets and continues to impact the requirements of other combatant commanders (COCOM). Today, USCENTCOM collection requirements absorb the majority of US ISR

assets, with other COCOM requirements met by residual US ISR assets on a shared or rotational basis.

ISR Strategy Review

This US ISR strategy review will not only reemphasize and highlight US priorities but also offer strategic areas where competing theaters can explore ways to leverage allied ISR capabilities to meet their needs. The 2006 national security strategy (NSS) stresses three major threats to American and allied interests: global terrorism, regional conflicts, and weapons of mass destruction (WMD).¹¹ Aside from strengthening US intelligence capabilities—especially against the WMD threat—working with allied power centers and strengthening relations with them are critical to countering these threats. The leveraging of “NATO capabilities must be accelerated” to strengthen this partnership and make it more effective.¹² America’s 2006 *National Security Strategy for Combating Terrorism* takes this one step further and calls for expanding partner capacity in the realm of intelligence and providing friendly states with the training, equipment, and assistance they need to partner with the United States.¹³

The 2009 national intelligence strategy (NIS) complements the two aforementioned national strategies in the priorities for the IC writ large. The first two mission objectives outlined by the director of national intelligence (DNI) deal with combating extremism and WMD proliferation. The third objective concerns strategic intelligence and warning and the monitoring of events so “policymakers and military officials can effectively deter, prevent, or respond to threats and take advantage of opportunities.”¹⁴ Interestingly, the NIS also calls on the IC to improve collaboration and “conduct strategic outreach to key external centers of knowledge and expertise.”¹⁵ The DNI’s message on leveraging allied partnerships is clear: due to worldwide threats of extremism, WMDs, and the necessary strategic warning nation states require, efficiency of scale in meeting these global challenges can be achieved only through collaboration with our allies.

Leveraging and expanding allied capabilities and coming to terms with efficiently managing LD/HD ISR assets are DOD-level issues. First, to address the problem of LD/HD asset management and developing an ISR strategy, the 2006 quadrennial defense review (QDR) established a joint functional component command (JFCC)-ISR under US Strategic Command to “synchronize strategy and planning and integrate all national, theater and tactical ISR capabilities.”¹⁶ JFCC-ISR is responsible for arbitrating competing command collection requirements and allocating ISR resources. With US intelligence focused on

USCENTCOM, however, JFCC-ISR processes do not guarantee an asset increase for competing COCOMs. Secondly, the QDR also addressed the criticality of bolstering allied capabilities and directed investments to stand up NATO's planned intelligence fusion cell, which would reside within USEUCOM. The fusion cell could help service the command's intelligence requirements if leveraged effectively.

The 2010 QDR continues the trend of expanding DOD ISR capabilities through greater investments in "long-dwell unmanned aircraft systems (UAS), such as the Predator and Reaper."¹⁷ Already on track to grow the number of Predator/Reaper orbits from 37 to 50 by fiscal year (FY) 2011, the Air Force is now committed to increasing the number to 65 by FY 2015; the Army will expand all classes of UASs.¹⁸

Problematic for USEUCOM, however, is that this increase in ISR capability is intended for counterinsurgency, stability, and counterterrorism operations.¹⁹ As Secretary Gates pointed out during the official release of the QDR, "We have to a considerable extent stripped the other combatant commands of much of their ISR capability to put into the fight in Iraq and Afghanistan. The reality is that huge demands all over the world are for these capabilities."²⁰ As long as contingency operations in Afghanistan and Iraq are ongoing, the QDR's increase in ISR investments will largely go to meet the requirements of those conflicts. The stripping of ISR assets from other commands will continue. The 2010 QDR continues the theme of leveraging partner capacities as an "important dimension of US defense strategy."²¹ USEUCOM must look toward greater engagement with its allies to overcome intelligence collection shortfalls and information gaps.

At a service level, the Air Force's 2006 *Security Cooperation Strategy* (SCS) is in line with the DNI's vision of increased intelligence cooperation with partner nations. In fact, the SCS states that "intelligence relationships provide a means of unique access to data that the US might be otherwise unable to obtain."²² However, US partners must have the capabilities and the capacity to obtain such information, and, if they do, these capabilities can be used to satisfy US "global and regional objectives."²³ The SCS speaks directly to USEUCOM's dilemma of not being able to satisfy all of its collection requirements due to lack of ISR resources and, from a DOD perspective, provides a possible strategy for leveraging allied capabilities to meet COCOM needs. This is critically important in light of the UK's RC-135 foreign military sales (FMS) procurement effort and the GAF's direct commercial sale (DCS) effort to procure the RQ-4 Global Hawk.

Air Force security cooperation objectives are important, but do they coincide with Air Force ISR strategy goals? A review of the service's 2008 strategy for ISR lacks any mention of partnering with al-

lies, expanding allied capacity, or leveraging allied unique ISR capabilities to satisfy US national or COCOM collection requirements. This does not mean that the SCS and ISR strategies contradict each other. While there is no specific mention of partnering with allies, the Air Force's ISR strategy stresses the criticality of "global cross-domain integrated knowledge dissemination."²⁴ At the heart of this effort is the distributed common ground station (DCGS) intelligence processing architecture. Allied investments in ISR capabilities compatible with DCGS, like the GAF's RQ-4 procurement effort, could be easily integrated into the Air Force's DCGS architecture.

USEUCOM's strategy of active security is fully in line with the three major threats found in the 2006 US NSS. USEUCOM's mission statement calls for maintaining ready forces for global operations, securing strategic access and global freedom of action, strengthening NATO, promoting regional stability, and countering terrorism.²⁵ The command does this through two regional plans for Europe and Eurasia to prevent regional conflicts and three functional plans, two of which are specifically designed to combat terrorism and prevent the proliferation of WMDs. The third functional plan focuses on theater force posture and transformation and stresses that, while a forward US presence is critical for theater security, teaming with partners is just as important. "The posture of our forces and installations is shaped as much by our security cooperation activities as by our requirements for war fighting."²⁶ Thus, a large part of the COCOM's strategic approach to dealing with regional threats is to "mitigate risk while the [US] is at war through building partner capacity and enhancing interoperability."²⁷

The Way Ahead: Utilizing NATO Capabilities

While traditionally lacking in quantity and quality, European airborne ISR capacity is seeing significant expansion in both areas. As a potential long-term solution for USEUCOM's lack of airborne ISR, this study proposes increased cooperation with NATO as the alliance prepares for the 2012–14 scheduled full operational capability (FOC) of its interoperable AGS system.²⁸ In September 2007, the 21 participating AGS nations abandoned an initial multiplatform concept for a single air vehicle approach utilizing the RQ-4 Global Hawk Block 40. The multiplatform radar technology insertion program (MP-RTIP) ground surveillance radar will be the primary sensor.²⁹ The AGS's "Core" segment includes line-of-sight and beyond-line-of-sight connectivity, as well as on-site data processing and exploitation capabilities. With Sigonella, Italy, destined to be the main operating base,

NATO will for the first time have a dedicated ISR collection capability.³⁰ However, the most promising benefit of the AGS Core segment is its fully equipped interfaces and interoperability with national ISR systems. "The Core system will be supplemented by interoperable national airborne stand-off ground surveillance systems from NATO countries, thus forming a system of systems."³¹ This is no small undertaking for NATO. Until AGS, NATO never had its own intelligence collection capability, but instead relied on the national assets of member states. Challenges in developing proper TTPs for platform and Core segment mission operations will abound.

NATO traditionally does not conduct its own intelligence collection. In fact, NATO's intelligence warning system (NIWS), with the NATO situation center at its hub, is primarily an analytical function that relies on information feeds from a variety of sources that include NATO-releasable messages from member states and information provided by the NATO political and military committees. This structure created a dependency on national architectures, with no ability by NATO to leverage those architectures. This offered little value-added to the nations providing the bulk of the information, that is, the United States and USEUCOM.³² In *NATO Intelligence and Early Warning*, John Kriendler said that "the ability of a nation to provide intelligence, the willingness of a nation to share this intelligence and the time required for this intelligence to be disseminated to NATO are all constraining factors which compromise the overall NATO intelligence effort."³³

The FOC of the NATO AGS in 2014 will change this dynamic. By acquiring an indigenous collection capability, NATO will be both a collector and a producer of intelligence and will no longer depend solely on member states. European ISR strategists such as Klaus Becher see this as an opportunity for greater transatlantic cooperation because NATO will finally have the leverage to request greater "access to US capabilities."³⁴ In fact, "Europe's access to US-controlled intelligence on global security issues will depend on the practical value of European assets to US intelligence."³⁵

AGS will provide practical value as its pending FOC date offers USEUCOM an opportunity to satisfy collection gaps. As stakeholders, USAFE and USEUCOM maintain the knowledge and expertise on how to conduct RQ-4 operations and postmission processing in their AOR. This study recommends that the command engage with NATO now to develop the requisite TTPs for proper Core system utilization that the alliance currently lacks. This especially makes sense given the projected basing of three new Block 30 RQ-4s at Sigonella AB in October 2010. These aircraft will be operated by USEUCOM within the constraints of the JFCC-ISR allocation process.³⁶

Helping NATO develop TTPs for postmission processing is one way to gain access to AGS sensors. However, this study also recommends that USEUCOM champion greater NATO access to US intelligence collection capabilities and information to build the enhanced atmosphere of cooperation proposed by Becher. This will improve the effectiveness of AGS operations and lead to a revolution in intelligence sharing, given the “not releasable to foreign nationals” barrier the US IC currently uses to deter unwanted access. As a RAND study on intelligence process reform recently argued, “For the intelligence community, operational innovation must focus on changing and perhaps completely rethinking core functions.”³⁷

By helping NATO navigate the uncharted waters of operational intelligence collection and processing at the start of the AGS program, USEUCOM will be in a better position four years from now to leverage AGS capability. This initiative will have far-reaching effects by complementing ongoing efforts of the information-sharing integrated process team (IPT) sponsored by DOD’s ISR task force. Based largely on the experiences of working with our allies in Afghanistan, the IPT seeks to transcend cultural, technical, and arcane classification barriers that prohibit the free-flow exchange of intelligence information with our allies. At a minimum, the results of the IPT will lead to a transformation of the DOD’s foreign disclosure and classification procedures, if not its core intelligence processes. USEUCOM could set the new standard for the DOD’s information sharing process with our allies.

The Way Ahead: Utilizing Bilateral Relationships

Mid- and near-term solutions to USEUCOM ISR collection gaps can be found in existing bilateral partnerships. Many changes are under way in the development and fielding of allied capabilities that promise to alleviate “fragile dependence.” Both the UK’s RAF and the Federal Republic’s GAF are in the process of leveraging and procuring US ISR technologies to meet their national intelligence requirements. There is no reason why USEUCOM and USAFE should not work with our allies to fully integrate their systems into USEUCOM’s ISR collection profiles and fill command collection gaps. Due to severe cost overruns of Project Helix, the replacement program for the UK’s ageing Nimrod aircraft, the UK approached the United States in 2007 to inquire about procuring three RC-135 Rivet Joint aircraft. Approved by the USAF chief of staff and Congress in 2008, the United States and the UK are now engaged in an FMS contract to deliver three RC-135 SIGINT aircraft. The deputy chief of staff for ISR and the DNI describe this effort as a “win-win” for both parties and an opportunity

to improve integration.³⁸ Fully in line with national strategy direction to engage with allies and harness their capabilities, the main objectives of this FMS contract address the command's "capability gaps through operational burden sharing" and focus on "maintaining and/or increasing manned SIGINT support to CENTCOM and EUCOM AORs."³⁹ With the first of three aircraft scheduled for delivery in 2013, RAF aircrews are now being trained on aircraft employment and utilization.⁴⁰ The RAF's RC-135 aircraft will provide a unique mid-term solution to help satisfy USEUCOM ISR collection gaps. The command should engage with the RAF now, through existing bilateral programs, and leverage in-theater Air Combat Command RC-135 expertise at RAF Mildenhall to plan the integration of the RAF's RC-135 aircraft into USEUCOM's theater ISR-collection profiles.

In the immediate future, a near-term opportunity to overcome USEUCOM's collection capability shortfalls presents itself in the GAF's fielding of the RQ-4 Block 20 "EuroHawk" remotely piloted aircraft (RPA). After a 2003 transatlantic test flight and associated sensor demonstration from Nordholz, Germany, the GAF signed a memorandum of understanding with the DOD in May 2006 that set the parameters for proceeding with a DCS contract of five RQ-4 RPAs.⁴¹ The rollout of the first EuroHawk vehicle was on 8 October 2009 in Palmdale, California.⁴² Current plans call for incorporating all five RQ-4 aircraft into the GAF's 51 Squadron, Jagel AB, Schleswig-Holstein, by 2011.⁴³ The GAF plans to use RQ-4's in-theater, rather than deploying them to Afghanistan. Germany is also procuring the Heron 1, a medium-altitude RPA from Israel, for use in overseas contingency deployments. With a total of five GAF-operated RQ-4s in its AOR by 2011, USEUCOM has a unique teaming opportunity to increase theater ISR-collection capability through the GAF.

One way to engage the GAF is by offering US expertise in developing TTPs for postmission processing of EuroHawk-derived SIGINT. The GAF will not be getting a turnkey system since the procurement effort is a DCS contract, consisting of the air vehicles and not the sensors (being developed by EADS). The 2003 electronics intelligence (ELINT) sensor demonstration showed that the GAF will be faced with significant mission and postmission processing challenges as it tries to operationalize its sensor packages.

According to a GAF spokesman, we were "surprised at the huge amount of radar emitters (merchant ships, airliners) that showed up in addition to the prepared [demonstration] profile . . . the ELINT Ground Support Station (EGSS) was quickly overwhelmed."⁴⁴ The GAF realized there "was more data than we could process," leading one to conclude that a DCGS stakeholder such as USEUCOM could

provide tremendous expertise to help the GAF normalize RQ-4 operations while gaining access to GAF sensors.⁴⁵

I recommend that USAFE expand its existing bilateral intelligence programs (traditionally focused on information sharing) to more dynamic agreements that include combined postmission processing opportunities with allied militaries such as the GAF. The intelligence gain for USEUCOM of integrating GAF operators into USAFE's DGS-4 ground station, or conversely, USAFE operators into the GAF's EGSS, will go a long way to help mitigate command ISR-collection gaps.

Conclusion

This study shows that despite continued DOD investments in ISR platforms, these capabilities will remain LD/HD assets as long as the United States is engaged in OCO with USCENTCOM. The Balkan conflicts of the 1990s proved ISR capabilities are force multipliers in the modern battlespace, prompting senior DOD leaders to take the right steps in calling for more ISR resources. These DOD leaders also acknowledged that due to the increased demand for ISR, they would be hard-pressed to field sufficient numbers of ISR assets to meet global needs. After the 9/11 attacks and the subsequent surging of ISR forces to the USCENTCOM AOR, ISR requirements from competing COCOMs could be met only through ISR rotational forces. This is still the case, causing collection gaps in all commands. National security and intelligence strategies, as well as USAF security cooperation and intelligence strategies, recognize that DOD ISR forces and capabilities are stretched thin. As this analysis demonstrates, national strategic direction provides guidance to warfighting commands to partner with allies and leverage their capabilities to help meet US national intelligence requirements. Intelligence is a field where synergistic efficiencies of cooperation can easily be achieved.

Given that President Obama's Afghanistan strategy calls for a surge in US forces and capabilities through 2011, USEUCOM must continue to look to other sources to mitigate its ISR collection gaps. In light of significant advances in allied ISR capabilities, teaming with NATO, the RAF, and the GAF presents itself as a unique opportunity for USEUCOM to bring about a revolution in intelligence sharing that could prove to be a benchmark of security cooperation success for other COCOMs to emulate.

Notes

1. Michael Hoffman, "USAFE Bases Key to Building, Maintaining Ties," *Defense News*, 21 September 2009.
2. US Department of Defense (DOD), *Quadrennial Defense Review Report 2010* (Washington, DC: Office of the Secretary of Defense [OSD], 2010), iii.
3. Robert C. Owen, *Deliberate Force: A Case Study in Effective Air Campaigning* (Maxwell AFB, AL: Air University Press, 2000), 234.
4. *Ibid.*, 228.
5. *Ibid.*, 223.
6. *Ibid.*, 228.
7. William S. Cohen and Gen Henry H. Shelton, *Kosovo/Operation Allied Force After-Action Report*, Report to Congress (Washington, DC: OSD and the chairman of the Joint Chiefs of Staff, 2000), 3.
8. *Ibid.*, xxi.
9. *Ibid.*, 54.
10. *Ibid.*, 131.
11. The White House, *National Security Strategy of the United States* (Washington, DC: Office of the President of the United States, 2006), 1.
12. *Ibid.*, 38.
13. The White House, *National Security Strategy for Combating Terrorism* (Washington, DC: Office of the President of the United States, 2006), 19.
14. US Director of National Intelligence, *National Intelligence Strategy* (Washington, DC: Office of the Director of National Intelligence, 2009), 7.
15. *Ibid.*, 8.
16. DOD, *Quadrennial Defense Review Report 2006* (Washington, DC: OSD, 2006), 56.
17. DOD, *Quadrennial Defense Review Report 2010*, 22.
18. *Ibid.*, 22.
19. *Ibid.*, 20.
20. DOD, "DoD News Briefing with Secretary Gates and Admiral Mullen from the Pentagon," <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4549>.
21. *Ibid.*, viii.
22. Department of the Air Force, *Security Cooperation Strategy: Building Capacity, Integrating Capabilities* (Washington, DC: Office of the Secretary of the Air Force, 2006), 10.
23. *Ibid.*, 10.
24. Department of the Air Force, *Lead Turning the Future: The 2008 Strategy for United States Air Force Intelligence, Surveillance and Reconnaissance* (Washington, DC: Office of the Deputy Chief of Staff for ISR, 2008), 14.
25. US European Command (EUCOM), *A Strategy of Active Security* (Stuttgart, Germany: Office of the Commander, EUCOM, 2008), 2.
26. *Ibid.*, 5.
27. *Ibid.*, 3.
28. "NATO Signs Initial \$26M Contract for AGS 'Eye in the Sky,'" *Defense Industry Daily*, <http://www.defenseindustrydaily.com/nato-signs-initial-26m-contract-for-ags-eye-in-the-sky-0450>.
29. Northrop Grumman, "NATO AGS," <http://www.as.northropgrumman.com/products/natoags/index.html>.
30. NATO, "Alliance Ground Surveillance," <http://www.nato.int/issues/ags/index.html>.
31. *Ibid.*
32. John Kriendler, *NATO Intelligence and Early Warning* (Watchfield, UK: Defence Academy of the United Kingdom, Conflict Studies Research Centre, 2006), 5-6.

33. Ibid., 4.

34. Klaus Becher, "European Intelligence Policy: Political and Military Requirements," in *Towards a European Intelligence Policy*, Chaillot Paper no. 34 (Paris: Western European Union Institute for Security Studies, 1998), 52.

35. Ibid., 53.

36. Tom Kington, "USAF Global Hawks to Patrol Europe, Africa from 2011," *Defense News*, 25 January 2010.

37. Deborah G. Barger, *Toward a Revolution in Intelligence Affairs*, RAND Technical Report (Santa Monica, CA: National Security Research Division, 2005).

38. Headquarters USAF, ISR Directorate, "US-UK RC-135V/W Rivet Joint Cooperative Program" (briefing, Washington, DC, 2009), slides 5–6.

39. Ibid., slides 9, 17.

40. Aeronautical Systems Center, "Rivet Joint 101" (briefing, Wright Patterson AFB, OH, 21 July 2009), slide 9.

41. Luftwaffe, "Vorstellung des Ersten Euro Hawk," 8 October 2009, <http://www.luftwaffe.de>.

42. Ibid.

43. Luftwaffe, "Mit Adleraugen," 24 November 2005, <http://www.luftwaffe.de>.

44. J. Lok Joris, "Global Hawk Demonstration Success Takes ISR Procurement One Step Closer," *Jane's International Defence Review* 37, nos. 1–3 (January–March 2004): 58–62.

45. Ibid.

Abbreviations

AGS	alliance ground surveillance
AOR	area of responsibility
ATO	air tasking order
CJCS	chairman of the Joint Chiefs of Staff
COCOM	combatant commander
DCGS	distributed common ground station
DCS	direct commercial sale
DNI	director of national intelligence
DOD	Department of Defense
EGSS	ELINT Ground Support Station
ELINT	electronics intelligence
FMS	foreign military sales
FOC	full operational capability
FY	fiscal year
GAF	German Air Force
IC	intelligence community
IPT	integrated process team
IS	Intelligence Squadron
ISR	intelligence, surveillance, and reconnaissance
JFCC	joint functional component command
LD/HD	low density and high demand
MP-RTIP	multiplatform radar technology insertion program
NATO	North Atlantic Treaty Organization
NIS	<i>National Intelligence Strategy</i>
NIWS	NATO intelligence warning system
NSS	<i>National Security Strategy</i>
OCO	overseas contingency operations
QDR	<i>Quadrennial Defense Review</i>
RAF	Royal Air Force
RPA	remotely piloted aircraft
SCS	<i>Security Cooperation Strategy</i>
SecDef	secretary of defense
SIGINT	signals intelligence
TPED	tasking, production, exploitation, and dissemination
TTP	tactics, techniques, and procedures
UAS	unmanned aircraft system
USAFE	United States Air Forces in Europe
USCENTCOM	United States Central Command
USEUCOM	United States European Command
WMD	weapon of mass destruction

Influence Operations and the Internet: A 21st Century Issue

Legal, Doctrinal, and Policy Challenges in the Cyber World

*Col Rebecca A. Keller, USAF**

The conduct of information operations (IO) by the US military, which includes military deception (MILDEC) and psychological operations (PSYOP), is based on doctrinal precedence and operational necessity. The increasing use of cybertechnology and the Internet in executing IO missions offers technological advantages while simultaneously being a minefield fraught with legal and cultural challenges. Using Joint and Air Force doctrinal publications, published books, and academic papers, this thesis defines relevant terminology and identifies current operational and legal constraints in the execution of IO using cybertechnology. It concludes with recommended remediation actions to enhance the use of the Internet as a military IO tool in today's cyber world.

Primer on Influence Operations

According to Joint Publication (JP) 3-13, *Information Operations*, IO is "integral to the successful execution of military operations. A key goal of IO is to achieve and maintain information superiority for the US and its allies . . . [in order] to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own."¹ Two of the five core capabilities of IO are PSYOP and MILDEC, while Public Affairs (PA) is considered an *IO-related capability*.² All three are inherent in the conduct of military operations from peacetime to wartime and are increasingly affected by cyber-technology. In order to understand these missions, it is important to first explain their definitions and functions.

According to JP 3-13.4, *Military Deception*, short of perfidy, the intent of MILDEC is the execution of actions "to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations."³ Deception has been a recognized component

*Lt Col Michael Masterson, USAF, was the essay advisor for this paper.

of war for millennia; nearly 2,500 years ago, Chinese military strategist Sun Tzu stated “all warfare is based on deception.”⁴ In modern times, two classic examples of military deception are (1) Operation Mincemeat, the World War II deception strategy that convinced the Germans that the Allies were preparing to invade Greece instead of Italy, and (2) a perfectly executed ruse by the Egyptians and Syrians giving the appearance of a military exercise. Instead, they initiated the 1973 Arab-Israeli War, catching the Israelis completely off guard.⁵

While MILDEC is customarily a wartime mission, PSYOP is conducted during all phases of military operations, including peacetime, and is authorized under Title 10, section 167 of the *US Code*, which allows the Department of Defense (DOD) to conduct PSYOP as part of special operations campaigns.⁶ JP 3-13.2, *Psychological Operations*, states the purpose of PSYOP is to influence foreign audience perceptions and behavior as part of approved programs supporting US policy and military objectives.⁷ Since World War I, the United States has released psychological leaflets across enemy lines to persuade and influence behavior. Other traditional forms of PSYOP include ground-based and airborne loudspeaker or radio broadcasts to foreign audiences and show-of-force missions where military ground personnel, aircraft, or ships visibly remind foreign nations of US combat capabilities.

Propaganda is “a form of communication aimed at influencing the attitude of a community toward some cause or position.”⁸ While historically not a pejorative term, the terms *PSYOP* and *propaganda* are often freely interchanged and have taken primarily derogatory connotations. This is in spite of the fact that both provide important national security tools and are truthful in content during the execution of conventional military operations.

Where PSYOP and propaganda are communications directed at foreign audiences, military PA offices provide similar information to journalists and the American public to articulate DOD positions on policies and operations. The same principles based upon the freedom of the press that guide civilian journalists also guide the activities of PA professionals. Military PA responsibilities are captured in JP 3-61, *Public Affairs*—“providing truthful, accurate and timely information . . . to keep the public informed about the military’s missions and operations, countering adversary propaganda, deterring adversary actions, and maintain[ing] trust and confidence of the US population, and our friends and allies.”⁹ Even Pres. Abraham Lincoln understood the importance of interacting with the public, stating, “Public opinion is everything. With it, nothing can fail. Without it, nothing can succeed.”¹⁰

The requirement to influence foreign attitudes and behaviors is not unique to the DOD; the Department of State’s (DOS) public diplo-

macy efforts can often overlap with military PSYOP or PA activities. Out of necessity, DOS public diplomacy and military PA distance themselves from the highly controversial MILDEC, PSYOP, and propaganda mission sets in order to maintain a sense of credibility and operational effectiveness which is "predicated on [the] ability to project truthful information to a variety of audiences."¹¹

Impact of Cybertechnology on Influence Operations

Increasingly, the use of the cyber domain is being actively researched and exploited by the United States and its adversaries to conduct influence operations via cell phone, e-mail, text message, and blogs in both peacetime and combat environments. The cyber world will progressively become both a boon and a bane to IO personnel, allowing a global audience reach but providing a large vulnerability to enemy deception and PSYOP efforts requiring a near immediate response to worldwide operational events.

While traditional forms of MILDEC—operational feints, displays, or instances of camouflage and concealment—are increasingly negated by advancements in intelligence, surveillance, and reconnaissance technology that quickly uncover the deception, cybertechnology has brought a new generation of MILDEC options to military planners.¹² These include digital imagery manipulation, computer file alteration, and false file storage where phony or deceptive electronic files are deliberately made accessible to an adversary.

Ubiquitous Internet availability and the global use of cell phones present new opportunities for PSYOP efforts. The proliferation of cell phone ring tones offers options for embarrassment or message delivery.¹³ For instance, altering a terrorist cell chief or military leader's ring tone to the refrain "God bless the USA" would cause embarrassment or shame when triggered to ring within earshot of subordinates or superiors. Additionally, some cell phone frequencies are "not detectable to people over the age of 30, while those younger than 30 can hear the frequency," which enables a targeted audience for some messages.¹⁴ Student revolutionaries in an adversary's country could be targeted to encourage their antiestablishment activities. In theory, the student could be alerted to a new text message or voice mail with a high-frequency alert tone audible to them without tipping off older, anti-American parents, teachers, or government officials.

The traditional airborne psychological leaflet has been modernized by an Internet version called an "E-flet," and the loudspeaker is being superseded by text messages delivered to cell phones and called the

"silent loudspeaker."¹⁵ Messages can even be sent to specific cell phone towers in a given geographic area, thus enabling regular news updates to a target audience to be sent.¹⁶ Again, the student protestors in an adversary's country could be targeted to receive text messages supporting their activities.

Web sites like *YouTube* and other social networking sites have become a battleground for "a global audience to share firsthand reports, military strategies, propaganda videos, and personal conflict as it unfolds."¹⁷ This public participation in conflict blurs the lines between combatant and noncombatant when operational data is involved. New counterpropaganda tools aided by the Internet combat this trend.

One method to fight foreign propaganda and lies is for the United States to use a blog or Web site in native languages to educate foreign citizens on political issues and to influence attitudes and advance education on a topic area. For example, if a country holds a constitutional referendum to do away with presidential term limits and the incumbent president is not a US ally, the United States could use the Internet to educate the citizens about the significance and impact of the referendum prior to the vote. Another example is "alert" software, such as "Megaphone," that notifies a special interest group about chat rooms or Internet polls that are counter to their special interest. This alert enables a counterpropaganda response and offers alternate or contradictory views.¹⁸

The importance of proactively capitalizing on the new range of cyber tools in performing IO missions is surpassed only by the requirement to identify and provide a defense against similar efforts by opponents.

Challenges to Effective Information Operations

While the lanes in the road between MILDEC, PSYOP, and PA seem clear cut in doctrine and theory, cyber operations have blurred the lines between operational missions and authorities due to outdated US laws, Internet technology, global media, and transnational threats. Seven challenges highlight conflicts and uncharted cyber areas in IO that must be addressed if the United States' national defense is not to be left vulnerable, both legally and defensively. If these areas are not addressed, the United States risks not only the ability to conduct effective cyber-related influence operations but also the capability to effectively employ military instruments of power throughout the range of operations from peacetime to wartime and defend against the same.

Keeping the American Public Informed

The American public plays a large role, both directly and indirectly, in the arena of influence operations. Doctrinally, "MILDEC operations must not intentionally target or mislead the US public, the US Congress, or the US news media."¹⁹ This insulation of the US public from US deception operations is understandable; however, it also leaves the United States vulnerable to foreign deception and propaganda efforts and "a questioning mind is the first line of defense."²⁰ Therefore, the general public should be taught how to identify and respond to propaganda, PSYOP, and deception operations launched by any foreign nation or other entity.

In the 2006 war between Israel and Hezbollah, Israel launched an airstrike on 30 July 2006 that allegedly killed as many as 57 civilians. It was later called the Qana massacre in the significant international media coverage.²¹ Ultimately, in light of postbattle assessment, the Qana massacre was determined to actually be "a stage-managed Hezbollah production, designed precisely to enflame international sentiment against Israel and compel the Israelis to accept a ceasefire that would enable the jihad terrorist group to gain some time to recover from the Israeli attacks."²² The Hezbollah manipulated the attack timeline and doctored photos of recovery workers and corpses to make the air strike appear genocidal and to cover up the military nature of the target. The inconsistencies in the images and the timeline of events were evident upon close scrutiny. Awareness of this type of deception must be developed in the American public and military personnel.

Legal Challenges to Combatant Command Responsibilities

In June 2007, the deputy secretary of defense (DEPSECDEF) issued a "Policy for Department of Defense (DOD) Interactive Internet Activities" memo authorizing the geographic combatant commands to provide information to foreign audiences via two-way communications—e-mail, blogs, chat rooms, and Internet bulletin boards.²³ A "Policy for Combatant Command (COCOM) Regional Websites Tailored to Foreign Audiences" followed in August 2007, which further authorized geographic COCOMs to produce and maintain "regionally-oriented websites" with "non-interactive" content for foreign audiences.²⁴ By direction, the Web site data must be accurate, truthful, and, in all but cases of operational necessity, attributable. On the surface, it makes sense for a COCOM to use interactive Internet activities (IIA) and regionally focused Web sites to counter extremist activity and thwart proterrorist mind-sets as well as to advance US

political-military interests overseas. However, IIA as defined and structured is the legal responsibility of the DOS and not the DOD.²⁵

The legal crux of the issue is whether these activities are PSYOP, which is a legally defined military mission set, or if they fall into the area of public diplomacy, which is the sole jurisdiction of the DOS.²⁶ While the DEPSECDEF policy letters did direct interagency cooperation with the DOS for international engagement, the term *PSYOP* is never used to define DOD activities. The DOD has limited congressional authority to conduct public diplomacy, and once it “no longer labels its communication measures as PSYOP, it potentially subverts its own statutory authorities to engage foreign audiences.”²⁷ At its core, IIA is public diplomacy conducted as a military mission, yet the appropriation of funds and the use of contractor support for foreign engagement via public diplomacy are more in line with congressional appropriations targeted to the DOS rather than the DOD.²⁸

Modernizing the Smith-Mundt Act

Related to the discussion of geographic COCOM and DOS responsibilities are the legal boundaries in the conduct of US propaganda instituted by the Smith-Mundt Act. Passed in 1948, the US Information and Education Exchange Act, also known as Smith-Mundt, was enacted to counter the worldwide communist propaganda being released by the Soviet Union during the Cold War era. “The Act’s principles are timeless: tell the truth; explain the motives of the United States; bolster morale and extend hope; give a true and convincing picture of American life, methods and ideals; combat misrepresentation and distortion; and aggressively interpret and support American foreign policy.”²⁹ In other words, create a forum for the international release of American news and information (propaganda) to counter the communist propaganda from the Soviet Union, which was “defaming our institutions in the eyes of the peoples of the world.”³⁰

The result was the creation of the US Information Agency (USIA), now a part of DOS, to undertake the mission. Additionally, some well-known media entities are also covered by the Smith-Mundt Act (Voice of America [VOA], Radio Free Asia and Europe, and Radio and TV Marti). A domestic dissemination clause was further strengthened by Congress in 1972 and 1985 to completely “block Americans from accessing USIA materials to the point USIA products were exempt from the Freedom of Information Act.”³¹ In essence, US citizens cannot be trusted to have access to the truthful materials promoting American ideals that are available to the rest of the world.

With the collapse of the Soviet Union and the worldwide communist threat, as well as the shrinking of the world due to the cyber age, a number of Smith-Mundt constraints have outlived their usefulness. First, the Smith-Mundt Act restrictions only cover the current DOS activities previously conducted by USIA, and not those of the entire US government. A 2006 legal review requested by the Defense Policy Analysis Office concluded that "the Act does not apply to the Defense Department."³² However, based upon implicit congressional support for the act that extends to the government, the DOD has applied the restrictions in its COCOM public outreach activities.³³

The Internet and satellite radio have also made it impossible to separate domestic from international audiences, calling into question whether it is illegal for online products supposedly covered by Smith-Mundt (a DOS or COCOM article produced for foreign consumption) to be accessible by American citizens.

Finally, the ability of the Department of Homeland Security (DHS) and US Northern Command to counter radical ideological products of terrorists, foreign and domestic, requires US truthful information developed by the DOS to be made available. For example, a Minneapolis, Minnesota, community radio station requested permission to rebroadcast a VOA news show that targeted Somalians. The intent was to "offer an informative, Somali-language alternative to the terrorist propaganda that [was] streaming into Minneapolis," home of the largest Somali community in the United States.³⁴ The VOA, as regulated by the Smith-Mundt Act, denied the request. This example highlights a new strategic vulnerability, the inability to combat a transnational terrorism threat within our own borders.

Countering Adversary Influence Operations

While Smith-Mundt prohibits dissemination of US influence information to American citizens, no corresponding law prohibits foreign nations or organizations from targeting US citizens with propaganda and/or deception. The lack of public awareness of this threat and the proliferation of cheap means for global message distribution leave the US public vulnerable to influence operations (propaganda) and deception by adversaries and other nations. This can include altered imagery, intentional falsehoods, and planted rumors. Some modern examples of influence operations against the US public include the Soviet KGB spreading "bogus stories linking the United States to the creation of HIV/AIDS . . . and [accusing the United States of] employing a Korean civilian airliner as a reconnaissance aircraft over the Kamchatka peninsula. [Additionally], John Kerry appeared in an al-

tered image seated near Jane Fonda at an anti-Vietnam War rally."³⁵ In order for Americans to recognize another nation's propaganda, the American educational system should have an information literacy program to ensure that US citizens "have the ability to distinguish truth from falsehood when information is presented."³⁶

Changing Pejorative Terminology

It seems that the modern usage of the terms *propaganda* and *psychological operations* is generally viewed by Americans as pejorative in nature, in spite of the fact that conventional military IO missions are truthful and accurate. As Hubert H. Humphrey once said, "In real life, unlike in Shakespeare, the sweetness of the rose depends upon the name it bears. Things are not only what they are. They are, in very important respects, what they seem to be."³⁷

Unfortunately, the words *propaganda* and *psychological operations* have evolved in usage over the past half century to imply deceit and trickery. Thus, the harmful connotation in the minds of Congress, the American public, and even some military leaders impacts negatively on the ability of the US military to effectively conduct influence operations, even truthful ones. When discussions of DOD information operations are made public, the potentially positive effects of the operations are overshadowed by the negative association of the terms themselves. Because the derogatory connotation associated with today's IO terminology can negatively impact the conduct of the mission and the ability to communicate, a name change should be considered.

Loss of High Ground in the Information Domain

That the United States has no peer competitor in conventional war fighting is not in question. However, the use of nonconventional, asymmetric techniques, particularly those enabled by the Internet, allows nonpeer competitor nation-states and nonnation-state actors a strategic equivalence or an advantage not found in conventional settings. During past conventional conflicts, the US military PA structure could effectively manage the information released to the public by civilian combat newsmen, protecting operations and personnel. However, today's technology, such as the cell phone, enables everyone the "capability to transmit audio, video and photographs . . . [and] such contributions from the street carry their own form of psychological persuasion."³⁸ Any incident occurring in a conflict today can be reported, correctly or incorrectly, via Internet chat room, YouTube, cell phone, or text messaging—long before a "legitimate news service can adjudicate its authenticity."³⁹ A cell phone enables a

group, or even an individual, the ability to conduct unilateral psychological or deception operations against the US, negatively impacting both peacetime and wartime missions by influencing public opinion. This can put pressure on public officials and military leadership regarding conduct, expected outcomes, and even the duration of combat operations.

With the growing dependence on the use of interconnected networks to function in an e-commerce society, cyber weapons are rapidly becoming the "nuclear weapon" of the millennial age. In the past, nuclear weapons were considered the ultimate deterrent and battlefield equalizer, which prompted the creation of international controls on development and possession of such technology. Fortunately, the cost of a nuclear weapons program was prohibitive to all but a handful of sovereign nations. But cyber technology is inexpensive, easy to obtain, and ubiquitous, thus offering an asymmetric advantage to adversaries, state sponsored and otherwise, to conduct "quite literally, war on the cheap."⁴⁰ As a result, it is incumbent upon the US military IO community to develop tactics, techniques, and procedures (TTP) for using the new technologies. The military must become proficient in the identification and defeat of foreign attempts at IO and learn to release "precision guided messages . . . to target friendly or enemy soldiers with equal ease."⁴¹

Defining Neutrality in Cyber Operations

The 1907 Hague Convention requires combatant nations to recognize the rights of neutral nations and that the territory of a neutral nation is inviolable by combatant nations.⁴² The latter neutrality specification causes many questions and is ill defined relative to the realm of cyber operations. The century-old Hague Convention was written when sovereign borders and national boundaries were purely geographic in nature. It must now be reconsidered in the cyber age.

Specifically, the Hague Convention states that, "belligerents may not move forces, weapons, or war materiel across a neutral country's territory, or conduct hostilities within a neutral's territory, waters, or airspace. A neutral nation jeopardizes its status if it permits belligerents to engage in such violations."⁴³ Two primary Internet-based examples highlight the difficulty of applying international laws of neutrality as they pertain to cyber operations—the use of a neutral country's cyber infrastructure and execution of cyber missions that cross neutral borders.

During the 2006 Israeli-Hezbollah conflict, Israel bombed the Al-Manar facilities in Lebanon prompting Al-Manar (an organization

outlawed in the United States due to its jihadist activities) to rehost its operations on an Austin, Texas-based server owned by Broadwing Communications.⁴⁴ The nature and intent of this rehosting were apparently unknown to Broadwing at the time. It could be argued that Hezbollah is not a sovereign state and the Al-Manar jihadist organization is not a legal combatant, so the Hague and Geneva neutrality conventions were not in play. However, this scenario and similar others demand some very intricate legal discussion on neutrality when cyber conflict occurs between nation-states and nonnation-states, especially the legal and practical consequences of a belligerent "occupying" a neutral nation's cyber infrastructure.

Another example of Internet rehosting by a belligerent took place in July 2008 in the cyber portion of the conflict between Russia and Georgia. When the Georgian government's Internet capabilities were rendered virtually nonfunctional by a Russian denial of service attack, Tulip Systems, a US Internet hosting company in Atlanta, "contacted [the] Georgian government officials and offered assistance in reconstituting Georgian Internet capabilities."⁴⁵ While Tulip Systems provided this assistance without the knowledge or permission of the US government, it calls into question the status of US neutrality during the cyber conflict between these two belligerents. Can a sovereign nation lose its neutral status based upon the unilateral actions of a single citizen?

Another gray area in the realm of cyber neutrality deals with influence operations and the release of E-flets, text messages, or deception efforts (such as altering the contents of a Web site) that involve crossing sovereign borders with respect to physical infrastructure. Similar to the conventions limiting belligerents' use of radio towers and broadcast equipment in neutral countries, does the execution of a cyber mission traveling across a neutral country's web infrastructure violate international neutrality laws? The neutrality laws must be modernized or the negative impact to the DOD is obvious.

Recommended Changes to Doctrine and Policy

The breadth of questions raised by the use of cybertechnology in the prosecution of influence operations requires further investigation and correction. To deal with the challenges discussed in the previous section, the following represent some suggested remediation efforts.

As a public service, DHS needs to develop and implement an IO education campaign to develop critical thinking skills to assist the American public in identifying foreign propaganda and deception encountered on the Internet and in cyber media. Additionally, busi-

ness owners of Internet servers would receive education on how their actions in hosting or assisting corporations or nations in countries under cyber attack could put the United States in jeopardy of losing its neutral status and unintentionally becoming a warring party within a conflict.

The DOD must determine whether new legal authorities to undertake Internet-based communications and Web site interactions with foreign audiences are required, as directed by secretary of defense policy letters of 2007. Regardless, the DOD must inform Congress of its public diplomacy (vice PSYOP) efforts and may even need to leave public diplomacy responsibilities to the DOS.⁴⁶

"Congress must undo changes to the Smith-Mundt Act that prevent accountability and effective global engagement. This language, inserted in the 1970's and 1980's, prevents transparency and awareness while ignoring the global movement of information and people."⁴⁷ Congress must amend Smith-Mundt to remove the ban on domestic dissemination of materials originally developed for foreign audiences. "In this age of communication without borders, the existence of such statutory language only subverts America's most powerful tool of soft power: our ideals."⁴⁸

Change the terms *propaganda* and *PSYOP* to something less pejorative to the American public. Hubert H. Humphrey once stated, "Propaganda, to be effective, must be believed. To be believed, it must be credible. To be credible, it must be true."⁴⁹ Given that IO and PA activities in conventional military operations are factual and truthful, the pejorative terms in use hinder the accomplishment of the mission. New terminology could be as simple as *operational communications*, *strategic effects*, *broadcast operations*, or *CYOP* (cyber psychological operations).⁵⁰

Update US influence operations doctrine to include cybertechnology. Specifically, develop TTPs for employing PSYOP, MILDEC, and PA using the new cybertechnology. Once developed, the TTPs must be incorporated into all applicable military exercises to allow the military IO operator an avenue for developing proficiency in the release of "precision-guided messages" to foreign audiences.⁵¹

Codify a US cyber policy on cyber neutrality that includes belligerent and neutral nation responsibilities. Since international law is often derived from common practice, the United States can be in the forefront of shaping international cyber neutrality laws and sovereign nation responsibilities when a "belligerent takes cyber refuge in a neutral country's territory."⁵² Ultimately, this requires a worldwide collaborative effort to "create a single set of cyber laws and procedures internationally in order to insure that there is no safe harbor

for cyber criminals.”⁵³ Cyber criminals would include state and non-state actors threatening our security.

Putting It All Together—Operational Examples

Assuming all of the previous challenges are addressed and resolved, the following example summarizes how the military commander can benefit from information operations in the cyber age. The examples use radical Islamic extremists as the notional enemy.

As radical Islam extremists expertly use the Internet and global media to publicize and advance their propaganda and lies, an educated American civilian and military population can recognize misinformation and deception using critical thinking skills, asking hard questions, and seeking alternate or corroborating sources of information before making judgments or believing the foreign stories. With a Smith-Mundt Act modification, DHS, in conjunction with the Northern Command, can provide a direct counterinformation campaign within US borders via the Internet, radio, and television (in English and other foreign languages). This campaign will reduce the domestic threat from misinformed potential terrorist recruits living in the United States.

Once cyber TTPs are codified and a well trained cadre of military professionals developed, the combatant commander will be able to informationally bombard Islamic terrorists and their potential supporters by sending precision-guided messages to specific cell towers, cell phones, e-mail, or Web sites as part of a public diplomacy or CYOP effort.⁵⁴ The ability to incorporate these tools as standard procedures will enhance a counterinsurgency campaign by actively persuading less radical terrorists and sympathizers to give up the fight without resorting to expensive (both monetarily and socially) conventional warfare.

Once international norms are established for cyber-based laws of armed conflict, commanders will better understand legal boundaries to recognizing, initiating, and defending against cyber warfare. This, in turn, leaves a training and education task for both the military professionals and the American information technology public. But, until those norms are codified, the United States is at risk of unintentionally becoming a belligerent in other countries' conflicts, having our military and civilian cyber professionals unwittingly held liable under the international court of justice or not recognizing that a cyber war attack has taken place against our nation, thus forfeiting our opportunity for a prompt and appropriate response.

Conclusion

The remediation actions and operational examples outlined in this thesis are not exhaustive and still leave a large gray area in the realm of influence operations and the use of cyber technology. They do represent a start, however, in identifying doctrinal gaps, outdated legal roadblocks, and deficiencies in policies, laws, and education. The United States must "amend existing policies to allow [influence operations] to embrace the range of contemporary media . . . as an integral asset" to military operations.⁵⁵ These changes would provide structure to largely disorganized and unnecessarily constrained efforts to fully employ cyber technology and provide a new opportunity for the United States to conduct effective and efficient influence operations using that technology. Without addressing these challenges promptly, the national security of our nation is at risk in current and future conflicts.

Notes

1. JP 3-13, *Information Operations*, 13 February 2006, I-1.
2. Ibid., II-8-9.
3. JP 3-13.4, *Military Deception*, 13 July 2006, vii. *Perfidy* is "the use of unlawful or prohibited deceptions. Acts of perfidy are deceptions designed to invite the confidence of the enemy leading to the belief that he/she is entitled to, or is obliged to accord, protected status under the law of armed conflict, with the intent to betray that confidence. Acts of perfidy include but are not limited to: feigning surrender or waving a white flag to lure the enemy into a trap; misusing protective signs, signals, and symbols to injure, kill, or capture the enemy; using an ambulance or medical aircraft marked with the red cross or red crescent to carry armed combatants, weapons, or ammunition in order to attack or elude enemy forces; and using false, deceptive, or neutral flags, insignia, or uniforms [in actual combat]." Ibid., I-8.
4. Sun Tzu, *The Art of War*, ed. and trans. Samuel Griffith (London: Oxford University Press, 1963), 66.
5. JP 3-13.4, *Military Deception*, I-7. A *ruse* is "a cunning trick designed to deceive the adversary to obtain friendly advantage. It is characterized by deliberately exposing false or confusing information for collection and interpretation by the adversary." Ibid., I-7.
6. Daniel Silverberg and Joseph Helmann, "An Ever-Expanding War: Legal Aspects of Online Strategic Communication," *Parameters*, Summer 2009, 80.
7. JP 3-13.2, *Psychological Operations*, 7 January 2010, vii.
8. Wikipedia, s.v. "Propaganda," <http://en.wikipedia.org/wiki/Propaganda> (accessed 25 January 2010).
9. JP 3-61, *Public Affairs*, 9 May 2006, xi.
10. Ibid., II-1.
11. Air Force Doctrine Document (AFDD) 2-5, *Information Operations*, 11 January 2005, 5.
12. JP 3-13.4, *Military Deception*, I-7. A *feint* is "an offensive action involving contact with the adversary conducted for the purpose of deceiving the adversary of the location and/or time of the actual main offensive action." *Displays* are "the simulation,

disguising, and/or portrayal of friendly objects, units, or capabilities in the projection of the military deception story. Such capabilities may not exist but are made to appear so (simulations)." Ibid., 1-7.

13. Timothy L. Thomas, "Hezbollah, Israel, and Cyber Psyop," *IO Sphere*, Winter 2007, 31.

14. Ibid.

15. Ibid.

16. Ibid., 32.

17. Ibid.

18. Ibid.

19. JP 3-13.4, *Military Deception*, II-8.

20. Scot Macdonald, *Propaganda and Information Warfare in the Twenty-First Century: Altered Images and Deception Operations* (New York: Routledge, 2007), 178.

21. Robert Spencer, "Stage-Managed Massacre," *Frontpagemag.com*, 2 August 2006, <http://97.74.65.51/readArticle.aspx?ARTID=3281> (accessed 13 February 2010).

22. Ibid.

23. Gordon England, deputy secretary of defense, "Policy for Department of Defense (DOD) Interactive Internet Activities," policy memorandum, 8 June 2007.

24. Gordon England, deputy secretary of defense, "Policy for Combatant Command (COCOM) Regional Websites Tailored to Foreign Audiences," policy memorandum, 3 August 2007.

25. Silverberg and Heimann, "Ever-Expanding War."

26. Ibid., 78.

27. Ibid.

28. Ibid.

29. Matt Armstrong, "Smith-Mundt Act," *Small Wars Journal*, 28 July 2008.

30. Ibid.

31. Ibid.

32. Ibid.

33. Ibid.

34. Matt Armstrong, "Censoring the Voice of America," *Foreign Policy*, 6 August 2009.

35. Macdonald, *Propaganda and Information Warfare*, 182.

36. Ibid.

37. Hubert H. Humphrey, *Quoteopia.com*, <http://www.quoteopia.com/famous.php?quotesby=huberthumphrey> (accessed 13 February 2010).

38. Thomas, "Hezbollah, Israel, and Cyber Psyop," 30.

39. Ibid.

40. Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, research publication (Colorado Springs, CO: Institute for Information Technology Applications, 1999), 10.

41. Thomas, "Hezbollah, Israel, and Cyber Psyop," 30.

42. Stephen W. Korn and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters*, Winter 2008-9, 62.

43. Ibid.

44. Thomas, "Hezbollah, Israel, and Cyber Psyop," 33.

45. Korn and Kastenberg, "Georgia's Cyber Left Hook," 67.

46. Silverberg and Heimann, "Ever-Expanding War," 90.

47. Armstrong, "Smith-Mundt Act."

48. Gregory L. Garland, "Editorials and Op-Eds," *AmericanDiplomacy.Org*, 3 January 2009, www.unc.edu/depts/diplomat/item/2009/0103/ed/garland_smithmundt.html (accessed 23 October 2009).

49. Hubert H. Humphrey, *BrainyQuote.com*, http://www.brainyquote.com/quotes/authors/h/hubert_h_humphrey_2.html (accessed 13 February 2010).
50. Thomas, "Hezbollah, Israel, and Cyber Psyop"; and AFDD 2-5: *Information Operations*, 30.
51. Thomas, "Hezbollah, Israel, and Cyber Psyop."
52. Korn and Kastenber, "Georgia's Cyber Left Hook," 66.
53. Paul Rosenzweig, "National Security Threats in Cyberspace," McCormick Foundation Conference series (Wheaton, IL: McCormick Foundation, 2009), 30.
54. Thomas, "Hezbollah, Israel, and Cyber Psyop."
55. Angela Maria Lungu, "War.com: The Internet and Psychological Operations," *Joint Forces Quarterly*, Spring/Summer 2001, 13-17.

Abbreviations

AFDD	Air Force doctrine document
COCOM	combatant command
CYOP	cyber psychological operations
DEPSECDEF	deputy secretary of defense
DHS	Department of Homeland Security
DOD	Department of Defense
DOS	Department of State
E-flet	Internet psychological leaflet
IIA	interactive Internet activities
IO	information operations
JP	joint publication
MILDEC	military deception
PA	Public Affairs
PSYOP	psychological operations
TTP	tactics, techniques, and procedures
USIA	US Information Agency
VOA	Voice of America

US National Security and Environmental Change in the Arctic

*Lt Col Lars Helmrich, Swedish Air Force**

Historically, dramatic changes in strategic geography have had a big impact on international relations, as illustrated by the discovery of America and the building of the Panama and Suez Canals. Today the warming climate is changing the strategic geography in the Arctic. The ice coverage is decreasing, which makes shipping possible and increases the possibility of extracting natural resources. Hence, the strategic importance of the Arctic is increasing.¹ This essay discusses the strategic impact of environmental change in the Arctic. The purpose is to explore how this change affects US national security and to suggest a future US policy in the region.

The existing academic analyses concerning US climate policy and Arctic policy generally propose increased international cooperation. However, the existing international framework for the Arctic is disputed and is not ratified by the United States. Moreover, the actions of countries in the Arctic suggest, contrary to their stated policies, a desire to unilaterally maximize their own economic gain. The United States does not have a well-developed Arctic policy. This essay suggests that the United States first ratify the United Nations (UN) Convention of the Law of the Sea. Then it needs to negotiate, bilaterally, agreements regarding the extent of the Arctic countries' exclusive economic zones (EEZ). To be successful, the United States should broaden these negotiations to include other areas of policy. The suggested policy does not seek to maximize the US EEZ; rather the objective is to reach a peaceful agreement with a positive effect on the world economy, while at the same time strengthening US strategic leadership.

The essay starts with a brief summary of environmental change in the Arctic and how that affects the strategic situation. Thereafter, it presents a synopsis of academic recommendations concerning US policy. This section is followed by an analysis of the current situation in the Arctic, pertaining to the status of international cooperation and the actions of involved countries. The fourth part covers US policy—what it is now and what it should be in the future.

*Dr. Christopher Hemmer, USAF civilian, was the essay advisor for this paper.

The Arctic Is Changing

Climate change in the Arctic is fundamentally altering the region's strategic importance. Increased accessibility, due to decreased ice coverage, leads to new possibilities for shipping and extraction of natural resources. For some time, the debate about whether the climate is changing has been decided. Currently, the debate concerns its implications, among which are those that affect international security. This is evident from President Obama's speech at the UN General Assembly on 23 September 2009: "The danger posed by climate change cannot be denied. Our responsibility to meet it must not be deferred. If we continue down our current course, every member of this Assembly will see irreversible changes within their borders. Our efforts to end conflicts will be eclipsed by wars over refugees and resources."²

An important actor concerning climate change is the Intergovernmental Panel on Climate Change (IPCC). It was established by the UN in 1989 to conduct an unbiased review of scientific evidence concerning climate change. The IPCC was honored with the 2007 Nobel Peace Prize. According to the IPCC, the polar regions are the areas where climate change will be most abrupt and will be experienced earliest.³ In fact, it is already occurring. The Arctic glaciers and the Greenland ice sheet are melting.⁴ According to the IPCC, by 2050 the Northern Sea Route, which passes through the Arctic close to the Russian coast, will have conditions that allow for the navigation of ice-strengthened cargo ships 125 days per year.⁵ The Northwest Passage, which passes close to Canada's northern coast, was ice free for the first time in 2007; it may shorten the journey between Europe and Asia by 2,500 miles. In the past 20 years, the ice coverage of the Arctic has decreased by an area equal to one-third of the continental United States.⁶

The decreasing ice coverage does not affect shipping routes only. The United States Geological Survey (USGS) assessed undiscovered oil and gas resources in the Arctic. It concluded that the region is the earth's largest remaining unexplored area for these resources. It is estimated that undiscovered oil and gas resources amount to 90 billion barrels of oil, 1,669 trillion cubic feet of natural gas, and 44 billion barrels of gas liquids.⁷ Compared to the total volume of estimated undiscovered energy resources, the Arctic's resources include 13 percent of the undiscovered oil and 30 percent of the undiscovered natural gas.⁸

Climate change is affecting the Arctic and shrinking the extent of the ice cap. The result is easier access to natural resources, as well

as the possibility of new, shorter sea routes. Hence, the strategic importance of the region is increasing. Additionally, the global consequences of climate change will include upward pressure on oil prices caused by instability in oil-producing regions.⁹ This development will further increase the importance of the region. The next section examines the broad trends of analysis about possible US policy on climate change and on the Arctic.

Existing Academic Recommendations concerning Strategies in the Arctic

Numerous organizations study climate change and its implications for international security. There is a general agreement that the challenges created by climate change, due to its global nature, should result in increased international cooperation.¹⁰ Even studies conducted at military academic institutions generally favor multinational cooperation.¹¹

In 2007 the CNA Corporation published the study *National Security and the Threat of Climate Change*. The study suggests that the main threats to international stability are increasing difficulties for failing states, mass migration, and conflicts concerning resources. Climate change will reinforce these threats.¹² The study recommends that the United States integrate the consequences of climate change in its national defense strategy, make a stronger commitment to stabilize climate change, commit to a global partnership to assist less-developed nations, improve energy (fuel) efficiency in its combat forces, and assess the impact on US military installations globally.¹³ The study argues that ongoing climate change is most significant in the Arctic. The decreasing amount of ice could bring more competition for resources as well as more commercial and military activity.¹⁴ The CNA study recognizes that projected climate change is a serious threat to US national security. It states that more international cooperation is needed to address the challenge.¹⁵

The Center for a New American Security (CNAS) performed an in-depth analysis of the implications climate change may have for national security. The analysis argues that climate change will aggravate existing international tensions.¹⁶ It also states that, if not addressed, the effects of climate change may come to represent the greatest challenge to US national security.¹⁷ Three different scenarios are studied: expected, severe, and catastrophic climate change.¹⁸ The study concludes by presenting 10 security implications of climate change, including north-south tensions, migration challenges, resource conflicts, challenges to global governance, China's role, and

the unpredictability in balance of power shifts.¹⁹ The policy recommendations for the United States are very vague. The CNAS argues for international cooperation, especially among the United States, China, and Europe, and stresses the importance of US leadership.²⁰ Concerning the Arctic, the report states that for the first time in recorded history, the Northwest Passage has become navigable and that the decrease in the Arctic ice cap is likely to continue.²¹

The Carnegie Endowment for International Peace, in its report *The Arctic Climate Change and Security Policy Conference*, stresses that the implications for US security interests as a result of climate change in the Arctic are profound. Its advice to the United States is to ratify the UN Convention of the Law of the Sea, promote a stronger role for the Arctic Council, and support Arctic subregional forums. According to the report, the key security issue in the Arctic is environmental security. The Carnegie Endowment for International Peace concludes that there are no significant geopolitical fault lines and no imminent reasons to expect wars because of natural resources.²²

Existing academic analyses are generally favorable to increased international cooperation. They do not address how to handle increased competition of resources other than stating the need for increased international cooperation. There is a common academic appreciation of the challenge, but when studying the Arctic, it is obvious that the foundation for international cooperation is fragile and that the main actors are not acting in accordance with the recommendations.

Recent Strategic Development in the Arctic

The actors in the Arctic consist of international agreements/institutions and states. Those discussed here are the UN Convention of the Law of the Sea (UNCLOS), the Arctic Council, the International Maritime Organization (IMO), the Seabed Arms Control Treaty, and the Arctic countries. For brevity's sake, this essay will analyze only the Arctic countries of Russia, Canada, Denmark, Norway, and the United States. Based upon tradition and geography, I deem these countries most important. The United States is discussed in a separate section.

International Agreements/Institutions

The UNCLOS was established on 10 December 1982 after 14 years of work involving more than 150 countries. It entered into force on 16 November 1994. The UNCLOS establishes rules concerning use of the oceans and extraction of their resources, as well as serving as a legal

framework for dispute resolution. The UNCLOS defines a state's EEZ, in which it has the sovereign right to extract natural resources, as an area within 200 nautical miles (nm) of its baseline.²³ This sovereign right may extend to 350 nm if the state's continental shelf extends beyond the 200 nm limit. The Commission on the Limits of the Continental Shelf (CLCS), established under the convention, makes recommendations concerning the extent of different states' continental shelves. To support a claim concerning its continental shelf, each nation is obliged to submit scientific evidence to the commission. Disputes regarding the right to resources can be submitted to the International Tribunal for the Law of the Sea, also established under the convention.

Of the Arctic countries, the United States is the only one that has not ratified the UNCLOS.²⁴ Several countries, though, have declared that they do not recognize the UNCLOS's right of binding decisions or have declared other exceptions. Russia, for example, does not accept the UNCLOS's procedures for binding decisions or dispute resolution concerning the exercise of sovereign rights. Canada reserves the right to take any position on any declaration by the UNCLOS that it deems appropriate. Both Norway and Denmark have made reservations concerning dispute resolution.²⁵ Although the UNCLOS is the critical framework in the Arctic, other relevant treaties and organizations exist.

The main purpose of the Arctic Council is to maintain peace and stability in the Arctic. The council was established in 1996, and today all of the Arctic countries are members. Besides nations, several organizations of indigenous Arctic populations are included as permanent participants in the council. The Arctic Council does not handle matters associated with military security. Instead, it contributes to peace and stability by addressing issues such as living conditions, sustainable development, and environmental protection. However, according to its chairman Lars Møller, the Arctic Council together with the UNCLOS can be viewed as the main framework within which security-related issues can be dealt with.²⁶

The International Maritime Organization, founded in 1958, is a UN organization concerned with maritime safety and cooperation. It is based in Great Britain and has 169 member nations. The safety issues encompass shipping as well as environmental safety.²⁷ The Seabed Arms Control Treaty of 1971 is a multinational agreement among 84 countries banning the placement of weapons of mass destruction on the ocean floor, beyond the 12-mile territorial zone.²⁸

With the exception of the Seabed Arms Control Treaty, the international framework in the Arctic does not consider those issues that

are strictly security related. A different international framework has developed for the Antarctic. The Antarctic Treaty was signed in 1959; among other things, it states that Antarctica is to be used only for peaceful purposes. It also allows for inspections of other nations' bases/stations on the continent. However, there are still unresolved overlapping territorial claims even in Antarctica.²⁹ There is an important difference between the Arctic and Antarctic and every other area on land or above the continental shelf. There is no history in the Arctic or Antarctic of territorial sovereignty; hence there exists no customary law of economic rights. At the same time, because several countries have declared they do not recognize the UNCLOS's right of binding decisions, the significance of the existing international framework is unclear.

State Behavior

Since the end of the Cold War, the Arctic has been somewhat disconnected from power politics. There are, however, certain indications that this is about to change.³⁰ Oil companies from several nations are extending their offshore fields farther north. The possibility of increased shipping has led to disputes between Canada and Denmark about Hans Island, located at the entrance of the Northwest Passage. Both countries, and Russia, have sent warships to the region to emphasize their interests.³¹ Additionally, several countries have made overlapping claims to parts of the Arctic.³²

In August 2007 a Russian adventurer placed a Russian flag on the ocean floor, 4,300 meters below the North Pole. By doing so, he claimed 1.2 million square kilometers of the Arctic for Russia.³³ Russia first made a claim to the UNCLOS about this territory in 2001. Russia argued that its continental shelf, and hence its EEZ, extended far beyond 200 nm. Because of lack of evidence, Russia's claim was turned down. However, both the expedition of 2007 and others were intended to document new evidence to support its claim.³⁴ Russia's security interests are in part military, since its nuclear submarine fleet is based at the Kola Peninsula.³⁵ Although the Russian Navy has downsized, the Northern Fleet is still vital to Russia's military strategy. It operates Russia's single aircraft carrier as well as the nuclear-powered missile submarines that are the backbone of Russia's strategic naval nuclear force.³⁶

A new Russian strategy for the Arctic was signed on 18 September 2008 by Pres. Dmitry Medvedev. Russia aims to maintain its leading position as an Arctic power and over time to transform the Arctic into its main resource base. This is a natural consequence of the Russian

argument that a large part of the Arctic seabed is an extension of the Siberian continental shelf. Russia is economically dependent on exports of oil, gas, and metals. The area's significance to Russia is apparent by the estimation that the amount of oil in the Arctic equals Russia's total known reserves.³⁷ The definition of Russia's continental shelf therefore becomes an important issue. Russia plans to develop military units capable of protecting its security interests in the region, among which are control of natural resources and increased control of a shipping route—the Northern Sea Route. Russia's strategy also states that competition about natural resources in the Arctic may result in military conflict.³⁸ However, Russian officials refer to the Arctic as a zone of peace.³⁹

Canada also appears to be building up its military capabilities in the region. A key issue for Canada is whether the Northwest Passage is in Canadian or international waters. Canada has made vessel notification in the Northwest Passage mandatory.⁴⁰ It appears that Canada is focusing on the Arctic's military strategic importance. During the Cold War, the United States contributed the bulk of military forces while Canada minimized its military presence. After the Cold War, Canada further reduced its military activity in the Arctic. Then in 1999 Canada created the Arctic Security Interdepartmental Working Group to coordinate the nation's security policy in the Arctic. Canada has acknowledged that the region has large amounts of natural resources as well as a fragile ecosystem. Canada's 2000 *Arctic Capabilities Study* is based on the assumption that the strategic situation in the Arctic is changing. The study made some recommendations to Canada's Department of National Defence, including the following: increase interdepartmental cooperation, increase Ranger capabilities, implement new exercises for the Canadian Forces, include the Arctic dimension in future Canadian Forces planning, and improve surveillance of the region. In 2002 the Canadian Forces conducted their first joint exercise in the Arctic in over 20 years, which has been followed by additional exercises.⁴¹

In 2005 Canada issued *Canada's International Policy Statement*. It elaborates the need for Canada to monitor and control events in its northern region and stresses the increasing demands on sovereignty as activities in the Arctic increase. As a consequence, the Canadian Forces need to increase their presence and capabilities in the region.⁴² This issue is addressed in Canada's current defense strategy, *Canada First*. It includes modernization of its military forces, Arctic patrol ships, destroyers, frigates, and maritime patrol aircraft, providing all with increased Arctic climate capabilities. Improved surveillance capability of the region is also being studied.⁴³ The defense

strategy should be considered together with Canada's Northern Strategy, released in the summer of 2009 by the minister of foreign affairs, Mr. Lawrence Cannon. The strategy acknowledges the need for international cooperation, but at the same time it states that the Arctic is a priority for Canada and that it intends to be the international leader in the region. The strategy expresses a commitment to protect and patrol the region. One Canadian goal is, through the UNCLOS, to obtain recognition of the extent of Canada's continental shelf beyond 200 nm.⁴⁴ An example of Canadian resolve is the previously mentioned dispute with Denmark about Hans Island. In 2005 Canada's defence minister visited the small uninhabited island, where Canadian troops erected a Canadian flag. Hans Island is claimed by both countries.⁴⁵

Both Denmark and Norway acknowledge the need for international cooperation in the Arctic. However, a study of their actions in the area shows that both countries are concerned with securing access to natural resources. Denmark's position is unique because of Greenland. Following the Russian expedition of 2007, Denmark launched its own expedition with the objective of establishing the extent of Greenland's continental shelf.⁴⁶ Norway's 2007 *Strategy of the High North* states that the Arctic is Norway's most strategically important area and that it will intensify its efforts to exercise Norwegian sovereignty. The area's importance is due to resources—fishing and energy. A focal point in the strategy is the islands of Svalbard and Spitsbergen. Further, the strategy discusses Norway's claims concerning the extent of its continental shelf. Norway appears to have identified Russia as its main counterpart in the region. The strategy praises cooperation with Russia, while it also expresses concerns over Russia's development. The presence of military combat forces, which provide the ability to exercise sovereignty and authority, is a vital part of Norway's strategy. However, the primary tasks for the armed forces in this region are surveillance and intelligence gathering, which are mainly done by Coast Guard assets and maritime patrol aircraft.⁴⁷ The status of the Svalbard archipelago is disputed. Norway claims exclusive rights to its resources through the Svalbard Treaty of 1920. Other states have expressed reservations about Norway's claim. The situation is complicated by the Svalbard and the Spitsbergen treaties as well as the UNCLOS. Occasionally, it has led to Norway's seizing of other countries' fishing vessels.⁴⁸

Territorial claims put forward to the UNCLOS contain both unclaimed areas and overlapping claims in the region.⁴⁹ The most interesting section is an almost circular area of 460,800 square miles, north of the nearest Arctic country's 200-nm zone.⁵⁰ Below this area

runs the Lomonosov Ridge. It expands 1,700 kilometers from the continental shelf of North America, over the North Pole, to the continental shelf of the New Siberian Islands.⁵¹ Hence, establishing the exact origin of the Lomonosov Ridge and the extension of the continental shelves of Canada, Russia, Norway, and Greenland becomes very important.⁵² Since the CLCS has a mandate only to review geological evidence and make recommendations, there may be counterclaims and appeals.⁵³

The lack of a security-related treaty in the Arctic is in stark contrast to the amount of security-related activities. All concerned countries stress the importance of international cooperation, but their actions imply that they do not trust the ability of international institutions/agreements to settle existing disputes. The disputes concern rights to natural resources, control of shipping routes, and, to some extent, the identity of the leading country in the region. All nations have shown resolve in protecting their interests.

So in a region that is changing and increasing in importance, there are conflicting interests, demonstrated national resolve, little historical guidance, and an impotent international framework. The framework that does exist is being used to promote national interests. Furthermore, the discussion above suggests that unfavorable recommendations by the UNCLOS and CLCS will not be easily accepted. With this conclusion in mind, the next section analyzes US Arctic policy.

US Policy concerning the Arctic

There are not many official documents concerning US Arctic policy. The 2002 and 2006 national security strategies and the 2008 national defense strategy do not include any specific US policy in the region. The White House Web site concerning foreign policy discusses a number of issues and identifies climate change as one of several distinct challenges but does not include a specific Arctic policy.⁵⁴ There exists an old presidential decision directive from 1994 (PDD-26, *US Antarctica Policy*) covering US Arctic and Antarctic policy. Then in January last year, the White House issued a new national security presidential directive (NSPD-66, *Arctic Region Policy*) concerning US Arctic strategy. The context for a new directive was, among other things, the effects of climate change and the recognition of the region's richness of resources. According to NSPD-66, US objectives in the Arctic can be simplified and summarized as intense international cooperation concerning environmental issues, freedom of the seas (for the Northwest Passage and the Northern Sea Route), and maximum extension of the US continental shelf. To attain these objectives,

ratification of the UNCLOS, as well as a significant military presence, is deemed vital. NSPD-66 supersedes PDD-26 concerning US Arctic policy, but not Antarctic policy.⁵⁵

In 2007 the Senate Foreign Relations Committee sent the UNCLOS treaty to the full Senate for ratification, where it needs a two-thirds majority for ratification. It has yet to be ratified. The main objections in the Senate are the short time frame available between ratification and the deadline for making territorial claims, an unclear dispute-resolution process, infringements on US sovereignty, and possible limitations on US military activity.⁵⁶

Not many US activities in the Arctic can be tied to an Arctic policy. Since 2006, the United States no longer has a permanent military presence in Iceland.⁵⁷ This may validate a continuing shift in military priority, from the Cold War fault lines toward the global war on terrorism and the Central Command area.

Suggestions for US Policy

In contrast to other countries, the United States does not have a highly developed Arctic policy and is not a member of the most important international institution concerning the Arctic, the UNCLOS. The directive that does exist is a legacy from former president George W. Bush.

The Arctic policy of the Obama administration should be shaped by overall US interests and the larger context for the policy. Although the new administration has yet to publish a national security strategy, US overall interests can be described as a combination of long- and short-term objectives. The long-term objectives concern the United States' role in the world and its perception in the international community. It is obvious that President Obama strives for a change in strategic leadership. The emphasis when interacting with other nations is on multilateral cooperation. The administration's preferred leadership style appears to be more persuasive than coercive and more inclusive than exclusive.⁵⁸ Therefore, US Arctic policy must be limited to actions that have legitimacy in the international community. At the same time, the security of the United States and its citizens is one of the president's main responsibilities and cannot be compromised.

The short-term objectives encompass avoiding military conflict as well as denying any other country dominance of the Arctic. From an economic perspective, US interests can be described as maximizing its access to natural resources and securing the access of new shipping routes. But solving the disputed issues may be more impor-

tant, and even more profitable, than maximizing the extent of the US continental shelf. Ensuring that available resources and shortened shipping routes benefit the world economy may be the true economic interest.

Besides considering US objectives, US Arctic policy must address recent and likely future developments in the region. A decrease in the Arctic ice cap will make new sea routes available and permit extraction of more natural resources. Since climate change is likely to increase instability in the Middle East, the strategic significance of the Arctic will grow, resulting in greater commercial as well as military activity in the region. The key strategic challenges are to settle the dispute concerning the EEZs and, to a lesser degree, the control over new shipping routes. It may be tempting to pursue a policy similar to that of other Arctic countries: to ratify the UNCLOS and then file US territorial claims. However, that would not bring the issue closer to a solution. Another possibility may be an international conference to reach an agreement concerning the continental shelf. Because of conflicting interests, this approach is unlikely to succeed. But it is possible to formulate a policy that creates synergy by combining the objective of increasing the credibility of US strategic leadership with securing economic gain and a peaceful development in the Arctic. Actually, this opportunity exists because of the conflicting national interests and the uncertain significance of the international framework. It combines multi- and bilateral initiatives within the existing international framework.

My suggestion for US Arctic policy encompasses broadening the issue to other areas and contains activities at several different levels. First, the foundation of the policy is the UNCLOS; it needs to be ratified by Congress. To convince the Senate, President Obama needs to invest political will in the issue and compromise in other areas. Next, it is highly unlikely that the concerned nations in the near future will be able to agree upon a solution about the continental shelf. Therefore, the US Geological Survey should be tasked to make an overall, and objective, recommendation about the continental shelf issue. The recommendation should be used as a starting point in bilateral negotiations with Russia, Canada, Denmark, and Norway to reach an agreement.

The United States must add other issues to the discussions, issues that may differ depending on the counterpart. Introducing the issue of control of shipping routes as well as other economic and military/security instruments of national power to the discussion can help the parties reach compromises. With Norway and Denmark, the United States could inject security and foreign military sales issues in the

discussion—for example, the condition for purchase of the joint strike fighter. In negotiations with Russia, the strategy versus Iran, cooperation in the conflict against Islamic fundamentalist groups, and NATO's missile defense system are possible issues to discuss. With Canada, control of the Northwest Passage and trade issues may be included in negotiations. The United States can then submit a final compromise multilaterally to the UNCLOS and CLCS. Additionally, a security-related treaty similar to the Antarctic Treaty should be initiated.

From a military perspective, the division of the Arctic among several combatant commanders is not preferable. The commander of the US Northern Command should be responsible for the Arctic area north of each Arctic country's 200-nm zone. Such a change would facilitate coordination of the national instruments of power. From the United States' perspective, the suggested policy would probably not maximize the extension of its continental shelf, a stated goal in NSPD-66. However, it would strengthen US strategic leadership, have a positive effect on the world economy, and promote peaceful development in the Arctic region. Hence, the suggested policy accommodates both the long- and short-term objectives concerning US interests. If the policy is wisely introduced in a strategic communications context, its outcome may be further enhanced.

Conclusion

History has shown that strategic geography influences international relations. For example, the United States has frequently used military means to demonstrate its interests in the Panama Canal, and in 1956 the Suez Canal was the scene of armed conflict involving two of the great powers: Great Britain and France. It is obvious that the European discovery of America—with the ensuing competition for America's resources and the eventual birth of a superpower—has affected great-power politics ever since. I do not suggest that these examples are perfect analogies. However, they do illustrate that important sea routes as well as disputed rights to natural resources can play an important part in international politics. A dramatic environmental change in the Arctic may cause serious competition over resources and affect international security.

The Arctic has some very specific characteristics. Most of its territory is neither a continent nor an island; hence, it does not and cannot have a tradition of ordinary human settlement. It has an inhospitable climate and was until recently extremely difficult to access. The shrinking Arctic ice cap will open new sea routes and permit increased extraction of natural resources. Therefore, the strategic sig-

nificance of the Arctic is increasing. The international framework that does exist is not sufficient. At the same time, several nations' actions imply a risk of increased tension concerning unresolved issues about the right to resources. The key strategic challenge for the United States is to settle the dispute concerning the EEZs, while at the same time protecting overall US interests. The suggested US policy would enhance its credibility as the world's strategic leader and encourage development of the world economy. Hence, it meets the nation's long- and short-term objectives.

Notes

1. I use the Arctic Council's definition of the Arctic. Countries include Canada, Iceland, Denmark/Greenland/Faroe Islands, Finland, Norway, Russia, Sweden, and the United States. Arctic Council, Protection of the Arctic Marine Environment Working Group, *Arctic Offshore Oil and Gas Guidelines 2009*, 29 April 2009, 5, <http://arctic-council.org/filearchive/Arctic%20Offshore%20Oil%20and%20Gas%20Guidelines%202009.pdf> (accessed 19 October 2009).

2. Pres. Barack Obama (speech, UN General Assembly, New York, 23 September 2009), http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-to-the-United-Nations-General-Assembly (accessed 28 September 2009).

3. Martin L. Parry et al., eds., *Climate Change 2007: Impacts, Adaptation and Vulnerability*, contribution of Working Group II to the Fourth Assessment Report of the Intergovernmental Panel on Climate Change (Cambridge, UK: Cambridge University Press, 2007).

4. *Ibid.*, 656.

5. *Ibid.*, 676.

6. Vsevolod Gunitskiy, "On Thin Ice: Water Rights and Resource Disputes in the Arctic Ocean," *Journal of International Affairs* 61, no. 2 (Spring/Summer 2008): 261-71.

7. Peter H. Stauffer, ed., "Circum-Arctic Resource Appraisal: Estimates of Undiscovered Oil and Gas North of the Arctic Circle," US Geological Survey Fact Sheet 2008-3049, 23 July 2008.

8. Zachary Colie, "Rush to Arctic as Warming Opens Oil Deposits," *San Francisco Chronicle*, 12 August 2008, <http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/08/12/MN5R1290QE.DTL> (accessed 28 September 2009).

9. Kurt M. Campbell et al., *The Age of Consequences: The Foreign Policy and National Security Implications of Global Climate Change* (Washington, DC: Center for a New American Security, November 2007), 65, <http://handle.dtic.mil/100.2/ADA473826> (accessed 28 September 2009).

10. See, as an example, Christiane Callsen, "Climate Change and Security Policy," CSS [Center for Security Studies] *Analyses in Security Policy* 2, no. 26 (December 2007): 3.

11. See, as an example, Douglas V. Johnson, II, *Global Climate Change: National Security Implications*, Colloquium Brief (Carlisle, PA: Army War College, Strategic Studies Institute, 2007), 2, <http://handle.dtic.mil/100.2/ADA466551> (accessed 28 September 2009).

12. David M. Catarious, Jr., et al., *National Security and the Threat of Climate Change* (Alexandria, VA: The CNA Corporation, 2007), 13ff., <http://securityandclimate.cna.org/report/National%20Security%20and%20the%20Threat%20of%20Climate%20Change.pdf> (accessed 28 September 2009).

13. *Ibid.*, 7–8.
14. *Ibid.*, 38.
15. *Ibid.*, 44–45.
16. Campbell et al., *Age of Consequences*, 8.
17. *Ibid.*, 10.
18. *Ibid.*, 38–39.
19. *Ibid.*, 105ff.
20. *Ibid.*, 99.
21. *Ibid.*, 5, 47.
22. Kenneth S. Yalowitz, James F. Collins, and Ross A. Virginia, *The Arctic Climate Change and Security Policy Conference: Final Report and Findings*, sponsored by Dickey Center for International Understanding at Dartmouth College, Carnegie Endowment for International Peace, and University of the Arctic Institute for Applied Circumpolar Policy, Dartmouth College, Hanover, New Hampshire, December 2008, 1–2, 17, http://www.carnegieendowment.org/files/arctic_climate_change.pdf (accessed 24 September 2009).
23. A nation's baseline is determined by UNCLOS. Normally, it is the low-water line along the coast.
24. UN, "United Nations Convention on the Law of the Sea of 10 December 1982: Overview and Full Text," http://www.un.org/Depts/los/convention_agreements/convention_overview_convention.htm (accessed 13 October 2009).
25. *Ibid.*
26. Arctic Council, "Declaration of the Establishment of the Arctic Council," <http://arctic-council.org/article/about> (accessed 19 October 2009).
27. International Maritime Organization, Web site, <http://www.imo.org> (accessed 19 October 2009).
28. "Treaty on the Prohibition of the Emplacement of Nuclear Weapons and Other Weapons of Mass Destruction on the Seabed and the Ocean Floor and in the Subsoil Thereof" (Seabed Treaty), 11 February 1971, 23 U.S.T. 701, T.I.A.S. No. 7337, <http://www.state.gov/www/global/arms/treaties/seabed1.html> (accessed 20 July 2010).
29. Secretariat of the Antarctic Treaty, "The Antarctic Treaty," http://www.ats.aq/e/ats_treaty.htm (accessed 19 October 2009).
30. Yalowitz, Collins, and Virginia, *Arctic Climate Change*, 15.
31. Doug Mellgren, "Technology, Climate Spark Race to Claim Arctic Resources," Associated Press, 24 March 2007, http://www.usatoday.com/money/world/2007-03-24-arcticbonanza_N.htm (accessed 19 October 2009).
32. Gunitskiy, "On Thin Ice."
33. Campbell et al., *Age of Consequences*, 5.
34. Oxford Analytica, "Russia's Arctic Plays Concern Region," *Forbes.com*, 12 August 2009, <http://www.forbes.com/2009/08/11/russia-energy-climate-change-business-energy-oxford.html> (accessed 19 October 2009).
35. Yalowitz, Collins, and Virginia, *Arctic Climate Change*, 15.
36. Ilya Kramnik, "Northern Fleet Protecting Russian Arctic," *Rianovosti*, 2 June 2009, <http://en.rian.ru/analysis/20090602/155147701.html> (accessed 28 September 2009).
37. Dmitry Solovyov, "Russia to Boost Arctic Troops to Defend Resources," Reuters, 27 March 2009, <http://www.reuters.com/article/environmentNews/idUSTRE52P5NS20090327> (accessed 19 October 2009).
38. Katarzyna Zysk, "Russia's National Security Strategy to 2020," Institut for forsvarsstudier, 15 June 2009, http://www.geopoliticsnorth.org/index.php?option=com_content&view=article&id=2%3A%Arussia-norway-and-the-high-north-past-present-future&catid=3%3Anewsflash&Itemid=1&limitstart=2 (accessed 26 October 2009).

39. Oxford Analytica, "Russia's Arctic Plays."
40. Yalowitz, Collins, and Virginia, *Arctic Climate Change*, 15–16.
41. Rob Huebert, "Renaissance in Canadian Arctic Security?" *Canadian Military Journal*, 14 July 2008, <http://www.journal.dnd.ca/vo6/no4/north-nord-eng.asp> (accessed 24 September 2009).
42. Ibid.
43. Department of National Defence, "Rebuilding the Canadian Forces," *Canada First Defence Strategy*, 3 April 2009, <http://www.forces.gc.ca/site/pri/first-premier/defstra/rebuild-rebatir-eng.asp> (accessed 26 October 2009).
44. Lawrence Cannon (address, Department of Foreign Affairs and International Trade Canada, Gatineau, Quebec, 26 July 2009), <http://www.international.gc.ca/media/aff/speeches-discours/2009/387436.aspx?lang=en> (accessed 26 October 2009).
45. "Charging round the Block," *Economist* 376, no. 8440 (20 August 2005): 29–30.
46. Gunitskiy, "On Thin Ice."
47. Norwegian Ministry of Foreign Affairs, *The Norwegian Government's High North Strategy*, report, 2006, <http://www.regjeringen.no/upload/UD/Vedlegg/strategien.pdf> (accessed 2 November 2009).
48. Torbjørn Pedersen, "The Dynamics of Svalbard Diplomacy," *Diplomacy and Statecraft* 19, no. 2 (June 2008): 236–37, 253.
49. Yalowitz, Collins, and Virginia, *Arctic Climate Change*, 16.
50. Gunitskiy, "On Thin Ice."
51. International Bathymetric Chart of the Arctic Ocean, "Selective Comparisons of GEBCO (1979) and IBCAO (2000) Maps," http://www.ngdc.noaa.gov/mgg/bathymetry/arctic/ibcao_gebco_comp.html (accessed 2 November 2009).
52. Colie, "Rush to Arctic."
53. Gunitskiy, "On Thin Ice."
54. Pres. Barack Obama, "Foreign Policy," White House Web site, <http://www.whitehouse.gov/issues/foreign-policy> (accessed 11 November 2009).
55. Pres. George W. Bush, National Security Presidential Directive (NSPD) 66, "Arctic Region Policy," 9 January 2009, <http://georgewbush-whitehouse.archives.gov/news/releases/2009/01/20090112-3.html> (accessed 2 November 2009).
56. Kevin Drawbaugh, "U.S. Senate Panel Backs Law of the Sea Treaty," Reuters, 31 October 2007, <http://www.reuters.com/article/idUSN31335584> (accessed 11 January 2010); and Clifford Krauss et al., "As Polar Ice Turns to Water, Dreams of Treasure Abound," *New York Times*, 10 October 2005, <http://www.nytimes.com/2005/10/10/science/10arctic.html> (accessed 11 January 2010).
57. Valur Ingimundarson, "Iceland's Post-American Security Policy, Russian Geopolitics and the Arctic Question," *RUSI Journal* 154, no. 4 (August 2009): 74.
58. This is evident from, for example, President Obama's recent speeches in Cairo and the UN and the White House Web site concerning foreign policy.

Abbreviations

CLCS	Commission on the Limits of the Continental Shelf
CNAS	Center for a New American Security
CSS	Center for Security Studies
EEZ	exclusive economic zone
IMO	International Maritime Organization
IPCC	Intergovernmental Panel on Climate Change
nm	nautical mile
NSPD	national security presidential directive
PDD	presidential decision directive
UN	United Nations
UNCLOS	UN Convention of the Law of the Sea
USGS	United States Geological Survey

Considerations for a US Nuclear Force Structure below a 1,000-Warhead Limit

*Lt Col David J. Baylor, USAF**

On 5 April 2009 in Prague, Czech Republic, President Obama committed the United States to seeking "the peace and security of a world without nuclear weapons."¹ This move toward a world free of nuclear weapons is not a new idea. In January 2008, George P. Shultz, William J. Perry, Henry Kissinger, and Sam Nunn authored an article in the *Wall Street Journal*, "Toward a Nuclear Free World," in which they suggested steps to "dramatically reduce nuclear dangers." More than a dozen former senior US officials from the past six administrations endorsed these suggestions.² While these officials offered "suggestions," they realized the challenge of achieving a nuclear-free world would be difficult. In fact, the president recognized this challenge in his Prague speech when he stated, "This goal will not be reached quickly—perhaps not in my lifetime."³ Just as importantly, the president went on to state, "As long as these weapons exist, the United States will maintain a safe, secure and effective arsenal to deter any adversary, and guarantee the defense of our allies."⁴

As the president moves toward a nuclear-free world, we must ask some very important questions about that journey: (1) Are there different negotiation considerations and dynamics in play when Russia and the United States go below 1,000 strategic warheads? (2) What are the implications of nonstrategic or tactical nuclear weapons in the world security environment? and (3) Finally, what are some potential implications for the US nuclear force structure and the impact on the role of nuclear deterrence as our national arsenal moves below 1,000 strategic warheads?

New Negotiation Dynamics below 1,000 Warheads

A world free of nuclear weapons is a noble goal and a commitment we have as a nation in accordance with Article VI of the Nuclear Non-proliferation Treaty (NPT) as ratified by the United States in March 1970.⁵ Over the past 40 years, the United States has negotiated directly with the Soviets, and now the Russians, to reduce their nuclear arsenals. While negotiations were difficult, viewed from a distance

*Dr. Barry Schneider, USAF civilian, was the essay advisor for this paper.

these talks were very similar to Newton's Third Law of Motion: "For every action there is an equal and opposite reaction."⁶ This is not to say there was a one-for-one reduction in warheads between the two nations. But as one nation proposed an action to reduce weapons, the other responded with what it saw as an equal reduction while always maintaining the status quo balance of power. As we move into a period where the United States and Russian arsenals are perhaps reduced below 1,000 warheads, we leave Newtonian physics of equal and opposite actions and enter a new quantum physics world of negotiations, with additional actors affecting strategic and crisis stability with implications we don't yet completely comprehend.⁷

In this quantum physics view of nuclear arms reduction, we must look at numerous additional actors and forces—great and small—that will play important roles. These actors include current nuclear weapons states, aspiring nuclear weapon counties, other states with some nuclear technology, and US allies operating under the cover of our "nuclear umbrella."⁸ To understand the impact that these countries will have on the negotiation process as we move toward a world free of nuclear weapons, we must first have a general understanding of their current position in the world security environment and the direction these countries are moving. While it is impossible to know everything about each of these nations or to do justice to the complexity of these countries, we will look at some important factors to consider as the United States and Russia move toward nuclear arsenals below 1,000 warheads and fewer associated strategic delivery vehicles.

To start our examination of these players in the new world of ever-deeper cuts, we will first look at those countries currently possessing nuclear weapons. Only five recognized nuclear weapons nations have signed and ratified the NPT: the United States, Russia, China, France, and Great Britain. Russia, with its large nuclear arsenal, possesses the greatest potential threat to US national security.⁹ It is therefore against the Russian threat that the United States' deterrent forces must be capably and properly sized, since this force poses the greatest existential threat to the United States. The Russian government is no doubt concerned with deterring what it may perceive as a US threat to its existence. With maintaining this deterrent capability in mind, the United States and Russia are currently negotiating a follow-on agreement to the Strategic Arms Reduction Treaty (START) that expired on 5 December 2009, with the goal of significantly reducing the size of each long-range nuclear arsenal.¹⁰

Recent press releases show that Russia is working closely with the United States to reduce both countries' strategic nuclear warheads to around 1,500–1,675, while limiting their delivery systems for those

warheads to 500–1,000.¹¹ If negotiations are successful, the two countries would be at their lowest number of strategic nuclear weapons and delivery vehicles since the early 1950s for the United States and 1960s for Russia (see fig. 1), bringing both countries' arsenals much closer in number to the Chinese and other nuclear-armed nations.

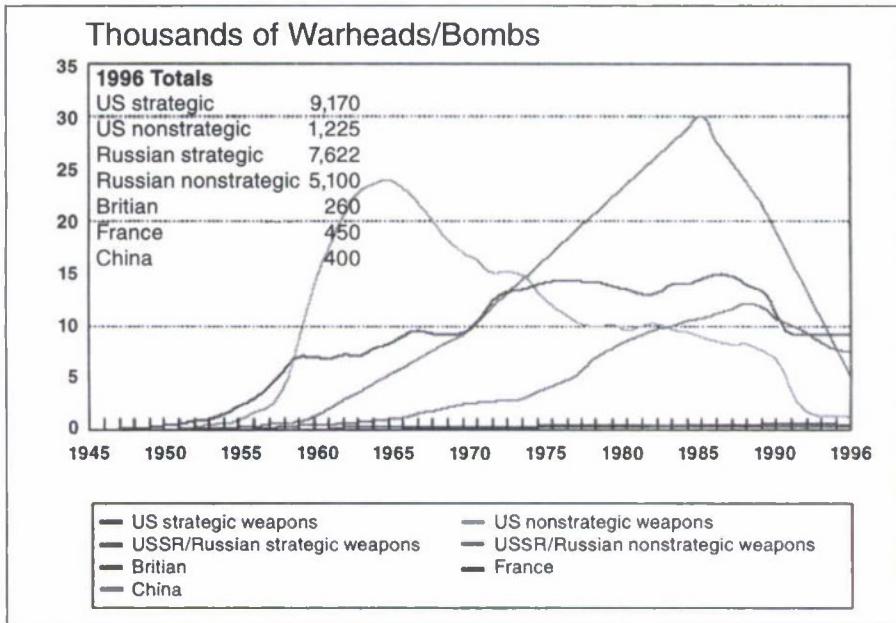


Figure 1. Global nuclear stockpiles, 1945–1996. These figures show active nuclear weapons. They do not include inactive but intact weapons awaiting dismantlement. For the United States, these warheads are estimated as follows: 241 (1988), 642 (1989), 752 (1990), 2,330 (1991), 5,261 (1992), 5,789 (1993), 4,916 (1994), 3,635 (1995), and 2,542 (1996). For the USSR/Russia, these are estimated as follows: 4,277 (1986), 4,141 (1987), 3,670 (1988), 3,183 (1989), 3,485 (1990), 5,394 (1991), 6,744 (1992), 8,215 (1993), 9,933 (1994), 11,385 (1995), and 12,278 (1996). It should be noted that there is a great deal of uncertainty as to the exact number of USSR/Russian nonstrategic nuclear weapons. South Africa (not shown) secretly built six nuclear weapons between 1979 and 1989; these were subsequently dismantled between July 1990 and July 1991. Israel (not shown) is assumed to have at present approximately 100–150 nuclear weapons. (Reprinted from Robert S. Norris and Thomas B. Cochran, *US and USSR/Russian Strategic Offensive Nuclear Forces, 1945–1996*, Nuclear Weapons Databook Working Paper 97-1 [Washington, DC: Natural Resources Defense Council, January 1997]; Robert S. Norris, "Nuclear Arsenals of the United States, Russia, Great Britain, France and China: A Status Report," Presented at the 5th ISODARCO Beijing Seminar on Arms Control, 12–15 November 1996; Robert S. Norris, Andrew S. Burrows, and Richard W. Fieldhouse, *Nuclear Weapons Databook*, vol. 5, *British, French, and Chinese Nuclear Weapons* [Boulder, CO: Westview Press, 1994]; and Robert S. Norris and William M. Arkin, "NRDC Nuclear Notebook [Global Nuclear Stockpiles, 1945–1997]," *Bulletin of the Atomic Scientists*, November/December 1997, 67.)

While publicly committing to a world free of nuclear weapons, Russia continues to replace its strategic nuclear warheads with new designs and delivery systems.¹² In recent defense budgets, it has allocated resources to procure new dual-capable strategic bombers while also attempting to reinvigorate its fleet of nuclear submarines.¹³ In addition, it is building new land-based RS-12M1/2 Topol-M intercontinental ballistic missiles (ICBM) with a multiple reentry vehicle capability.¹⁴ Most importantly, Russia is placing more emphasis on its large stockpile of tactical nuclear weapons in its national defense strategy.¹⁵ Its shift to a “first use” strategy is a counterbalance and cost-savings move while it is downsizing and modernizing its conventional military forces.¹⁶ With this increased reliance on nuclear weapons in a first-use capacity, it will be difficult for the Russians to reduce their nuclear arsenal below START Follow-on levels until they feel their conventional forces are equal or greater in capability to North Atlantic Treaty Organization (NATO) and Chinese conventional forces on their borders.

According to open sources, China possesses approximately 240 nuclear warheads, with approximately 186 operationally ready for employment on aircraft and ballistic missiles.¹⁷ With such a small force, China appears to have adopted a minimum deterrence strategy. Of these warheads, approximately 20 CSS-4 ICBMs are able to reach the United States.¹⁸ The remaining warheads are programmed to be delivered by aircraft along with short- and medium-range missiles.¹⁹ The Chinese have publicly declared a “no first use” policy, with a self-defense nuclear strategy.²⁰ China has taken the route of defense against attack by developing underground facilities to house its nuclear weapons, providing for maximum survival of its arsenal from a first strike and guaranteeing a robust retaliatory capability.²¹ Maintaining a secure second-strike retaliatory force rather than an insecure and vulnerable nuclear force is also better for crisis stability.²²

When we include the Chinese at the arms control negotiation table, we must first consider their strategic situation of being surrounded by such nuclear-armed countries as the United States, Russia, India, North Korea, and Pakistan and within striking distance of Iran. While China has formidable conventional forces, as long as surrounding countries have nuclear weapons, the Chinese are unlikely to reduce their nuclear arsenal. Indeed, all countries with nuclear arms need to be included in future nuclear arms control treaty negotiations, including the United Kingdom and France.

The UK currently maintains approximately 160 nuclear warheads configured to be delivered by submarine launched ballistic missiles (SLBM) from four *Vanguard*-class Trident fleet ballistic missile sub-

marines (SSBN).²³ The UK currently only has the ability to deliver nuclear weapons from its submarines. Researchers at the Stockholm International Peace Research Institute (SIPRI) believe that some of the UK missiles only contain one warhead and are configured for a "low yield" by using only the "fission primary." The UK Ministry of Defense believes this "provides a 'sub-strategic' role to the Trident Fleet."²⁴ Britain has reduced its reliance on nuclear weapons since the end of the Cold War, and, from recent comments made by Prime Minister Gordon Brown, it appears it is willing to reduce its number of new nuclear submarines purchased by 25 percent, from four to three.²⁵

France possesses approximately 300 nuclear weapons that are widely dispersed on four SSBNs and 84 tactical aircraft.²⁶ While the French have recently rejoined NATO's Integrated Military Command after 43 years, they still pride themselves on a nuclear capability that could be used independently of the NATO command structure.²⁷

While the UK, France, Russia, and China are all important players as nuclear powers and permanent members of the United Nations (UN) Security Council, when the United States goes below 1,000 strategic nuclear warheads, it and all other states that possess nuclear weapons will need to be included at the negotiations table. These additional countries—India, Pakistan, North Korea, and Israel—are not signatories to the NPT but already have or, in the case of Israel, are believed to have, nuclear weapons.

India currently maintains an arsenal estimated at approximately 60–70 tactical nuclear weapons delivered by aircraft along with short- and medium-range missiles.²⁸ India and its rival, nuclear-armed Pakistan, have fought three wars and continue to threaten each other, suggesting these two states must, at some point in the near future, be included in multilateral nonproliferation and nuclear arms control talks.

Pakistan is estimated to possess 60 tactical nuclear weapons along with enough plutonium and highly enriched uranium to produce 40 more.²⁹ It sees India's larger and technologically more advanced conventional military as an existential threat.³⁰ Pakistan will not give up its nuclear weapons, seen as equalizers, as long as it sees India as a threat. In addition, as the only Muslim nation with nuclear weapons, Pakistani leaders and citizens take pride in the prestige conferred by their nuclear arsenal. While India and Pakistan should be essential players in future negotiations, we must also consider crafting agreements to take into account and limit other states that have or are pursuing nuclear weapons, such as North Korea, Iran, and Israel.

North Korea has twice demonstrated the ability to detonate a nuclear weapon while it refines its ICBM capabilities. Iran, already with a proven short- and medium-range missile capability, continues to

defy UN mandates as it develops its uranium enrichment technologies. Israel has chosen a nondeclaratory policy toward nuclear weapons, but some analysts estimate that Israel maintains approximately 100 nuclear warheads.³¹ These three states, with their nuclear ambitions, influence and threaten the security of countries around them that either already have some nuclear technology or have the funding to acquire nuclear technology and weapons.

For example, North Korea's nuclear ambitions affect the Republic of Korea and Japan. These are two of 30-plus countries under the United States' nuclear umbrella.³² Japan has the technological knowledge to build nuclear weapons if it chooses.³³ On the other side of Asia, Iran's drive to acquire nuclear weapons has inspired other Middle Eastern countries such as Saudi Arabia, Egypt, and Turkey to consider pursuing their own enrichment capabilities.³⁴

Prestige is another important consideration in future nuclear negotiations. Many countries, such as the UK, France, India, Pakistan, Iran, and North Korea, see nuclear weapons not only as part of their national security policy but also as important status symbols providing them influence in the international community and a seat at the table with the United States, Russia, and China. Asking these countries to give up their nuclear weapons and perceived political status in international relations will complicate all future nuclear arms negotiations directed toward that end.

While prestige is a factor to consider, ironically, democracy will add one of the biggest unknown variables to all future negotiations. With elections held at periodic intervals throughout the various democratic countries around the world, internal politics of the moment can almost instantly change the direction that country takes concerning nuclear weapons. Some examples include the US election with the change in direction between the Bush and Obama administrations. The various NATO allies can easily change their stance on nuclear weapons and forward deployment of US nuclear weapons within their countries. The recent Japanese election demonstrates how an administration can take a significantly different approach to nuclear weapons, as demonstrated by their recently launched probe into reported "secret nuclear pacts" with the United States.³⁵ While all states, democratic and autocratic, can be reversed by their opponents taking power, this is more likely to occur within democracies.

Another potential problem is that verification of compliance by nine to 10 different nuclear-armed countries will slow the progress and complicate nuclear disarmament talks. Current bilateral US and Russian negotiations have yielded an accepted inspection protocol

that works in the current negotiation environment. However, future multinational negotiations may present numerous new questions:

- Can 10 different states agree upon a rigorous and adequate verification regime?
- What kind of international inspectorate can be formed?
- Will each state be willing to open its country to adequate types of inspections?
- What is the role that the UN will play in treaty execution?
- How does the United States manage and verify stockpiles to ensure other nuclear states do not reweaponize?
- How do we prevent countries from nuclear weapons breakouts from their treaty obligations and, thereby, gaining strategic advantages denied to others?
- As we disarm further, can we ensure the protection to our allies currently under our nuclear umbrella?
- Will these countries pursue their own nuclear weapons as the US nuclear force shrinks?
- Will their foreign policies change in favor of nuclear neighbors, making us less secure?
- Is there some alternative other than nuclear protection that the United States can substitute?

This discussion identifies some of the players and future questions that must be considered in forging new nuclear arms reduction agreements, along with the dynamics in play within and among these nations. It is easy to understand why President Obama does not see a world free of nuclear weapons as happening within his lifetime. With the rapid spread of nuclear energy and weapons technology, we are about to enter a new world of arms negotiations much different from those we have practiced with the Russians. What this means is that we may be on a path to reduce our weapons and delivery systems to numbers closer to other nuclear-armed countries around the world in the next decade or so. If this happens, we will then enter a period in history with multiple countries possessing relatively equal numbers of nuclear weapons, while others still seek to acquire nuclear weapons.

When we negotiate with these multiple nuclear powers in the future in bringing our warhead numbers below 1,000 to around 500, we will be negotiating less from the position of superior numbers and

relative strength and more from relative parity. This will require a dramatic shift in our national security outlook. Indeed, should such deep cuts be taken, we will have fewer warheads and delivery vehicles than we have had since the 1950s, and more countries will possess or be seeking to acquire nuclear weapons.

Significance of Tactical Nuclear Weapons

While most other nuclear nations around the world are upgrading their delivery systems and replacing their old warheads, the United States has placed a self-imposed freeze on the replacement of our nuclear stockpile.³⁶ In addition, due to our geographic location in the world and historical context, we are sitting on a stockpile of what are considered strategic nuclear weapons, while the preponderance of other nuclear weapons around the world are considered tactical. This is an important factor to consider as the START Follow-on talks with the Russians only address strategic nuclear weapons, allowing Russia to retain an advantage in tactical nuclear weapon inventory to defend its borders.³⁷

The simple difference between strategic and nonstrategic or tactical nuclear weapons, as defined by the United States and Russia, is the difference in the range of delivery vehicles. ICBMs, SLBMs, and long-range bombers with the intercontinental range to destroy military, industrial, and leadership targets in each other's homelands are considered strategic nuclear weapons. Nuclear weapons that do not have the ability to reach the United States' or Russian heartlands when launched from their homelands are considered tactical nuclear weapons.³⁸ While there are some exceptions to this definition, it is important to realize that under the Strategic Arms Limitation Talks (SALT) I, SALT II, START, START II, the Strategic Offensive Reduction Treaty (SORT), and START Follow-on treaties, only strategic warheads and delivery systems (ICBMs, SLBMs, long-range bombers) are considered. This leaves out of the negotiations Russia's large nonstrategic weapons arsenal estimated at 2,000 to 6,000 tactical nuclear weapons.³⁹

The actual number of Russian nonstrategic or tactical nuclear weapons is difficult to pinpoint. In its 2009 yearbook, *Armaments, Disarmament and International Security*, SIPRI places Russian operational numbers at the low end of 2,047 deployed tactical warheads. Of these, 701 tactical nuclear weapons are assigned to missile-defense interceptors. The remainder of the nonstrategic weapons is offensive, including 648 weapons for delivery by land-based bombers like the Tu-22M Backfire and Su-24 Fencer. Further, the Russian Navy pos-

sesses 237 tactical nuclear weapons to be delivered by naval aircraft and 276 on sea-launched cruise missiles to be launched from ship platforms. Another 185 tactical nuclear weapons are dedicated to antisubmarine warfare and surface-to-air missiles.⁴⁰

These numbers are in contrast to the 400 US operational non-strategic weapons—all B61 gravity bombs delivered by fighters and bombers.⁴¹ Excluding missile-defense warheads, the Russians have a three-to-one numerical advantage over the United States in tactical nuclear weapons. However, these shorter-range weapons, if based on Russian soil, cannot reach the continental United States. Tactical nuclear arms would primarily be the concern, therefore, of states along Russia's periphery in Asia and Europe.

While the United States and Russia have their understanding and definition of strategic nuclear weapons worked out by negotiations, it is difficult for most countries in Europe and Asia to distinguish between Russia's strategic and tactical nuclear weapons. To countries like Estonia, South Korea, or Japan, one low-yield "tactical" nuclear weapon delivered by a missile or fighter aircraft would have devastating strategic implications.

These tactical nuclear weapons present additional challenges to negotiations and proliferation. First, tactical nuclear weapons are, on average, smaller than strategic weapons. Yields can vary anywhere from subkiloton to the strength of a strategic nuclear weapon. Smaller-sized weapons present multiple challenges. First, these weapons are easier to hide, complicating verification of treaty limits. In addition, unlike a bomber, ICBM, or SLBM force, tactical nuclear weapons are easily moved, contributing to counting and verification problems. Finally, the relatively low yield of some of these weapons may increase the likelihood of use in certain crisis contingencies. In some cases, this can improve deterrence effects versus an adversary but also might tempt decision makers to use them more readily. These tactical nuclear weapons spread around the world will put the United States in a difficult strategic position. If moved forward nearer the United States either clandestinely or on mobile platforms, these "tactical" weapons could become "strategic."

Impact on the United States and the Air Force in the Near Future

As START Follow-on Treaty negotiations continue and as we strive for a nuclear-free world in perpetuity, the United States will find itself in a unique situation. Unlike Russia and China who have chosen to modernize their nuclear arsenals, or countries like India, Pakistan,

and Iran who have recently developed or are developing new weapons, the United States has chosen a path of "life extension" for its weapons.⁴² This life extension approach can be complicated, as some components originally developed for these weapons are no longer manufactured.⁴³ This new paradigm of parity in numbers, more nuclear nations around the world, and an aging US arsenal will present numerous challenges to the United States over the next few decades.

First, as we move below 1,000 strategic warheads and toward 500 or fewer delivery systems, the Department of Defense will be forced to make difficult force structure decisions.⁴⁴ Just a reduction to the numbers Russian president Dmitry Medvedev proposed in September 2009 would force the United States to look seriously at reconfiguring its current strategic nuclear weapons triad of ICBMs, SLBMs, and long-range bombers of B-52s and B-2s, while considering the inefficiencies of maintaining three separate weapon systems in small quantities.⁴⁵

The United States might take numerous approaches when apportioning its nuclear weapons and delivery systems. An in-depth study will be required to optimize deterrence effects of the US nuclear arsenal following any future arms treaties, but two general approaches will most likely be considered. The first is an across-the-board reduction in all weapon systems to include ICBM's, bombers, and SLBMs. Another more likely approach will be to completely eliminate one leg of the triad. Each leg of the triad possesses strengths and weaknesses, and each adds a certain element of deterrence that translates into retaliatory strength. If we look at other nations, such as Great Britain, that have trimmed their nuclear arsenals over the years for an indication of the direction we may go, it appears SLBMs would be the weapon systems of choice to maintain. The primary advantage of the SLBM force is its likely survivability from a rival's surprise first strike. The downside is the "all of your eggs in one basket" syndrome. Advances in antisubmarine warfare by our adversaries may materialize in the future, threatening the survivability of our submarines. If so, then the preponderance of our nuclear capability could be lost. Indeed, a single submarine malfunction might instantaneously bring its 24 missiles off alert.⁴⁶ If there were a defect in a missile or warhead type, then all US SLBMs could possibly be rendered useless. Therefore, it would be prudent for the United States to maintain some semblance of diversity in its nuclear arsenal.

Unfortunately, the Air Force, as has been documented in several recent studies, for a time had neglected its maintenance, security, funding, and advocacy for nuclear weapons, thereby somewhat eroding its ability to carry out its mission of strategic deterrence.⁴⁷ Atrophy of our capabilities over the past 17 years has produced a genera-

tion of leaders who are not well versed in the nuclear mission and who are unable to advocate properly the advantages and necessity of the Air Force's role in nuclear deterrence.⁴⁸ As a service, we continue to look to the future for the next new thing while sometimes forgetting our heritage.

This loss of mission focus may regrettably cause the Air Force to lose much of the nuclear mission it fought the Navy so hard for.⁴⁹ As the Air Force revitalizes the nuclear enterprise, part of the price of neglect might be the eventual loss of the nuclear strategic bombing mission. US bombers are dual capable and can easily be used in conventional-only missions, much like the B-1 transition made in the early 1990s. This would be an easy force structure modification, leading to a dyad of US nuclear weapons rather than a triad. Removal of the bombers from our nuclear arsenal would eliminate an important signaling capability. Unlike other legs of the triad, bombers can be both launched and recalled. By scrambling our bomber forces, getting them airborne poised to strike, the country can signal its willingness (an important part of deterrence) to use nuclear weapons. Yet US decision makers can still recall the bombers once launched. Without bombers to put on alert, this traditional signaling mechanism could be lost.

Recent revitalization of the nuclear enterprise is not limited to the bomber force; it also includes the ICBM career field. As the Air Force strives to provide those who work with ICBMs a sense of purpose and mission in a post-Cold War era, it will be faced with increased reductions, as the ICBMs will be the second most likely delivery system in the US nuclear arsenal to be reduced, if not eliminated.

These reductions in USAF resources and missions, if taken, would exacerbate the nuclear culture problems it currently faces. With fewer nuclear billets in the Air Force at fewer locations, there would be an even smaller numbers of officers and senior noncommissioned officers to call upon to fill important command-and-control and critical nuclear-related staff and leadership positions. With a continued decrease in emphasis within the Air Force on the nuclear mission, it would be even more difficult to draw the best and brightest young Airmen into this dying career field, causing many to pursue other career opportunities. On the other hand, while it looks like there may be a reduction in Air Force strategic nuclear weapon delivery systems, there may be an associated increase in the deterrence role for the Air Force's fighter community.

To maintain some semblance of a triad to provide the necessary deterrence effects and security for our allies, the fighter community could ultimately pick up more of the aircraft nuclear weapons deliv-

ery mission formerly provided by heavy bombers. With the new Joint Strike Fighter becoming the Air Force's weapons system of choice, its mandated nuclear weapons delivery capability will be a vital part of its mission.⁵⁰

With a world moving toward a preponderance of tactical nuclear weapons (see fig. 2), it will be important for the United States to demonstrate its tactical nuclear capability. This capability could be a critical element of our future deterrence posture. It can be used in a show of force and national resolve when the aircraft are forward deployed and placed on airborne alert.

F-35s picking up the nuclear deterrence role from the bombers will present its own set of problems to the Air Force. Tactical nuclear weapons may not be regularly deployed to Asia and Europe due to the constantly changing political environments. However, if F-35s are to play a nuclear deterrent role, it would be wise to continue to deploy most of the estimated 200–350 forward-based nuclear bombs and air-to-ground missiles in NATO countries (see table 1).⁵¹ Otherwise, the F-35 community will face the challenges of keeping fighter crews, maintainers, security forces, and support personnel associated with

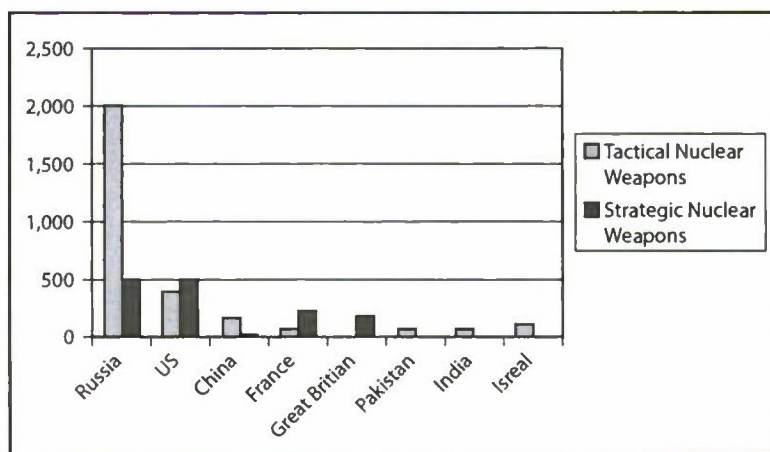


Figure 2. Future US/Russian strategic warhead limit of 500 with current tactical nuclear weapons. Strategic numbers are based on any future agreement between Russia and the United States that limit strategic nuclear weapons to 500 warheads each. Strategic nuclear weapons for China, France, and Great Britain along with all tactical nuclear weapons numbers are based on current strategic nuclear weapons and tactical nuclear weapons as reported by the Stockholm International Peace Research Institute. (Reprinted from SIPRI, *SIPRI Yearbook 2009, Armaments, Disarmament and International Security* [Oxford, UK: Oxford University Press]).

Table 1. Status of US nuclear weapons in Europe, 2008

Country	Air Base	Custodian	Delivery	Deployment	
				W53 vaults	Est. Weapons
Belgium	Kleine	701st MUNSS ^a	Belgian F-16s	11	10–20
Germany	Broegel Büchel	702d MUNSS	German Tornadoes	11	10–20
Holland	Volkel	703d MUNSS	Dutch F-16s	11	10–20
Italy	Aviano Ghedib	31st Fighter Wing	US F-16s	18	50
		704th MUNSS	Italian Tornadoes	11	20–40
Turkey	Incirlik ^c	39th Air Base Wing	Rotational US aircraft from other wings	25	50–90
				33	50–110
UK	Lakenheath	48th Fighter Wing	US F-15Es	33	50–110
				<i>Total</i>	200–350

Source: Hans M. Kristensen, "USAF Report: 'Most' Nuclear Weapons Sites in Europe Do Not Meet U.S. Security Requirements," Federation of American Scientists, Strategic Security Blog, <http://www.fas.org/blog/ssp/2008/06/usaf-report>, 19 June 2008.

^aMunitions Support Squadron

^bRumored decision to withdraw 704 MUNSS and consolidate weapons at Aviano.

^cNo permanent fighter wing at base. National Turkish nuclear strike mission in doubt.

nuclear weapons fully qualified and capable of completing the nuclear mission while not actually having nuclear weapons at their forward locations. This shift to the F-35 as the primary airborne delivery system would provide enhanced deterrence for our nation at the cost of a cultural shift among the fighter community as it takes on this important role.

Conclusion

In April 2009, President Obama set the nation on the path toward the eventual long-term goal of zero nuclear weapons. Nuclear disarmament has been a worldwide goal since the Nuclear Non-proliferation Treaty was opened for signature in 1970. Over the years, states have taken numerous positive steps toward that end. Now the United States finds itself in negotiations with Russia to further reduce our nuclear arsenal. Perhaps in later rounds, after the current START Follow-on negotiations, the sides may agree to levels below 1,000 warheads. Once we cross the 1,000 threshold, we will be entering a new, more complicated world of nuclear arms negotiations.

As previously noted, it will take time to understand the different players, motives, and issues that each of the new players brings to the negotiation table. The challenge is to coordinate the step-by-step disarmament of the nine current members of the nuclear weapons state club while simultaneously attempting to persuade others from "going nuclear." New challenges on the path to zero may emerge as allied nations consider acquiring nuclear weapons to make up for a perceived loss of US umbrella protection or as other nations see an opportunity to increase their relative military/political power and prestige.

To counter these unintended consequences, it is important to bring into negotiations all of the world's nuclear-armed nations as soon as possible. However, even if we were to bring all other nuclear-armed nations into negotiations today, it would likely be a long time, if ever, before all parties would be able to agree on total disarmament or even on the next steps to be taken. During this protracted period of negotiations, we are going to find ourselves in a world with a group of countries that possess a relatively large and growing number of nuclear weapons.

The preponderance of weapons in this new environment will be so-called nonstrategic nuclear weapons, which will present a different dimension to our national security posture and force structure. The United States will have to make some tough choices as negotiations further limit delivery vehicles and warheads. With the most likely losses to the strategic retaliatory forces being first the bombers and then, possibly later, a reduction of ICBMs, the Air Force will need to focus more on its tactical nuclear mission. This proposed shift to tactical nukes would have a dramatic impact on the Air Force's efforts to reinvigorate its nuclear enterprise.

As the Air Force endeavors to recapture the pride and discipline of Strategic Air Command (SAC) without actually resurrecting SAC, it will be faced with the additional challenges of a nuclear force structure so small that it will be even more difficult to maintain and inspire those to join and work with high energy and commitment. In addition, if the United States shifts to F-35s as the foundation of its nuclear airborne arsenal, the service will experience a cultural shift among aircrews as fighter pilots more fully join the nuclear enterprise by taking on the traditional role of the bombers.

The United States is committed to a path of a nuclear-free world. Meanwhile, the Air Force is committed to reinvigorating its nuclear enterprise. The first is a noble goal fraught with unknown challenges, numerous new actors, and dynamics that will yield surprises. The latter will reinvigorate the USAF nuclear force while simultaneously

downsizing that arsenal, reducing the role of nuclear weapons in the US national security strategy. This downsizing may ultimately result in a shift of focus on the Air Force's nuclear deterrence role from the strategic bomber community to tactical fighters.

Notes

1. "Remarks by President Barack Obama, Hradcany Square, Prague, Czech Republic," Office of the Press Secretary, The White House, 5 April 2009, http://www.whitehouse.gov/the_press_office/Remarks-By-President-Barack-Obama-In-Prague-As-Delivered.

2. George Shultz, William J. Perry, Henry A. Kissinger, and Sam Nunn, "Toward a Nuclear-Free World," *Wall Street Journal*, 15 January 2008, http://online.wsj.com/public/article_print/SB120036422673589947.html.

3. "Remarks by President Barack Obama."

4. Ibid.

5. US Department of State (DOS), "Treaty on the Non-Proliferation of Nuclear Weapons (NPT)," entered into force 5 March 1970, *United States Treaties and Other International Agreements*, vol. 757, no. 10485, <http://www.state.gov/t/isn/trty/16281.htm>.

6. Isaac Asimov, *Understanding Physics* (New York: Walker, 1966), 34.

7. The Heisenberg uncertainty principle simply states that you can't know the position and momentum of an atom at the same time; similarly, under the current international environment no country or entity completely knows the "nuclear position" or the "direction and speed" (momentum) a country is moving with regards to nuclear weapons. Richard Rhodes, *The Making of the Atomic Bomb* (New York: Simon & Schuster, 1986), 130.

8. James Schlesinger, chairman, *Report of the Secretary of Defense Task Force on DoD Nuclear Weapons Management: Phase I: The Air Force's Nuclear Mission* (Washington, DC: Department of Defense, 2008).

9. US DOS, "Treaty on the Non-Proliferation of Nuclear Weapons."

10. US DOS, "START II Treaty," 1997, <http://www.state.gov/www/global/arms/starthtm/start2/st2intal.html>.

11. RIA Novosti, "Russia, U.S. to Slash Nuclear Delivery Vehicles—Medvedev," 24 September 2009, <http://en.rian.ru/world/20090924/156243233.html>.

12. Schlesinger, *Report of the Secretary of Defense*, 18.

13. RIA Novosti, "Russia Air Force to Get New TU-160 Strategic Bomber in April," 22 April 2008, <http://en.rian.ru/russia/20080422/105640820.html>; and RIA Novosti, "Russia to Start Construction of 4th Borey-Class Sub in December," 5 October 2009, <http://en.rian.ru/russia/20091005/156357397.html>.

14. Stockholm International Peace Research Institute (SIPRI), *SIPRI Yearbook 2009: Armaments, Disarmament and International Security* (Oxford, UK: Oxford University Press, 2009), 353.

15. For an in-depth study of US and Russian nonstrategic or tactical weapons, see Amy F. Woolf, *Nonstrategic Nuclear Weapons* (Washington, DC: Congressional Research Service, 2009), 14–17.

16. Stephen J. Cimbala, "Forward to Where? U.S.-Russia Strategic Nuclear Force Reductions," *The Journal of Slavic Military Studies* 22, no. 1 (January 2009): 68–86, <http://www.informaworld.com/smpp/ftinterface~db=all-content=a909097059~fulltext=713240928>.

17. SIPRI, *SIPRI Yearbook 2009*, 364.

18. Ibid.

19. Ibid.
20. Office of the Secretary of Defense, *Annual Report to Congress, Military Power of the People's Republic of China 2009*, 24, <http://www.cfr.org/publication/18943>.
21. Hans M. Kristensen, "Estimated Nuclear Weapons Locations 2009," Federation of American Scientists, Strategic Security Blog, November 2009, <http://www.fas.org/blog/ssp/2009/11/locations.php>.
22. States with vulnerable nuclear forces may be tempted to launch their forces on warning (LOW) or under attack (LUA), and this could put a hair trigger on their weapons to prevent their being destroyed by surprise attack. The Chinese seem to have solved this "use or lose" dilemma by deploying nuclear arms underground.
23. SIPRI, *SIPRI Yearbook 2009*, 359.
24. Ibid., 360.
25. Elliott Francis and Michael Evans, "Britain's Nuclear Overture—We Will Cut Trident Fleet," *Timesonline*, 22 September 2009, <http://www.timesonline.co.uk/tol/news/politics/article6845247.ece>.
26. SIPRI, *SIPRI Yearbook 2009*, 360.
27. Edward Cody, "After 43 Years, France to Rejoin NATO as Full Member," *Washington Post*, 12 March 2009, <http://www.washingtonpost.com/wp-dyn/content/article/2009/03/11/AR2009031100547.html>.
28. SIPRI, *SIPRI Yearbook 2009*, 367, 370.
29. Ibid., 367, 372.
30. Rolf Mowatt-Larssen, "Nuclear Security in Pakistan: Reducing the Risks of Nuclear Terrorism," Arms Control Association, *Arms Control Today*, July/August 2009, http://www.armscontrol.org/act/2009_07-08/Mowatt-Larssen.
31. SIPRI, *SIPRI Yearbook 2009*, 375.
32. Schlesinger, *Report of the Secretary of Defense*, 18.
33. Federation of American Scientists, "Nuclear Weapons Program," 16 April 2000, <http://www.fas.org/nuke/guide/japan/nuke>.
34. Joseph Cirincione, *Bomb Scare: The History and Future of Nuclear Weapons* (New York: Columbia University Press, 2007), 103.
35. Jun Hongo, "Probe Launched into Four Secret Pacts with U.S.," *Japan Times Online*, September 2009, <http://search.japantimes.co.jp/cgi-bin/nn20090926a2.html>.
36. Jeffrey Lewis, "After the Reliable Replacement Warhead: What's Next for the U.S. Nuclear Arsenal?" Arms Control Association, *Arms Control Today*, December 2008, http://www.armscontrol.org/act/2008_12/Lewis.
37. Woolf, *Nonstrategic Nuclear Weapons*, 14–16.
38. Ibid., 5.
39. Ibid., 17.
40. SIPRI, *SIPRI Yearbook 2009*, 354.
41. Ibid., 348.
42. William J. Perry, chairman, and James R. Schlesinger, vice-chairman, *America's Strategic Posture, The Final Report of the Congressional Commission on the Strategic Posture of the United States* (Washington, DC: United States Institute of Peace Press, 2009), 40, http://www.usip.org/files/America's_Strategic_Posture_Auth_Ed.pdf.
43. Ibid.
44. Joint Working Group of the American Association for the Advancement of Science (AAAS), American Physical Society, and the Center for Strategic and International Studies, *Nuclear Weapons in 21st Century U.S. National Security* (Washington, DC: AAAS, 2008), 8, <http://www.aps.org/policy/reports/popa-reports/upload/nuclear-weapons.PDF>.
45. President Medvedev stated on 24 September that the United States and Russia were discussing the possibility of slashing nuclear weapon delivery vehicles by 67 per-

cent. From the US State Department report in April, the United States has 1,198 delivery vehicles; this cut would reduce US delivery vehicles to below 500. RIA Novosti, "Russia, U.S. to Slash Nuclear Delivery Vehicles."

46. "Trident Fleet Ballistic Missile," US Navy Fact File, *Navy.mil*, 17 January 2009, http://www.navy.mil/navydata/fact_display.asp?cid=2200&tid=1400&ct=2.

47. Schlesinger, *Report of the Secretary of Defense*, 51.

48. *Ibid.*, C-1.

49. Walter J. Boyne, *Beyond the Wild Blue: A History of the United States Air Force, 1947-1997* (New York: St. Martin's Press, 1997).

50. Adam J. Hebert, "New Nukes, Old Nukes," *Air Force Magazine* 92, no. 10 (October 2009): 20.

51. Ian Anthony, *The Future of Nuclear Weapons in NATO* (Stockholm, Sweden: SIPRI, 4 February 2008), 28.

Abbreviations

ICBM	intercontinental ballistic missile
LOW	launch on warning
LUA	launch under attack
NATO	North Atlantic Treaty Organization
NPT	Nuclear Non-proliferation Treaty
SAC	Strategic Air Command
SALT	Strategic Arms Limitation Talks
SIPRI	Stockholm International Peace Research Institute
SLBM	submarine launched ballistic missile
SORT	Strategic Offensive Reduction Treaty
SSBN	fleet ballistic missile submarine
START	Strategic Arms Reduction Treaty
UN	United Nations

Getting War Fighters What They Need, When They Need It

*Col Carl E. Schaefer, USAF**

In 1981 the Air Force completed the requirements for the Advanced Tactical Fighter (ATF) and began the longest fighter aircraft acquisition program in history. The ATF was to replace the F-15, 13 years old at the time, and counter the proliferation of Soviet Su-27 advanced fighter planes. Ten years later, in 1991, Lockheed's ATF prototype, the YF-22, won the flyoff competition against Northrop Grumman's YF-23. The initial program called for 750 F-22s to be Initial Operational Capable (IOC) in 1995.¹ Following the flyoff and 14 more years of development, the F-22A became IOC with 12 aircraft in December 2005, 10 years later than desired. Twenty-four years of acquisition developed the most capable and complex fighter in the world, but the schedule and cost overruns contributed to the Air Force being authorized to procure 187 of the 750 required to replace the F-15.

Almost 25 years after the initial ATF requirements, Marine commanders developed the requirements for the mine-resistant ambush protected (MRAP) vehicle in 2005.² This vehicle was developed to stem the horrific affects from improvised explosive devices (IED), accounting for 75 percent of all US casualties in Iraq and Afghanistan.³ Using streamlined acquisition processes, the MRAP became IOC in 2007, 33 months after identifying the need.⁴ As of July 2009, 16,204 MRAP vehicles have been produced, and over 13,000 have been fielded.⁵

Although it is unfair to compare the F-22 and MRAP vehicle acquisitions based upon weapon system complexity, urgent need, streamlined acquisition processes, and supplemental congressional funding, the MRAP example clearly points to the government's ability to quickly procure military weapon systems when required. These rapid acquisition processes are slowly being institutionalized throughout the services to meet urgent needs for our war fighters in the face of a rapidly evolving threat.

Currently, each service and combatant command (COCOM) has its own rapid acquisition process. The Defense Science Board (DSB) completed a study in July 2009 which states, "Current approaches to implement rapid responses to urgent needs were found to be unsustainable, and institutional barriers—people, funding, and processes—

*Col Norman Potter, USAF, was the essay advisor for this paper.

are power inhibitors to successful rapid acquisition and fielding of new capabilities.”⁶ The study found that rapid acquisition processes should be based on proven technology to deliver capability to the war fighter within two to 24 months. The study also recommends that the Department of Defense (DOD) “establish a streamlined, integrated approach for rapid acquisition.” Finding a rapid acquisition standard for all services is the focus of this paper.⁷

I propose the United States Special Operations Command’s (SOCOM) rapid acquisition process offers a benchmark that should be adopted throughout the military. SOCOM’s rapid acquisition process could be used to acquire a limited major weapon system (MWS) (e.g., a light attack aircraft) in less than two years.

Deliberate and Rapid Acquisition— What’s the Difference?

When people think of DOD acquisition processes, they are generally thinking about deliberate acquisition. Programs like the B-2, F-22, F-35, and the Army’s Future Combat System come to mind. These large programs take years and billions of dollars to develop. Many don’t survive the cost overruns and schedule delays associated with these programs. In May 2009, Defense Secretary Robert Gates announced the cancellation of the VH-71 presidential helicopter, the Air Force Combat Search and Rescue X program, ground components of the Future Combat System, and missile defense’s multiple kill vehicle.⁸ Secretary Gates stated the root causes for the cancellations were immature technology and unnecessary requirements, which led to cost and schedule overruns and fewer quantities procured.⁹

The 2009 DSB states, “Over the course of the wars in Iraq and Afghanistan, it became apparent that U.S. forces were not adequately equipped for ongoing stability or counter insurgency operations.”¹⁰ The report also notes that “the reality is that the Department is not geared to acquire and field capabilities in a rapidly shifting threat environment.”¹¹ The deliberate acquisition process was not developed to handle urgent needs, so each service and COCOM developed its own processes. As a foundation for this paper, the deliberate acquisition process and selected rapid acquisition processes are examined.

Deliberate Acquisition

Deliberate acquisition is governed by the Joint Capabilities Integration and Development System (JCIDS) for requirements; the DOD 5000-series of regulations for acquisition guidance; and the Plan-

ning, Programming, Budgeting, and Execution (PPBE) for funding.¹² Details of each process are beyond the scope of this paper, but as shown in figure 1, the JCIDS precedes the acquisition process to validate the joint capabilities required to counter current and future threats. Once a required capability is identified, a service (Army, Navy, or Air Force) is designated to acquire the weapon system to meet the capability shortfall. To develop the system, the designated service will request funding from Congress through the PPBE system.

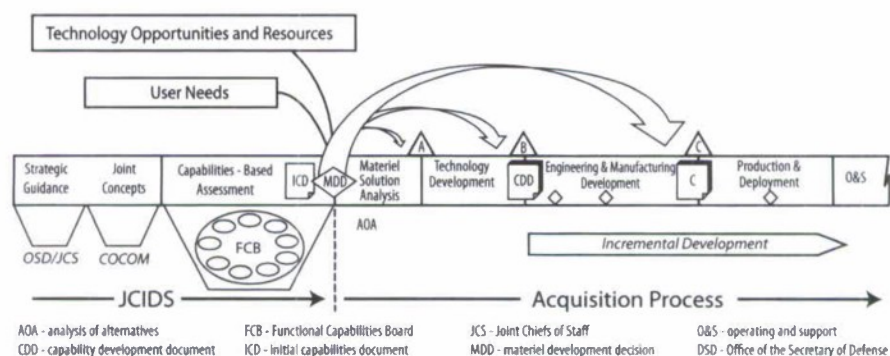


Figure 1. JCIDS/Acquisition Process

According to the Congressional Research Service, "the PPBE is intended to provide Combatant Commanders the best mix of forces, equipment, and support within fiscal constraints; the PPBE develops DOD's proposed budget for all acquisitions."¹³ Each service and COCOM plans and develops a five-year program to fulfill its mission responsibilities. This five-year plan is called the program objective memorandum (POM) and is submitted to the OSD for approval. Concurrent with the POM process, each service develops a budget estimate submission (BES) to support the POM and then submits it to the OSD. The OSD then consolidates each service's BES for a DOD budget submission to the president. Following presidential approval, the budget is submitted to Congress for approval. Although this is a simplified explanation of the DOD's deliberate acquisition process, it is clear to see the multistep process and review system to approve funding for a particular program.

In 1987 SOCOM was established to "oversee the training, doctrine, and equipping of all U.S. Special Operations Forces."¹⁴ To meet the unique needs of special operations forces, SOCOM was granted certain exceptions to the deliberate acquisition system. Under provisions of Title 10, *US Code*, "the commander of special operations command

shall be responsible for, and shall have the authority to conduct, the following: development and acquisition of special operations—peculiar equipment and acquisition of special operations—peculiar material, supplies, and services.”¹⁵ No other combatant commander has been given direct congressional authority to develop and acquire equipment for their forces. Under this law, SOCOM developed its own version of JCIDS—the Special Operations Forces Capabilities Integration and Development System (SOFCIDS). SOFCIDS is a streamlined version of the JCIDS process, wholly owned by the SOCOM commander for SOF-particular acquisition. SOFCIDS reduces the requirements of JCIDS documents and streamlines the coordination process within the command. Even with SOCOM’s acquisition exceptions, the deliberate acquisition process is unable to support the rapidly changing needs of the current war fighter. Based on these unique needs, each service and COCOM developed its own rapid acquisition process.

Rapid Acquisition

There are over 20 different urgent needs processes throughout the DOD, Joint Staff, COCOMs, and services.¹⁶ Each process carries varying and overlapping definitions of rapid acquisition. This paper discusses the documents, approval authority, funding, and timelines of the joint, Army, Air Force, Navy, and SOCOM rapid acquisition processes.

Joint Rapid Acquisition

Joint rapid acquisition is centered on fulfilling a combatant commander’s joint urgent operational need (JUON). A JUON addresses “urgent operational needs that: (1) fall outside of the established Service processes; and (2) most importantly, if not addressed immediately, will seriously endanger personnel or pose a major threat to ongoing operations.”¹⁷ The governing regulation for joint rapid acquisition is Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3470.01, *Rapid Validation and Resourcing of Joint Urgent Operational Needs (JUONS) in the Year of Execution*, which details the JUON process and provides an overview for each service’s rapid acquisition process.¹⁸ The timeline to deliver a JUON is normally 120 days to two years to provide the 70–80 percent solution.¹⁹ If the material or logistics solution is needed in less than 120 days, the JUON is designated as an immediate war fighter need (IWN) and handled by the Joint Rapid Acquisition Cell (JRAC) for oversight of the process.²⁰ The JRAC tracks the IWN and provides updates to the deputy secretary of defense. The funding for an IWN has been sourced primarily from the Iraq Freedom Fund, which has been designated by Congress for the

funding of the wars in Iraq and Afghanistan.²¹ In contrast, there is no designated funding for a JUON, where the solution takes longer than 120 days. Funding for JUONs come from sources within the COCOM or a designated service. Funding approval for both the JUON and IWN comes from Budget Office Director's Board, cochaired by the OSD comptroller and the J-8, deputy for resources and acquisition.²² Based on the nature of the JUON or IWN, the J-8 designates a lead service to provide a material or logistic solution for the war fighter.

Army Rapid Acquisition

The core of the Army's rapid acquisition process is the operational needs statement (ONS) process and the Rapid Equipping Force (REF). Army field commanders and combatant commanders submit an ONS to fulfill an "urgent need for a materiel solution to correct a deficiency or to improve a capability that impacts upon mission accomplishment."²³ The ONS is submitted via the Equipment Common Operation Picture (ECOP), an information technology tool. ECOP allows commanders to submit and track ONS documentation and approval of the capability.²⁴ The ONS is validated and authorized by Headquarters, Department of the Army (HQDA). If the cost of the material solution is expected to be under \$100,000, commanders can submit a "10-liner" to the REF.²⁵ The Army established the REF in 2002 to rapidly respond to war fighter needs. The 10-liner consists of the following: (1) problem, (2) justification, (3) system characteristics, (4) operational concept, (5) organizational concept, (6) procurement objective, (7) support requirements, (8) availability, (9) recommendation, and (10) coordination accomplished.

The Army G3 (Operations Branch) runs the REF process, and the Army vice chief of staff normally approves solutions. Commercial off-the-shelf (COTS) solutions generally take three to six months to field, whereas new technology may take 12-18 months.²⁶ The REF and ONS do not have a specific funding source but are normally funded through a number of joint and Army research, development, test, and evaluation funding based on the material solution (e.g., robotic or IED funding). The goal of the Army's rapid acquisition process is to quickly field the 80 percent solution to meet the war fighter's need versus waiting longer for the 100 percent solution.²⁷

Air Force Rapid Acquisition

The Rapid Response Process (RRP) is the Air Force's rapid acquisition method, detailed in Air Force Instruction (AFI) 63-114, 12 June 2008. The RRP begins when a major command or COCOM identifies an urgent operational need (UON). The requirements of the UON are

normally documented in a combat capability document and submitted to the assistant secretary of the Air Force for acquisition (SAF/AQX), the focal point for the RRP. No specific funding exists for the RRP; SAF/AQX recommends sources, and the chief of staff, US Air Force (CSAF), approves them.²⁸ According to AFI 63-114, "Capability must be fielded in time to impact an ongoing conflict or a crisis (nominally within 60 days of initial warfighter request)."²⁹ SAF/AQX represents the Air Force on the JRAC, and the RRP is the process used when the Air Force is assigned the responsibility of fulfilling a JUON.

Navy Rapid Acquisition

The Urgent Needs Process (UNP) is the Navy's rapid acquisition system, outlined in Secretary of the Navy Notice (SECNAVNOTE) 5000, 12 March 2009. A combatant, Navy, or Marine commander identifies an urgent need, defined as "an exceptional request . . . for an additional warfighting capability critically needed by operating forces conducting combat or contingency operations. Failure to deliver the capability requested is likely to result in the inability of units to accomplish their missions or increases the probability of casualties and loss of life."³⁰ The goal of the UNP is to provide the war fighter with a fielded solution in less than 24 months. Based on the technology readiness of the solution, the Navy employs a range of acquisition strategies to include COTS/government off-the-shelf (GOTS) procurement, rapid deployment capability for slightly modified COTS/GOTS, and rapid deployment and development when no commercial solution is available.³¹ The chief of naval operations (CNO) is the approval authority for the UNP, and the CNO staff is the focal point for the process. No separate funding exists for the UNP; the CNO approves funding sources. Similarly to the other services, the UNP supports the JUON process when the Navy is designated as the lead service to field the JUON.

SOCOM Rapid Acquisition

SOCOM's rapid acquisition process consists of the Special Operations Forces Capabilities Integration and Development System-Urgent (SOFCIDS-U). As described earlier, SOCOM is unique among COCOMs because Congress has granted it the ability to acquire its own solution to meet war fighter needs. SOCOM's rapid acquisition process is governed by USSOCOM Directive 71-4, *Special Operations Forces Capabilities Integration and Development System*, which states that "SOFCIDS-U may be used when a SOF unit, either deployed or during pre-deployment, identifies an urgent and compelling capability gap or requirement derived from combat survivability deficiency or risk to op-

erational success."³² SOFCIDS-U is initiated through the chain of command by a combat mission needs statement (CMNS). The CMNS process is well defined in USSOCOM Directive 71-4 and consists of defining the capability gap, environment, material approach, concept of operations, and an analysis summary. Once the CMNS is submitted, the SOCOM J-8 convenes a rapid response team (RRT) within 24 hours.³³ The RRT provides expeditious review and coordinates the solution and fielding of the needed capability. The deputy SOCOM commander normally approves the solution, and designated CMNS funding provides resources. If CMNS funding is not available, funding may be sourced from other programs.³⁴ The goal of the SOFCIDS-U is to field the solution within 180 days of CMNS submittal. The solution is planned to be sustainable for the duration of the need or one year, whichever is less.³⁵ Sustainment of the solution expires after one year unless a CDD is approved through the normal SOFCIDS process. Other than the joint rapid acquisition process, the SOFCIDS-U is the only process with a separate funding source. Also, based on my review of existing documentation, the SOCOM rapid acquisition process is the most detailed and well defined.

The table below summarizes the numerous joint, Army, Air Force, Navy, and SOCOM rapid acquisition processes:

Table 1. Summary of rapid acquisition processes

	<i>Joint</i>	<i>Army</i>	<i>Air Force</i>	<i>Navy</i>	<i>SOCOM</i>
<i>Rapid acquisition process name</i>	Joint urgent operational need	Operational needs statement & Rapid Equipping Force	Rapid Response Process	Urgent Needs Process	SOFCIDS-U
<i>Primary document</i>	CJCSI 3470.1 (15 July 2005)	ECOP User's Guide	AFI 63-114 (12 June 2008)	SECNAVNOTE 5000 (15 March 2009)	USSOCCOM D 71-4 (9 June 2009)
<i>Approval</i>	Budget Office Director Board	HQDA	CSAF	CNO	Deputy SOCOM
<i>Funding</i>	No specific fund	No specific fund	No specific fund	No specific fund	CMNS fund
<i>Timeline to IOC</i>	IWN—120 days JUON—120 days–2 years	REF—90–360 days ONS—90 days–2 years	60 days	Less than 2 years	180 days–2 years
<i>Solution goal %</i>	70–80%	80%	None specified	None specified	80%

Defense Science Board Recommendations

Only five of the more than 20 rapid acquisition processes have been discussed in this paper. As shown, there are numerous documents, timelines, definitions, approval authorities, and funding sources for rapid acquisition. In response to the numerous processes, the undersecretary of defense for acquisition, technology, and logistics directed the DSB to study the situation and present recommendations. In July 2009, the DSB published the study *Fulfillment of Urgent Operational Needs*. The DSB makes five specific recommendations for the DOD rapid acquisition process:

1. The Secretary of Defense should formalize a dual acquisition path (deliberate and rapid).
2. Executive and legislative branches must establish a fund for rapid acquisition and fielding.
3. The Secretary of Defense should establish a new agency: the Rapid Acquisition and Fielding Agency (RAFA).
4. Initial funding and billets for RAFA will be based on absorbing and integrating existing programs and organizations.
5. DOD should establish a streamlined, integrated approach for rapid acquisition.³⁶

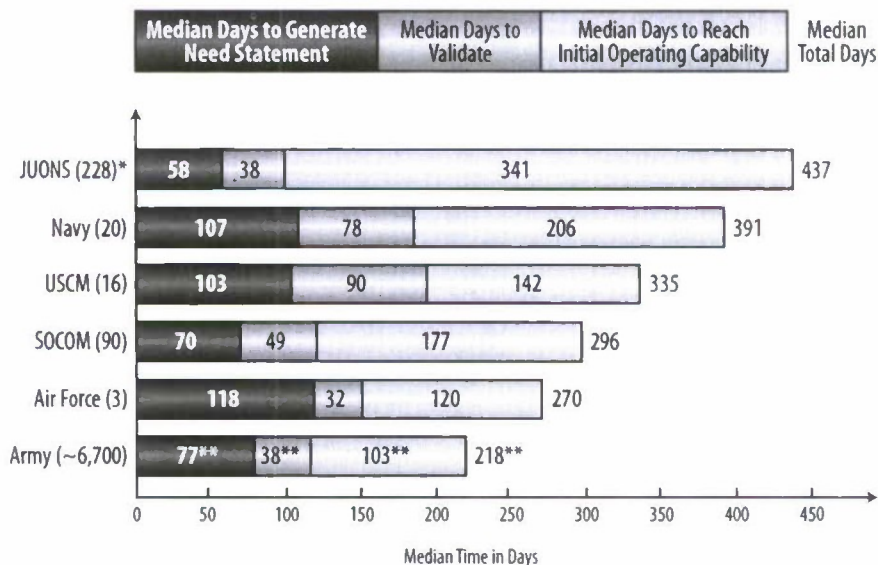
The DSB's final recommendation on "a streamlined, integrated approach for rapid acquisition" is a key finding and the premise of this paper. The DSB highlights the need for a process to validate the COCOM's request in 48 hours and then to use a tightly coordinated acquisition and funding framework to meet the COCOM's need.³⁷ Specifically, under the DSB's recommendations, the RAFA would concurrently assign acquisition responsibility to an appropriate organization that would analyze alternatives, approve funding, and work with the COCOM for concept of operations approval and IOC. This course of action would produce a solution for the COCOM within two to 24 months and is intended to have maximum flexibility to minimize time.³⁸ This paper suggests that SOCOM's SOFCIDS-U process is the benchmark to fulfill this streamlined, integrated approach for all services. The strengths and weaknesses of SOCOM's rapid acquisition process are examined next.

USSOCOM's Rapid Acquisition Success

This discussion supports the first half of my recommendation: SOCOM's rapid acquisition process offers a rapid acquisition benchmark that should be adopted throughout the military.

SOCOM's SOFCID-U process stands out for one main reason: results. Based on data that the DSB has collected, if the goal of any urgent needs process is to get a capability into the war fighter's hands, the SOFCID-U process has the lowest time to IOC for the war fighter. The data below were submitted by each major rapid acquisition organization and compiled by the DSB (see fig. 2).

The data indicate that SOCOM's process takes an average of 296 days to become IOC. Upon initial investigation, it appears the Army takes the least time to IOC. However, the Army process is skewed by 94 percent of the urgent needs being met by a redistribution of inventory. With only three UONs, the Air Force process does not meet requirements for statistical significance. Also, according to AFI 63-114, the Air Force goal is to fulfill the urgent need within 60 days. Based on the three submitted UONs, it takes 118 days just to generate the needs statement. With a lack of significant Army and Air Force data, SOCOM bears the shortest IOC time of 296 days. Although it appears that SOCOM's process is the fastest based on technicalities, it is also



*Numbers in parentheses indicate the number of needs statements evaluated.

**More than 94 percent of Army ONSs (~6,400) were for redistribution of inventory, which skews data to shorter times.

Figure 2. Urgent need data. (Reprinted from Defense Science Board [DSB] Task Force, *Fulfillment of Urgent Operational Needs* [Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, July 2009], 22.)

the only service or COCOM with a designated funding source and the congressional authority to acquire its own solution. This frees SOCOM from bureaucracy that exists in the other processes. These strengths of fastest to IOC, designated funding, and the ability to acquire its own solution are not without a few weaknesses.

The weakness of the SOFCIDS-U process is that it is only intended to sustain a war fighter solution for one year. Other urgent needs processes did not specify a specific length of time for sustainment. Sustaining a solution for one year cuts down on the planning and scope required for the solution and decreases the time necessary to field the capability. However, this limits the ability to perform a "system of systems" approach to acquisition, especially in the area of logistics. Ultimately, the war fighter desires the capability solution to integrate into other war fighting systems to enhance mission effectiveness. The logisticians want the solution to integrate into the existing supply and sustainment system. The planning required for the complete system of systems acquisition approach does not meet the war fighter's urgent timeline. However, the war fighter knows that the 80 percent solution now is better than the 100 percent solution years from now. The compromise is that under the SOFCIDS-U process, if the solution needs sustainment beyond a year, a CDD must be submitted and approved. Fortunately, the SOCOM CDD under the SOFCIDS has fewer requirements than a CDD under the JCIDs process.

In summary, SOCOM's rapid acquisition process rises to the top based on IOC results data, specified funding, and the ability to manage its own acquisition. This makes SOCOM's SOFCIDS-U process a DOD benchmark for streamlined acquisition. Based on SOCOM's success, a similar process could be used to acquire and sustain a limited major weapon system.

Two-Year Limited Major Weapon System Acquisition

Funding changes could support my premise that SOCOM's rapid acquisition process is a model for acquiring a limited MWS, such as a light attack aircraft, in less than two years. Indeed, research shows that the Air Force has already accomplished something similar.

In a recent article, Gen David Deptula, the current deputy CSAF for intelligence, surveillance, and reconnaissance (ISR), states "We need to make accelerated acquisition the norm. An example is the MC-12W [ISR aircraft]. The first was delivered in less than eight months."³⁹ The MC-12 Project Liberty was delivered in less than eight months from contract to combat missions. General Deptula goes on to say,

We are in an information age, but we have an industrial-age acquisition system. We have to be more agile in this regard because our adversaries are not limited by the same bureaucratic and legislative constraints that we have. Al Qaeda doesn't have a JCIDS (Joint Capabilities Integration and Development System) process. If we're going to succeed, we have to operate inside our adversaries' decision loop. To do that is going to require significant changes not just to the acquisition processes we built in the last century, but to our decision-making processes.⁴⁰

Using streamlined acquisition processes, Big Safari, the Air Force's ISR program office, turned a COTS King Air into an ISR platform to meet the war fighter's need in under a year. Big Safari's success is built on having a small acquisition team closely integrated with a contractor, in this case, L-3 Communications Corporation. Unfortunately, this streamlined process has yet to be institutionalized for programs outside of Big Safari. The following topics outline some requirements for institutionalizing rapid acquisition.

Entry Criteria

To develop a limited MWS in under two years, the solution needs to meet three specific criteria: (1) stable requirements, (2) a COTS platform, and (3) stable technology for systems integration. First, to meet an urgent war fighter need, the requirements must be thoroughly vetted before acquisition and not change during the rapid acquisition process. SOCOM would be unable to achieve its average of 296 days to IOC with changing requirements. Second, the primary platform needs to be a COTS item currently in production. For example, in the case of a light-attack weapon system, the primary platform could be the T-6 Texan II. The Air Force uses these aircraft for primary training, and Hawker-Beach is still producing them. Third, any technology added to the weapon system needs to be stable technology. Using the Navy guidance for rapid acquisition, the solution would require an 8-9 technology readiness level (TRL) or better.⁴¹ For example, in the case of weaponizing the T-6, a production small diameter bomb would be integrated versus developing a new weapon.

SOFCIDS-U Additions

Minor additions to the SOFCIDS-U process are required to support two-year limited MWS acquisition. Currently, the SOFCIDS-U process does not mandate a systems engineering plan, which would outline the cradle-to-grave implications of the MWS and integration with other weapon systems. A systems engineering plan needs to be developed for any MWS. A subset of the systems engineering plan is the supportability plan. Currently, the SOFCIDS-U process intends to

support a solution for only one year and does not include a robust sustainment plan. To support an MWS, a supportability plan would need to be developed for the intended life of a weapon system. Although these two items would increase the planning time upfront, they would provide the war fighter a sustainable system into the future.

Timeline

The current SOFCIDS-U process delivers capability to the war fighter in an average of 296 days; Big Safari was able to deliver the MC-12 in under a year. The limited MWS acquisition team could use either process as a timeline model. The crucial factors for maintaining an acquisition timeline are a small team of highly experienced acquisition personnel with an intimate oversight relationship with the contractor. As an example, Big Safari assigns program office personnel to oversee its contractor, L3 Communications, in Greenville, Texas.

Funding

Rapid acquisition funding needs to be a priority for the DOD and Congress. Currently, the SOFCIDS-U process uses CMNS funding specifically allocated to fulfill urgent needs. This should be accepted as the service model to fulfill urgent needs, including a limited MWS. Congress also provides the COCOM with the "Combatant Commanders Initiative Fund (CCIF) as a means to finance unforeseen contingency requirements critical to combatant commanders' joint warfighting readiness and national security interests."⁴² This fund is managed by J-7 and could be used as a source for a limited MWS. Institutionally, Congress has recognized the need for creating funding to meet urgent war fighting needs. However, other than SOCOM, no specific service is authorized such a fund. Each service normally resorts to its own sources to meet war fighter needs. The practice of robbing other programs to pay for urgent needs disrupts other acquisition programs and ultimately increases the cost to the taxpayer. The DSB recommended that 0.5 percent of the DOD budget be set aside for rapid acquisition, and such a fund could be used to procure a limited MWS.⁴³ The key for funding a limited MWS would be military transparency with Congress on how the money is managed and spent.

To summarize, the SOFCIDS-U provides a model for acquiring a limited MWS, but not the only model. Big Safari's acquisition process could also be leveraged to acquire an MWS, provided the MWS meets specific entry criteria and incorporates systems engineering planning. The acquisition team also needs to maintain an intimate contractor relationship as well as work with Congress on funding.

Recommendations

Based on the research presented, I propose three recommendations:

1. *Rapid acquisition must be consolidated into one process.* I agree with the DSB findings that over 20 rapid acquisition processes are unwieldy and redundant. As shown, with the myriad of terms and processes between SOCOM, the Air Force, Navy, and Army, rapid acquisition is disjointed and inefficient. Like the DSB, I recommend creating and codifying a separate deliberate and rapid acquisition system. This would identify a single rapid acquisition process and bring clarity to cloudy process and funding issues.
2. *SOCOM's rapid acquisition process should be used as a benchmark.* SOCOM's SOFCIDS-U process offers a streamlined acquisition process with proven delivery to the war fighter. SOCOM's process should be adopted by OSD as the single rapid acquisition process.
3. *Future acquisition of limited major weapons systems (e.g., light attack aircraft) should use rapid acquisition processes.* Acquisition of a limited MWS to support the war fighter should use a rapid versus deliberate acquisition process. Taking five, 10, or 20 years to field a system is unacceptable in today's rapidly changing environment. Our acquisition system must adapt to defeat the threat. MWSs that meet specific entry criteria—stable requirements, COTS platform, and mature systems integration (8–9 TRL)—should be considered for rapid acquisition. The SOFCID-U or Big Safari processes offer benchmarks for limited MWS acquisition.

Conclusion

In 2008 the Government Accountability Office published four main causes for defense acquisition delivering war fighter capabilities an average of 21 months late: unstable requirements, frequent program manager turnover, overreliance on contractors to perform roles previously performed by government employees, and difficulty managing software.⁴⁴ While the DOD attempts to transform deliberate acquisition to repair the aforementioned problems, the need for rapid acquisition to support the war fighter has been recognized. Although the F-35 is in its 12th year of development with IOC still years away, rapid acquisition success exists with programs like the MRAP and

MC-12. All services desire to get the necessary equipment into the war fighter's hands to defeat the enemy, but no DOD institutionalized processes exists for this critical endeavor.

This paper outlined the difference between deliberate and rapid acquisition; discussed the joint, Army, Air Force, Navy, and SOCOM rapid acquisition processes; argued the success of the SOCOM model; and explored the possibility of acquiring a limited MWS with a rapid acquisition process. My proposal was that SOCOM's rapid acquisition process offers a rapid acquisition benchmark that should be adopted throughout the military and that could be used to acquire a limited MWS (e.g., a light attack aircraft) in less than two years. The limited data showed that SOCOM's rapid acquisition process consistently fulfills urgent needs in the least amount of time—296 days. However, when proposing a process to acquire a limited MWS, both SOCOM and Big Safari stand out as best practices.

This paper made three specific recommendations: rapid acquisition must be consolidated into one process, SOCOM's rapid acquisition process should be used as a benchmark, and future acquisition of limited major weapons systems (e.g., light attack aircraft) should use rapid acquisition processes. These recommendations are congruent with Defense Secretary Robert Gates's comments during a speech in July 2009: "The Defense Department needs to think about and prepare for war in a profoundly different way than what we have been accustomed to throughout the better part of the last century. What is needed is a portfolio of military capabilities with maximum versatility across the widest possible spectrum of conflict. As a result, we must change the way we think and the way we plan—and fundamentally reform—the way the Pentagon does business and buys weapons."⁴⁵

Changing the way the Pentagon buys weapons is crucial to our national security. Using SOCOM's processes as a model is a proven way to meet the war fighter's needs and posture our military's acquisition system to defeat future threats.

Notes

1. James Rothenflue and Marsha Kwolek, eds., *Streamlining DOD Acquisition: Balancing Schedule with Complexity*, Occasional paper no. 57-59 (Maxwell AFB, AL: Center for Strategy and Technology, Air War College, 2006), 32.

2. Statement of Michael J. Sullivan, director, acquisition and sourcing management, in *Defense Acquisitions: Rapid Acquisition of MRAP Vehicles: Testimony before the House Armed Services Committee, Defense Acquisition Reform Panel* (Washington, DC: Government Accountability Office [GAO], 8 October 2009), GAO-10-155T, 1.

3. *Ibid.*, 1.

4. *Ibid.*, 6.

5. *Ibid.*

6. DSB Task Force, *Fulfillment of Urgent Operational Needs* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, July 2009), iii.
7. *Ibid.*, xii.
8. Moshe Schwartz, *Defense Acquisitions: How DOD Acquires Weapon Systems and Recent Efforts to Reform the Process* (Washington, DC: Congressional Research Service, 2010), 17.
9. *Ibid.*, 17.
10. DSB Task Force, *Fulfillment of Urgent Operational Needs*, 2.
11. *Ibid.*, 4.
12. *Ibid.*
13. Schwartz, *Defense Acquisitions*, 4.
14. US GAO, *Defense Acquisitions: An Analysis of the Special Operations Command's Management of Weapon System Programs: Report to the Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services, U.S. Senate* (Washington, DC: GAO, June 2007), GAO-07-620, 1.
15. US Code, Title 10, "Armed Forces," chap. 6, sec. 167, "Unified Combatant Command for Special Operations Forces," 4A, 8 January 2008.
16. DSB Task Force, *Fulfillment of Urgent Operational Needs*, 9.
17. *Ibid.*, 10.
18. CJCSI 3470.01, *Rapid Validation and Resourcing of Joint Urgent Operational Needs (JUONS) in the Year of Execution*, 15 July 2005.
19. William Beasley, "Institutionalization of DOD Processes in Support of Immediate Warfighter Needs" (professional student paper, Army War College, 11 August 2009), 10.
20. CJCSI 3470.01, *Rapid Validation and Resourcing*, A-5.
21. Beasley, "Institutionalization of DOD Processes," 10.
22. CJCSI 3470.01, *Rapid Validation and Resourcing*, GL-2.
23. *Ibid.*, 12.
24. Beasley, "Institutionalization of DOD Processes," 2.
25. DSB Task Force, *Fulfillment of Urgent Operational Needs*, 13.
26. *Ibid.*, 13.
27. "U.S. Army Rapid Equipping Force," REF Web site, <http://www.ref.army.mil/textonly/default.html#about>.
28. AFI 63-114, *Rapid Response Process*, 12 June 2008, 3.
29. *Ibid.*, 6.
30. SECNAVNOTE 5000, "Urgent Needs Process," 12 March 2009.
31. *Ibid.*, 5.
32. USSOCOM Directive 71-4, *Special Operations Forces Capabilities Integration and Development System (SOFICIDS)*, 9 June 2009, 23.
33. *Ibid.*, C-7.
34. *Ibid.*, 23.
35. *Ibid.*, C-1.
36. DSB Task Force, *Fulfillment of Urgent Operational Needs*, x-xii.
37. *Ibid.*, 39.
38. *Ibid.*
39. David A. Deptula, "Fast Forward," *Defense Technology International*, December 2009, 46.
40. *Ibid.*
41. SECNAVNOTE 5000, "Urgent Needs Process," 5.
42. Beasley, "Institutionalization of DOD Processes," 15.
43. DSB Task Force, *Fulfillment of Urgent Operational Needs*, 33.

44. Statement of Michael J. Sullivan, director, acquisition and sourcing management, in *Defense Acquisitions: Results of Annual Assessment of DOD Weapon Programs: Testimony before the Committee on Oversight and Government Reform and the Subcommittee on National Security and Foreign Affairs, House of Representatives* (Washington, DC: GAO, 29 April 2008), GAO-08-674T, 2-3.

45. Secretary of Defense Robert Gates (speech, Economic Club of Chicago, 16 July 2009), news transcript, DOD Web site, <http://www.defense.gov/transcripts/transcript.aspx?transcriptid=4445>.

Abbreviations

AFI	Air Force instruction
AOA	analysis of alternatives
ATF	Advanced Tactical Fighter
BES	budget estimation submission
CDD	capability development document
CJCSI	chairman of the Joint Chiefs of Staff instruction
CMNS	combat mission needs statement
CNO	chief of naval operations
COCOM	combatant command
COTS	commercial off-the-shelf
CSAF	chief of staff, US Air Force
DOD	Department of Defense
DSB	Defense Science Board
ECOP	Equipment Common Operation Picture
FCB	Functional Capabilities Board
GAO	Government Accountability Office
GOTS	government off-the shelf
HQDA	Headquarters, Department of the Army
ICD	initial capabilities document
IED	improvised explosive device
IOC	Initial Operational Capable/Capability
ISR	intelligence, surveillance, and reconnaissance
IWN	immediate war fighter need
JCIDS	Joint Capabilities Integration and Development System
JCS	Joint Chiefs of Staff
JRAC	Joint Rapid Acquisition Cell
JUON	joint urgent operational need
MDD	materiel development decision
MRAP	mine-resistant ambush protected
MWS	major weapon system
O&S	operating and support
ONS	operational needs statement
OSD	Office of the Secretary of Defense
POM	program objective memorandum
PPBE	Planning, Programming, Budgeting, and Execution
RAFA	Rapid Acquisition and Fielding Agency
REF	Rapid Equipping Force
RRP	Rapid Response Process
RRT	rapid response team
SECNAVNOTE	Secretary of the Navy Notice

SOFCIDS	Special Operations Forces Capabilities Integration and Development System
TRL	technology readiness level
UNP	Urgent Needs Process
UON	urgent operational need
USSOCOM	United States Special Operations Command

Developing a Situation Awareness Environment for the Distribution Process Owner

Recommendations for US Transportation Command

*Lt Col James Michael Doolin
USAF Reserve/YC-3, DAF civilian**

This study addresses three basic questions: (1) what should be the endgame objective for distribution process owner (DPO) situation awareness (SA)? (2) what is in the critical path to achieve the objective? and (3) how does the DPO get to the objective end state? DPO decision makers need to have confidence in their information for successful SA. Integral to this trust is the requirement for accurate, timely, and relevant information; this leads to confident and actionable decision making.¹ Decisions based on confidence in trusted information lead, in turn, to effective and efficient logistics actions in support of global Department of Defense (DOD) operations. Therefore, US Transportation Command (USTRANSCOM) should pursue information confidence as the endgame objective for DPO SA. That assertion leads to the thesis that the DPO should articulate the need for information confidence as its fundamental requirement for an effective and successful SA environment. Considering information confidence as its primary objective will drive the DPO to understand all of the necessary critical-path elements to achieve success.

In addressing how the DPO reaches its objective, this study provides three macrolevel recommendations for USTRANSCOM:

1. leverage pertinent SA industry research and adopt user-centered design as the foundation for a DPO SA environment;
2. adopt a knowledge-centric approach to DPO culture by defining ownership of information, processes, and business rules; and
3. address critical-path concerns for DPO SA through appropriate governance forums.

*Col Alvin M. Lowry, Jr., USAF, was the essay advisor for this paper.

These broad findings highlight the need for the DPO to advocate development of information-confidence factors as a microlevel recommendation for its SA environment.

A basic definition of *information-confidence factors* is a visual, audible, or textual indicator that communicates a level of confidence (low, medium, or high, based on appropriate business rules) for a given element of SA information. The basic business rules associated with information-confidence factors should be based on providing timely, accurate, and relevant information to the decision maker (see fig. 1).²

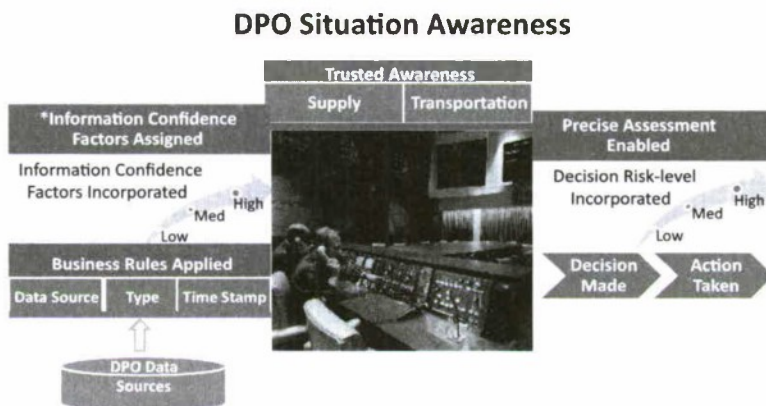


Figure 1. Incorporating information-confidence factors for SA

As a foundation to understanding the concept of information confidence, other elements should be addressed. This study introduces some of these, for instance, the basic process of decision making within the DPO SA environment. Its major premise, however, is that information confidence lies within the critical path of successfully providing actionable (decision-ready) information and, therefore, should be an integral part of any best-practice-driven solution (see fig. 2).

This research provides recommendations for USTRANSCOM leaders to consider as they embark upon a major business transformation effort called “Agile Transportation for the 21st Century” (AT21) and rolls out information technology (IT)-enabled capabilities as part of its corporate services vision.³ The DPO SA environment will be integral to successful realization of the AT21 vision. USTRANSCOM commander, Gen Duncan J. McNabb, noted in a 27 March 2009 statement before the Senate Armed Services Committee that “when fully operational, AT21 will provide the warfighter full distribution pipeline visibility and enable throughput management at critical

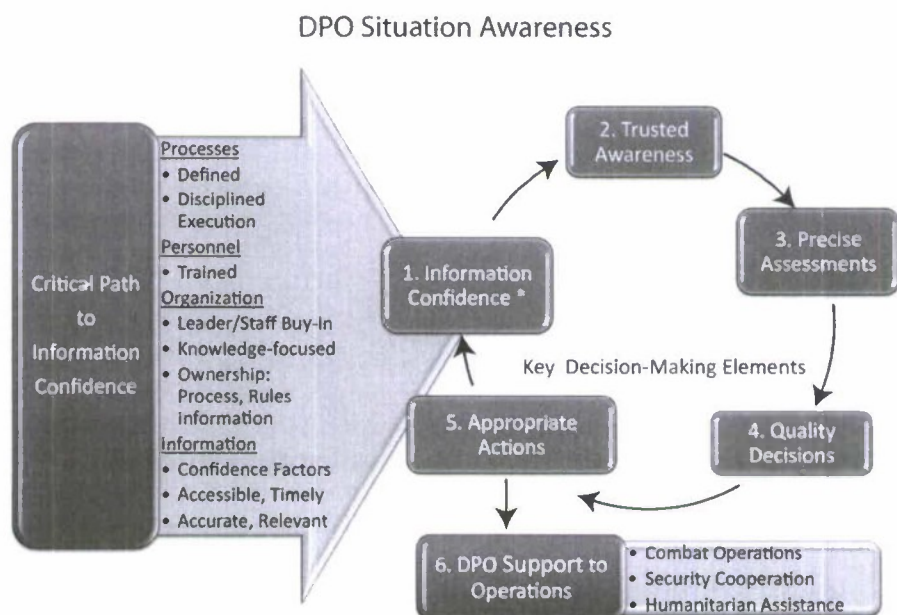


Figure 2. DPO SA decision-making model (*information confidence is the first step)

ports and waypoints around the world.”⁴ Undoubtedly, the success of AT21 will depend upon confidence in the underlying information.

Background

This study leverages specific research centered upon designing for SA and human factors engineering as the basis for its recommendations for USTRANSCOM. As a further clarification, one should consider that the distribution process is part of the greater domain of logistics within the DOD. As such, logistics-centered topics are directly relevant to the DPO discussions herein. A basic definition of SA is required to establish the baseline discussion. There are at least 26 SA definitions, according to a 2001 systematic classification of SA definitions by Richard Breton and Robert Rousseau.⁵ The well-known Endsley definition is used herein: “the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future.”⁶

This translates well for the DPO environment and the capabilities envisioned for AT21. Consider Endsley’s definition of SA as it relates to the capability of AT21 to provide distribution pipeline visibility and

enable throughput management. "The perception of the elements in the environment" relates well to visibility of assets within the distribution pipeline such as material supplies, transportation conveyances (a ship, plane, truck, or railcar), supply depots, and ports of embarkation and debarkation. "Within a volume of time and space" translates nicely to the location of a transportation conveyance and timeliness of the relevant information to enable throughput management of people, equipment, and supplies. And finally, "the comprehension of their meaning and the projection of their status in the near future" enable visibility and planning for throughput management by reporting whether the item of interest is expected to arrive early, on time, late, or not at all.

The Importance of Information Confidence

One key to successful logistics planning and execution is the need for actionable information. For information to be actionable, however, the decision maker must be confident in the information being presented. Confidence is fundamentally achieved when the decision maker accepts that the information being acted upon meets the requirements of timeliness, accuracy, and relevance. To deliver these requirements for decision makers, it is necessary to develop and present information-confidence factors (high, medium, or low) in the SA environment. The decision maker can then consider a level of risk (low, medium, or high) associated with the decision to be made and decide—based on the confidence and risk levels—whether or not to make a decision that will lead to a subsequent action. The importance of information confidence in the decision-making process leads one to deduce that information-confidence factors are in the critical path for the logistics decision maker. Therefore, information-confidence factors should be addressed as part of the solution to providing situation awareness for USTRANSCOM (see fig. 3).

To better understand the importance of information confidence, consider the example of a key logistics decision affecting the safety and lives of war fighters during Operation Iraqi Freedom.⁷ In 2004 enemy threats evolved as insurgents strategically placed improvised explosive devices (IED) along roads traveled by US forces. The interim solution to help counter that threat was to ship add-on armor for installation on US vehicles in Iraq. The planners in the joint operations center at USTRANSCOM were working diligently with their counterparts at the USAF's Air Mobility Command (AMC) and the Army's Military Surface Deployment and Distribution Command (SDDC) to ensure the most expeditious shipping solution (air and/or surface).

DPO Situation Awareness

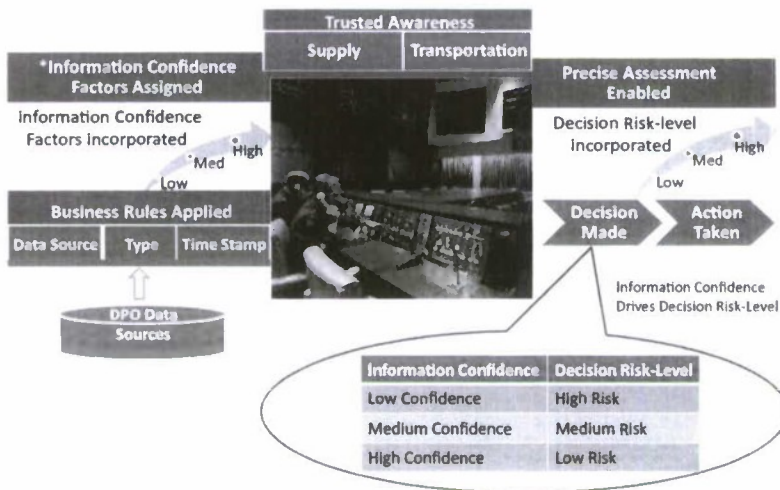


Figure 3. Relationship of information confidence to decision risk level

Although planners were leveraging all of their IT systems capabilities, there was no automated way to indicate a level of confidence in the information associated with timeliness, accuracy, or relevance. Conflicting information was available, and much of it was being validated verbally by a "human in the loop" prior to final decisions for shipment to Iraq by air or surface. Traditionally, critical logistics decisions have been made only after checking and double-checking information gained from the various IT systems available across the department, followed by verbal confirmation on the agreed-upon information from all parties involved.

By implementing information-confidence factors associated with corresponding risk levels, decision makers can focus attention on the most critical decisions, trusting business-rule-based software to provide confidence and risk levels versus having to manually engage in the process every time. The bottom-line benefit to users is that they can allow software to perform confidence checks (starting with the least-critical decisions). That, in turn, frees decision makers to perform more critical analysis for the higher-risk decisions. Therefore, it is necessary for USTRANSCOM to define, develop, and field the capability to display information-confidence factors leading to trusted situation awareness and effective logistics decision making.

The Critical Path to DPO Situation Awareness

How does the DPO reach the objective end state of information confidence? To answer that question, this study highlights other critical-path requirements to illustrate how information confidence drives effective logistics decision making. The critical path to deliver actionable or decision-ready information contains DOD-level concerns, as well as those within USTRANSCOM's direct sphere of influence as the DPO and distribution portfolio manager for DOD distribution.

USTRANSCOM should continue to address concerns with the Office of the Secretary of Defense (OSD), the Joint Staff, the military services, and agencies such as the Defense Logistics Agency (DLA), Defense Information Systems Agency, and others as appropriate to realize the stated SA environment end game. Of the many elements external to the DPO, three stand out as essential for success within the military services' purview to organize, train, and equip its forces: (1) the need for trained personnel engaged in well-defined and understood DOD logistics business processes, (2) a disciplined approach to information gathering and reporting, and (3) universal access to information through appropriate fielding of IT.⁸

Logistics personnel are key to successful delivery of trusted SA for decision makers. Therefore, the proper mechanics for conducting the business of logistics should be inherent in training, and the impact of shortcutting processes that support logistics visibility should be understood. For example, failure to ensure that cargo is appropriately marked with accurate shipping labels or radio-frequency identification (RFID) tags causes information gathering and reporting problems within the supply and transportation domains ranging from rework at the next location to reordering a critical supply item that might be needed for a mission-essential task or operation. Trained personnel must have the discipline to ensure timely gathering and reporting of information to enable information confidence for decision makers and to guard against "the possible loss of life and equipment resulting from poor planning" based on incomplete or inaccurate logistics information.⁹ Along with training and disciplined execution of logistics processes comes the requirement to ensure complete access to the necessary IT solution that supports execution of logistics duties. Today, access to logistics information via Web-enabled services and applications is prolific through the fielding of capabilities like the Global Combat Support System-Joint Common Operating Picture Deployment and Distribution (GCSS-J COP D2) structure. All new IT services should be Web-enabled to ensure the widest access possible.

The scope of this research does not allow in-depth discussion regarding the importance of these DOD-level critical-path items or others like them. However, the DPO should pursue their accomplishment to realize its objective of a successful SA environment. It should also continue to leverage governance forums like the Distribution Executive Board and the Distribution Transformation Task Force to address essential elements within the critical path of providing decision-ready information for decision makers.¹⁰

USTRANSCOM-Centric Critical-Path Discussion

Three DPO-centric elements are necessary for USTRANSCOM to achieve success: senior leader buy-in and staff advocacy; ownership of processes, information, and business rules; and adopting a knowledge-centric culture.

Senior Leader Buy-in and Staff Advocacy

Delivering a secure SA environment for the DPO requires that senior leaders are an integral part of achieving the endgame objective. This is apparent from General McNabb's statement to the Senate Armed Services Committee. In addition to senior leader buy-in, the power of the entire staff should be focused on the same goals. Success is predicated on a horizontal, integrated team approach to planning and executing the solution. Isolated requirements development and materiel solution design and fielding should be viewed as counter-productive to a successful outcome.

Ownership of Processes, Information, and Business Rules

To achieve the desired confidence in information necessary for logistics decision makers in a future DPO SA environment, one must first ensure that ownership of major business processes and the information supporting those processes is clearly defined and that those identified as responsible are empowered, resourced, and engaged accordingly. For example, who owns the strategic surface transportation process from the seaport of embarkation to the other end at the seaport of debarkation? One can argue that ownership is split between two of USTRANSCOM's component commands, the Army's Surface Deployment and Distribution Command (SDDC) and the Navy's Military Sealift Command (MSC), depending on the type of sealift employed (contract or organic). This is one example of the complexities associated with the duties of distribution process owner. Clearly understanding who owns a business process is critical to

determining other key relationships fundamental to the discussion of information confidence.

The process owner should also own the information related to that process and be solely responsible for updating and reporting that information within the decision-making environment. In the current DPO environment, a user can determine which information source (IT system) to access for logistics information. This can, and does, result in different answers to the same question. To eliminate this occurrence, an integral first step in the right direction is to assign responsibility or ownership of information to an organization. Next comes designating an authoritative information source and providing a time stamp associated with currency of the information. This should enable tagging of information and subsequent development of information-confidence factors.

Achieving a successful DPO SA environment also involves business rules. The information owner should make information that is critical to a future DPO SA environment available in a standard manner that articulates the confidence level for the information being presented. The same pertains for other major process owners in the distribution domain. AMC should be responsible for airlift transportation information, the DLA and military service supply organizations should manage supply information, and USTRANSCOM should oversee information for joint intermodal transportation decisions. The information should be "tagged" to indicate high, medium, or low confidence based on a definitive, minimal criteria articulated as business rules.

To understand this concept, consider the following notional example of an information tag for an airlift transportation manifest:

1. type of information (e.g., airlift manifest),
2. organization responsible and point of contact for the information (e.g., Tanker Airlift Control Center: TACC OpsCtr@AMC.af.mil, 618-229-3131),
3. authoritative information source (e.g., "Gates"), and
4. date/time stamp of last update for the information provided.

By providing basic tag information (also known as metadata) one can next move on to developing the business rules for displaying information-confidence factors (see fig. 4).

Adopting a Knowledge-Centric Approach to DPO Culture

A trusted SA environment for DPO decision makers requires a culture that values knowledge as a central theme for success. Along the path to

DPO Situation Awareness

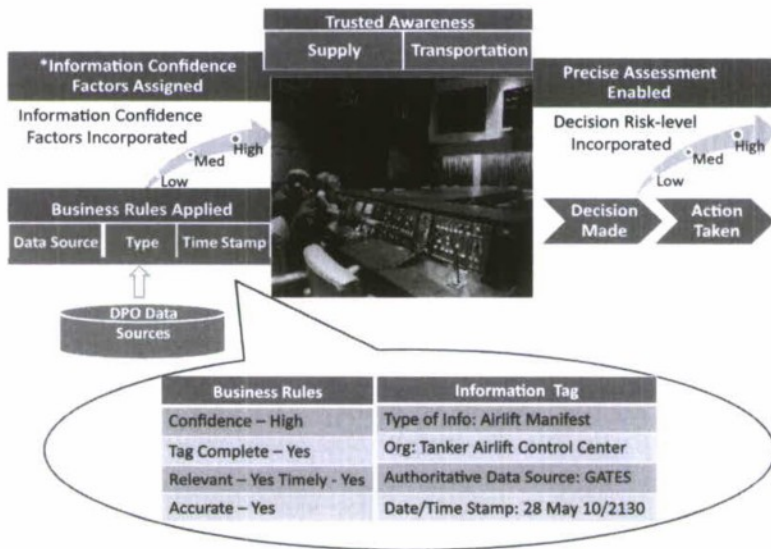


Figure 4. Example: business rules and information tag

becoming a knowledge-centric organization are the fundamentals of disciplined information management. These fundamentals include, but are not limited to, some of the following basic information management principles. A knowledge-centric organization should tag and categorize information in a standard way, with agreed-upon naming conventions, to be able to discover the information with an automated search engine. Otherwise, even the most powerful search engines available will only retrieve unorganized lists of disjointed information.

Practicing the fundamentals of disciplined information management is foundational to achieving information confidence and realizing ultimate transformation to a knowledge-centric organization and culture. None of these can be achieved through technology alone, and all should be realized to ensure information confidence. The DPO should continue to institutionalize ownership of processes, information, and business rules to fully reap the benefits of a DPO SA environment enabled by technology.

Analysis of Situation Awareness Research

To understand why information confidence is in the critical path of DPO decision makers, consider the mechanics of the decision-making

process within the SA environment (see fig. 1). The decision maker is the center of focus in the SA environment. The desired outcome of the model is a trusted decision which then leads to an appropriate action being taken in response to the information being presented. To achieve a trusted decision, the decision maker must have confidence in the information. The purpose of providing information-confidence factors is to enable the decision maker to proceed based on a visible level of confidence (high, medium, or low), such that minimal rework is required to validate and/or verify information prior to an ultimate decision being made.

A review of readily available SA research led to several primary references that were pertinent to USTRANSCOM's request for best practices for a COP for D2, that is, the DPO SA environment. Two were considered most pertinent for discussion: *Designing for Situation Awareness, An Approach to User-Centered Design* by Mica R. Endsley, Betty Bolte, and Debra G. Jones; and *A Cognitive Approach to Situation Awareness Theory and Application*, edited by Simon Banbury and Sébastien Tremblay.

Endsley has worked extensively in the SA field and is president of SA Technologies in Marietta, Georgia. Her area of SA expertise is in aviation, the military, and the medical profession. Her work provides a detailed approach to SA that focuses on the business of the user and a holistic SA business solution that guides development through user-centered design, focusing on user requirements, and applying SA-oriented design to the entire system of the mission environment.¹¹

Banbury and Tremblay complement Endsley's work by providing a broader review of SA research. Their book includes 17 chapters from 41 contributors. Endsley provides her insights regarding progress and directions for SA, providing a brief 2004 update to her extensive research from 2003 (see chap. 17). Banbury and Tremblay look critically at defining and modeling SA, questioning Endsley's 2003 work as being focused on a basic descriptive approach instead of a detailed prescriptive approach. While there may be some validity to that criticism, Endsley's detailed template for design principles is an excellent source from which USTRANSCOM can draw to perform a comprehensive baseline review of user requirements as it moves to a future DPO SA environment. The Banbury and Tremblay work draws credibility and strength from the 41 individuals across theoretical perspectives, research approaches, and domains of application.¹²

Why User-Centered Design and SA-Oriented Design Principles?

Foremost, Endsley's work impresses as a comprehensive design checklist that identifies the user as the appropriate focus versus driving solutions based on technology. She compares user-centered design with technology-centered design and ends with a detailed list of 50 design principles that appear to cover a grounded approach for addressing requirements for SA design. A review of the design principles reveals six areas for consideration: general, certainty, complexity, alarm, automation, and multioperator.¹³ To reinforce the value of this list, consider the primary assertion of this study: USTRANSCOM should identify information confidence and information-confidence factors as key requirements for its future SA environment, as articulated and supported by the proposed DPO SA decision-making model (see fig. 2). Endsley's "certainty" design principles speak directly to information confidence as follows: (1) explicitly identify missing information, (2) support sensor reliability (e.g., passive and active RFID sensor reliability), (3) use data salience in support of certainty, (4) represent information timeliness, (5) support *assessment of confidence in composite data*, and (6) support uncertainty management activities. More specifically, Endsley notes, "as more systems employ classification algorithms, sensor fusion, and decision support systems, the need will arise to *appraise operators of the reliability or confidence levels of these systems' outputs.*"¹⁴

One inclined to disagree with the need for information-confidence factors will possibly cite the net-centric data strategy that identifies an unrealized goal within the DOD—to introduce information pedigree as part of the overall data strategy for the department.¹⁵ Many of the standards or strategies for data in the DOD have been "all or none" propositions. These strategies have arguably led to shortfalls in expectations due to the enormous amount of work required to engineer information pedigree into the DOD data environment. The recommendation herein for implementation of information-confidence factors focuses on only relevant data. In other words, USTRANSCOM should leverage the power of user-centered design to identify the relevant data or information necessary to provide the most pertinent SA for its decision makers. The application of information-confidence factors should start with the relevant information that is valued most by USTRANSCOM and move forward based on an appropriate business case that identifies the return on investment. This will preclude much of the discussion regarding magnitude of effort and feasibility.

It will also cause the DPO to consider what information is most critical to its core mission and provide appropriate focus for SA designers.

**If Not User-Centered Design,
Then What Should Be the Focus?**

Some may still argue for a technology-centered versus user-centered design. However, the focus should be on human factors such as processes, information assimilation, business rules, and measuring successful mission outcomes. Reaching the DPO objective is also about technology—the good news is that technology is well matured and deployed in today's Web-enabled, connected IT world. Access to information is provided universally via portal technology, geographic visualization is readily provided by mapping tools like Google Earth, data warehouses and operational data stores are foundational capabilities in any corporate IT environment, and reusable Web portlets provide active content for the user experience. The user experience or interface is realized through common capabilities like iGoogle where a user can customize the views that are most relevant, such as international news, weather, sports, and so forth. All of the foregoing is made possible due to the years of foundational code development and subsequent proliferation through reuse in the world of software development. While technology is in the critical path for successful fielding of SA tools, it is well matured and readily available for implementation by any fundamentally competent IT organization. Therefore, a technology-centered design approach is not the answer for the DPO. Focusing on human engineering factors associated with user-centered design allows developers to focus on important outcomes, such as information confidence for the decision maker. Perhaps most critical to success, this strategy places users at the center of attention and involves them from concept to the fielding of capabilities.

Recommendations for USTRANSCOM

SA research and design appear to have come a long way in the last 10 years. SA research for the military has centered on the command and control domain. But the basic research, which is focused on design principles, crosses over to the logistics domain. (Several reference books have been cited in this study.) Based on this research and the author's personal experience with USTRANSCOM operations and IT programs, USTRANSCOM is at an opportune juncture to benefit from the extensive work done by many in the SA profession.

Leverage SA Industry Research and Adopt User-Centered Design Principles

The most relevant research for USTRANSCOM at this point in its maturity with DPO SA is that by Endsley, Bolte, and Jones. Based on their work, this paper identifies information-confidence factors as a micro-level recommendation and one of the key elements in USTRANSCOM's critical path to achieving successful DPO SA. Their approach to SA-oriented design is founded on three overarching principles that are recommended as best practices for USTRANSCOM leaders to consider as they continue transformation of the AT21 initiative: (1) organize technology around the user's goals, tasks, and abilities; (2) implement technology according to the way users process information and make decisions; and (3) use technology to keep the user in control and aware of the state of the system.¹⁶ The author's research offers a list of 50 design principles that the DPO should use as the basis for development of its SA requirements and subsequent development of a DPO SA environment. The research also directly supports the need to address what is termed *certainty design principles*, leading the DPO to address information confidence and understand the value of displaying information-confidence factors as part of its SA solution.

Adopt a Knowledge-Centric Approach: Define Ownership of Processes, Information, and Business Rules

By adopting a knowledge-centric approach and redefining the DPO culture as dependent upon trusted information, the DPO will set the tone for taking its SA game to the next level. The DPO should not treat all information as equal in terms of relevance to its mission. As a start, the process owner should determine which information is relevant to its SA environment and then establish information-confidence factors. In turn, this will enable decision makers to more expeditiously make critical logistics decisions. To embrace a knowledge-centric approach, the DPO should institutionalize disciplined information management principles. Otherwise, future DPO SA solutions may be relegated to providing the latest ways to present "uncertain" information, or users will continue to be burdened with checking, double-checking, and calling someone to ensure information confidence prior to making a decision. To solidify this recommendation, the DPO should adopt process, information, and business-rule ownership, to include identification of ownership stewards and measurement of information and knowledge management performance.

Address Critical-Path Concerns for DPO SA in Appropriate Governance Forums

As outlined earlier, several factors influence the achievement of information confidence. They range from personnel training, disciplined information reporting, and access to appropriate technology, to ownership of processes, information, and business rules—to name but a few. USTRANSCOM should continue to leverage the DPO and department-level governance forums to better ensure information confidence within the DPO SA environment. Some elements are directly within USTRANSCOM's control (e.g., senior-leader buy-in), and many are influenced at the DOD level.

Conclusion

This study posed three questions to help frame the discussion. First, what should be the endgame objective for DPO SA? The answer proposed forms the basis for the argument that the DPO should articulate the need for information confidence as its fundamental requirement for an effective and successful SA environment.

Secondly, what is in the critical path to achieve the DPO SA objective? The study provided an overarching look at several elements within the critical path for success (some within USTRANSCOM's direct control and some requiring coordination at the DOD level of responsibility). Finally, it asked, how does the DPO get to the objective end state? The recommendations given should provide a sound start to USTRANSCOM's pursuit of a future DPO SA environment. The author's intent was to address the DPO's considerations in a holistic manner, spanning multiple areas that will undoubtedly influence USTRANSCOM's ability to transform to the DPO of the future.

There is no single silver bullet for success here. As USTRANSCOM moves forward with DPO transformation through implementation of the AT21 initiative and delivery of IT-enabled capabilities through its corporate services vision, it should take advantage of the aforementioned research, best practices, and industry standards. This will help guide its end game for a future DPO SA environment informed by an appropriate cost-benefit analysis to determine the value of such an undertaking.

Notes

1. Lt Gen Claude V. (Chris) Christianson, USA, retired, "In Search of Logistics Visibility: Enabling Effective Decision Making," *Logistics Spectrum* 41, no. 3 (July–September 2007): 17.

2. Ibid.
3. Scott D. Ross, "The DPO's Corporate Services Vision: Learning from E-Commerce Leaders," release no. 090218-1, 18 February 2009, <http://www.transcom.mil/pa/body.cfm?relnumber=090218-1>.
4. Gen Duncan J. McNabb, USAF, commander, US Transportation Command, "Statement before the Senate Armed Services Committee on the State of the Command," 27 March 2009, <http://armed-services.senate.gov/statemnt/2009/March/McNabb%2003-17-09.pdf>.
5. Robert Rousseau and Richard Breton, "Defining and Modeling Situation Awareness: A Critical Review," in *A Cognitive Approach to Situation Awareness: Theory and Approach*, eds. Simon Banbury and Sébastien Tremblay (Hampshire, UK: Ashgate Publishing, Ltd., 2004), 3.
6. Ibid., 3-4.
7. Norah O'Donnell and Ted Savaglio, "Bush: Soldier's Equipment Gripes Heard," *MSNBC.com*, 9 December 2004, <http://www.msnbc.msn.com/id/6676765>.
8. James C. Bates, "Joint Asset Visibility: Why So Hard? The Way Ahead," *Army Logistician*, January-February 2008, 31; Timothy N. McCarter Sr., "Logistics Status Reports and the Logistics Common Operating Picture," *Army Logistician*, November-December 2008, 5; and David S. Alberts and Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age* (Washington, DC: DOD Command and Control Research Program, 2005), 191.
9. McCarter, "Logistics Status Reports," 7.
10. DPO Web site, "Governance Structure," <http://www.transcom.mil/dpo>.
11. Banbury and Tremblay, *Cognitive Approach to Situation Awareness*, viii.
12. Ibid., xiv.
13. Mica R. Endsley, Betty Bolte, and Debra G. Jones, *Designing for Situation Awareness: An Approach to User-Centered Design* (New York: Taylor & Francis, Inc, 2003), 251-52.
14. Ibid., 129.
15. Net-Centric Enterprise Services Tech Guide, "Net-Centric Data Strategy (NCDS) Goals," sec. 1.4, "Trustworthy," https://metadata.dod.mil/mdr/ns/ces/tech-guide/net_centric_data_strategy_ncds_goals.html.
16. Endsley, Bolte, and Jones, *Designing for Situation Awareness*, 8-10.

Abbreviations

AMC	Air Mobility Command
AT21	Agile Transportation for the 21st Century
COP	common operating picture
D2	deployment and distribution
DLA	Defense Logistics Agency
DOD	Department of Defense
DPO	distribution process owner
GCSS-J	Global Combat Support System-Joint
IED	improvised explosive device
IT	information technology
MSC	Military Sealift Command
OSD	Office of the Secretary of Defense
RFID	radio-frequency identification
SA	situation awareness
SDDC	Surface Deployment and Distribution Command
USTRANSCOM	US Transportation Command

The Need for a Global Space-Traffic-Control Service

An Opportunity for US Leadership

*Lt Col Matthew C. Smitham, USAF**

Losing a satellite to an accidental on-orbit collision is no longer hypothetical but real and increasingly likely. As a result, the space-faring nations of the world, especially the United States, need to address a global space-traffic-control service. The fiscal and national security ramifications are too significant to ignore. The replacement cost of a satellite, perhaps hundreds of millions of dollars, is the most obvious impact. But this may be the most trivial consideration. The greatest concern is the potential catastrophic loss of vital communications, navigation, weather, and other services we depend on for daily global commerce and defense. This paper explains the problem, examines some possible paths to address the problem, and recommends actions.

In February 2009, a spectacular collision grabbed headlines around the world. In low Earth orbit (LEO) 400 miles above Siberia, an American commercial communications satellite, *Iridium 33*, collided with the defunct Russian satellite, *Cosmos 2251*.¹ The probability of this first known satellite-to-satellite collision was estimated to be one in 100,000.² With a closing velocity of 22,000 mph, the satellites were instantly pulverized into debris clouds, creating more than 870 objects observed by the US Air Force Space Surveillance Network (SSN).³

The specter of collisions is not new, despite the “big sky” theory.⁴ Although *Iridium-Cosmos* is the first known collision between two satellites, this was the fourth documented accidental collision in space (intentional destruction is described later). In 1991, coincidentally, a defunct Russian satellite, *Cosmos 1934*, collided with a fragment from another *Cosmos* launch.⁵ Five years later, the French reconnaissance satellite *Cerise* was damaged by colliding with a fragment from an Ariane rocket body, another French object. In this collision, the fragment struck *Cerise* with a closing velocity of 32,400 mph, cleaving its 20-foot boom in half. Experts estimate the probability of this collision was one in a million—so much for the big sky theory.⁶

*Mr. Allen Sexton, USAF civilian, was the essay advisor for this paper.

Luckily, the satellite remained operational.⁷ In 2005 the third confirmed collision occurred. The final stage of a US *Thor Burner 2A* rocket, in orbit more than 31 years, struck a fragment from the upper stage of a Chinese *Long March 4* rocket.⁸

Beyond collisions, other events also present dangers to satellite traffic. Lt Gen Larry D. James, commander of the Joint Functional Component for Space, reported that the Chinese antisatellite test that destroyed *Fengyun-1C* in January 2007 was the worst fragmentation event in the history of spaceflight. This event added “2,400 pieces of potentially destructive debris,” increasing the number of objects that Air Force Space Command (AFSPC) tracked by over 10 percent.⁹ A month later, a Russian upper stage from a Proton rocket, loaded with fuel leftover from a failed boost, exploded and created another 1,100 pieces of debris.¹⁰ As of April 2009, the Air Force was tracking approximately 19,000 objects larger than 10 centimeters. If it could track objects down to one centimeter, the Air Force estimates that number would increase to about 300,000.¹¹

As space becomes more crowded with debris, it may be reaching a precarious tipping point. In 2006 National Aeronautics and Space Administration (NASA) scientists warned that unless space debris is removed, the likelihood of collisions will increase. They predict that beyond 2055 “the creation of new collision fragments [will exceed] the number of decaying debris,” while the “current debris population in the LEO region has reached the point where the environment is unstable and collisions will become the dominant debris-generation mechanism in the future.” In other words, as collisions create more debris, the collisions themselves become the primary source for debris.¹² As a result, NASA is concerned about the risk debris poses to its manned systems.

During 2008, with the aid of the Department of Defense’s (DOD) Joint Space Operations Center (JSpOC), NASA made five collision-avoidance maneuvers to protect its human spaceflight missions and maneuverable robotic assets.¹³ In March 2009 alone, the International Space Station had three near misses, which required the crew to prepare for emergency evacuation in one case and change orbit in another.¹⁴ GeoEye, a commercial imaging company, reported it has maneuvered its Ikonos satellite seven times and *GeoEye-1* satellite four times to avoid space junk in the LEO region.¹⁵ In addition, the Massachusetts Institute of Technology’s Lincoln Laboratory has recommended 65 avoidance strategies in the geosynchronous Earth orbit (GEO) belt since 1997.¹⁶ Although these efforts are encouraging, they are insufficient.

Today, most of the world's satellites fly in the blind, operating under the safety assumptions inherent in the big sky theory. However, Gen Kevin P. Chilton, commander of US Strategic Command (USSTRATCOM), stated that big sky has now "[come] to a close."¹⁷ Of the 19,000 objects that AFSPC and the JSpOC were tracking in April 2009, 1,300 were active payloads.¹⁸ In the next decade, an additional 200 payloads are expected.¹⁹ This growth in satellite numbers and the world's dependence on these systems points to the need for global space-traffic control. As the *Iridium-Cosmos* collision illustrates, the ad hoc efforts of NASA and others are not enough. Without a robust service to mitigate potential collisions, operators of military, civil, and commercial satellites are without the means to avoid catastrophe.

This paper advocates that the United States establish a global service with the cooperation of the international community and private sectors. To support this recommendation, we will examine existing global services that could serve as a model for a space-traffic-control service. But first, we will review the functional components of a service, the current space environment, the state of fielded space situational awareness (SSA) systems, gaps in these systems, and liability implications.

The Current Landscape

Before discussing the current space environment and the systems which monitor space, let's first describe what would make up a worldwide 24/7 space-traffic-control service. From a functional view, this service must be able to accurately search, detect, track, identify, and catalog space objects in Earth's orbit. The service would then need to predict the future positions of these objects, analyze the traffic for possible collisions (referred to as conjunctions), issue timely warnings to affected parties, and direct avoidance maneuvers, if required. If damage is sustained, per international treaties, the service would then need to assist to the greatest extent feasible in identifying the space objects and nations involved to help determine liability.²⁰ Logically, these functions can be organized into three categories: acquire, analyze, and act (see fig. 1), which parallel how data can be transformed into information and knowledge.

Monitoring and understanding the space environment comprise the essential first steps towards building a space-traffic-control service.²¹ This is traditionally referred to as SSA. SSA by itself is necessary but insufficient. A space-traffic-control service goes beyond this by also actively mitigating potential collisions (acting with knowledge, see fig. 1). Currently, a service which actively controls the global space

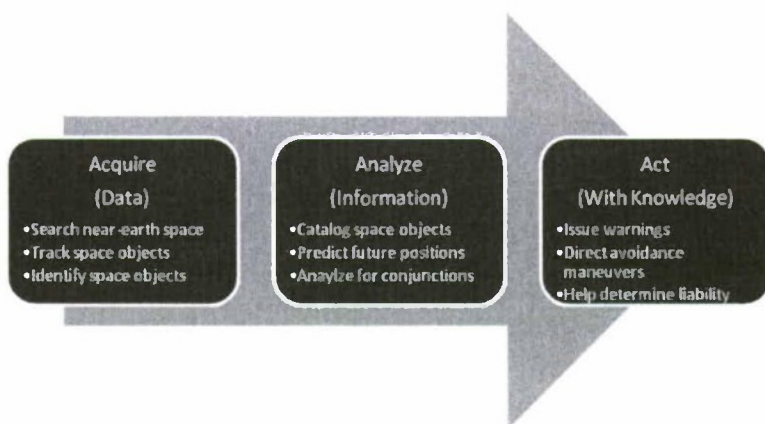


Figure 1. Functional view of a global space-traffic-control service

traffic does not exist.²² To begin this discussion, let's first examine the near-Earth space environment.

The number of man-made objects in Earth's orbit tracked by the Air Force has quadrupled to 19,000 over the past 29 years.²³ By 2015 the Air Force plans to upgrade its space surveillance network. With its increased sensitivity, the Air Force expects the catalog to grow fivefold to 100,000 objects.²⁴ The vast majority of these space objects and debris are in the LEO region.²⁵ This is the orbital region of most manned space flights and also where all the collisions described earlier occurred. However, objects in LEO are not the only ones susceptible to collision. The GEO belt is another region of concern.²⁶ Almost one-third (380) of the total 1,300 active payloads is in the GEO belt. Most of these are the high-value, high-bandwidth communication satellites used for television and communications. To complicate matters, another 750 dead satellites dangerously drift uncontrolled in the GEO belt.²⁷ In all, the Air Force tracks between 2,000 and 2,500 objects in GEO.²⁸

Beyond satellite-to-satellite collisions, as discussed earlier, satellite collisions with debris are another concern. Historically, 94 percent of all tracked objects is debris. Debris includes nonfunctional spacecraft, spent rocket bodies, breakup fragments, deterioration and exhaust products, objects released during spacecraft deployments and operations, and refuse from human missions.²⁹ In the last 20 years, fragmentation debris has comprised roughly 40–45 percent of all objects tracked. Large debris, such as dead satellites and old rocket bodies, comprises another 35–40 percent.³⁰

Recent events in the LEO region have made the debris environment even messier. The 2007 Chinese antisatellite test added another 2,400 pieces of potentially destructive orbital debris, a 2.7-fold increase in debris centered at 850 kilometers (km) in altitude. The *Iridium-Cosmos* collision added another 870 objects, a 33 percent increase at 780 km.³¹ As discussed earlier, unless debris can be removed, the problem will only get worse. Scientists predict that by 2055 new debris generated by collisions will outpace debris naturally removed through orbital decay.³²

Currently, only two nations have the necessary network of ground-based sensors and computational capabilities to attain the minimum degree of SSA to bootstrap a global space-traffic-control service. These are the American SSN and Russian Space Surveillance System (SSS).³³ Other government agencies with limited or nascent capabilities include the Chinese, French, and German militaries and the European Space Agency (ESA). Nongovernmental agencies such as the International Scientific Optical Network, operated by the Russian Academy of Sciences, and amateur astronomers also produce orbital data.³⁴ However, to achieve a truly global system, none of these are adequate; they all require upgrades and/or cooperation.³⁵

The US SSN is by far the most comprehensive system in the world. It is a global network of 29 ground-based sensors. In general, it uses radars to track LEO objects and optical telescopes to track GEO objects. Combined, these sensors provide the JSpOC with roughly 300,000 to 400,000 measurements (observations) per day. The JSpOC then has the enormous computational task of merging these observations into tracks, correlating the tracks with a priori information on known objects, and updating the 19,000 objects in the unclassified space catalog.³⁶ For high-priority US military and NASA analyses, the JSpOC also generates high-accuracy analyst sets available only to military personnel at JSpOC.³⁷

In comparison the Russian SSS has 22 sensors, which include military and civilian radars and telescopes. These systems collect approximately 50,000 observations per day. To make up for fewer observations (as compared to the Americans), the Russians depend on superior mathematical and predictive abilities to maintain their catalog. However, the SSS is not a global network; it is geographically confined to the longitudes of Russia and former Soviet republics. This geometry hinders their ability to track low-inclination LEO and GEO satellites in the Western Hemisphere. Further, unlike the Americans, the Russians do not publish a publically available catalog.³⁸

For self-stated reasons of sovereignty and independence, the Europeans are proposing an SSN of their own. The European Union real-

izes that its economy depends on space technologies and that protection of space systems is vital to its security. Some of its member states, such as Germany and France, already have some space-surveillance assets, but these are limited and not integrated into a holistic system. The ESA's director general said that "Europe is blind to what happens in space and wholly dependent on US supplied data."³⁹ To remedy this situation, the ESA plans to invest \$66 million over the next three years to develop its own capability.⁴⁰

A new US government initiative is also emerging. In 2003 Congress directed the secretary of defense to conduct SSA for all US government space systems and, as appropriate, for commercial and foreign entities (CFE). In response, AFSPC made available conjunction analyses via the Space-track.org Web site to nongovernmental entities as a pilot program. As of September 2009, 18 commercial companies, which operate 66 satellites, have signed quid pro quo agreements with the US government for conjunction analyses and launch support. In October 2009, AFSPC transitioned CFEs to USSTRATCOM as an operational program. However, the high-precision conjunction analyses needed for effective collision avoidance are not universally available. This is limited to high-value satellites (as prioritized by the US military) because it is labor intensive and not automated.⁴¹

Along with Space-track.org (as part of CFEs), several other public-domain services, such as HeavensAbove.com and Celestrack.com, also publish the space catalog on the Internet. Although they provide a valuable service, they are not necessarily providing new data. Essentially, they republish the unclassified space catalog provided by the Air Force, the so-called two-line element (TLE) sets. Although available to the world, these TLE sets do not have the requisite accuracy needed for precision conjunction analysis. In fact, the Air Force warns Space-track users to use the data at their own risk.⁴² Additionally, at least 6,000 objects do not appear in the Space-track catalog because the launching nation could not be identified.⁴³ With these restrictions and limitations, the underlying message is that users need more accurate data.

In an apparent response to these deficiencies, three of the world's largest commercial satellite operators—Intelsat, SES, and Inmarsat—in a cooperative private venture, created the Space Data Association in November 2009. They expect eight companies to participate in collision avoidance and another 14 companies to be involved in reducing satellite radio-frequency interference. Although they acknowledge that the US CFE program has some benefit, they feel compelled to invest their own capital because the "information is not always as

precise or up to date—nor is it disseminated as quickly—as it needs to be to protect against close encounters between satellites.”⁴⁴

Two other organizations also provide conjunction analyses and warnings of possible satellite collisions. Lincoln Laboratory, as part of a cooperative research and development agreement, fielded the Geosynchronous Monitoring and Warning System (GMWS) for its four member partners. The automated GMWS, via high-precision orbits derived from three Lincoln Laboratory-operated radars merged with SSN data, produces 60-day watch lists and two-week warning lists of close encounters for 60 commercial satellites. Lincoln Laboratory typically reports 250 conjunctions per year and has recommended 65 avoidance strategies to its partners since 1997.⁴⁵ A second service, the Satellite Orbital Conjunction Reports Assessing Threatening Encounters in Space (SOCRATES), is hosted on Celestrack.com and available to anyone interested. It provides twice-a-day analyses for all orbital regions based on the Air Force’s unclassified TLE sets. Although it’s not very accurate—the positional uncertainties are hundreds or thousands of meters due to the limitations of the TLE sets—the SOCRATES reports can be used as tip-offs by satellite operators for further investigation.⁴⁶

Despite these efforts, there is a significant gap between current space surveillance capabilities and what is needed for comprehensive, global space-traffic control. For example, as good as the US system is, General James says it still lacks the ability to acquire all on-orbit objects. He stated that the SSN has a significant coverage gap in the Southern Hemisphere and often loses some GEO satellites.⁴⁷ To plug this hardware gap, the Air Force is investing \$45 million to field a new ground surveillance system—an expansion of the “Space Fence”—with initial deployment by 2015.⁴⁸ In addition, the Space-Based Space Surveillance System, slated to launch in 2010, will provide the ability to scan the entire GEO belt from space and maintain “track custody” of GEO objects every 24 hours.⁴⁹ However, these efforts mainly address data acquisition (see fig. 1), not holistic solutions for space-traffic control.

Beyond hardware, the US software system is also imperfect and antiquated. In some cases, the Americans are behind Russian mathematical practices to process and predict high-quality space tracks.⁵⁰ For example, the US military is still using decades-old astrodynamics techniques to create element sets, mainly because the costs to redesign and recertify its operational systems would be enormous.⁵¹ To make up some of this deficit, the Air Force uses the brute-force method of oversampling (lots of observations) versus elegant mathematics. Until recently JSpOC was performing conjunction analyses

only for priority US satellites, such as manned flights and US defense satellites. After the *Iridium-Cosmos* collision and renewed interest by DOD senior leaders, the JSpOC recently upgraded its computational systems to give it the ability to run conjunction analyses for all active satellites within the catalog.⁵² However, precision analysis needed for positive collision avoidance is still only on a case-by-case basis because it is labor intensive and not automated.⁵³

Another challenge is data sharing. Only the United States currently shares its unclassified space TLE catalog with the world (with some restrictions). But its information sharing is criticized for being untimely and insufficient for conjunction assessment and warning.⁵⁴ Russia and China currently do not share.⁵⁵ And the ESA does not plan to publicly share data either. An ESA official stated, "We will send our data only to those who really need it."⁵⁶ Further complications arise from security. For example, the Americans do not share orbital information on their national-security satellites. The French were frustrated that the United States publishes data on French classified satellites and asked that the Americans withhold this information.⁵⁷ Dr. William Ailor, Aerospace's director for the Center for Orbital and Reentry Debris Studies, states that an effective space-traffic-control system would need to incorporate data from all sources, government and private, and would need to protect proprietary and sensitive data.⁵⁸

Beyond the inadequacies of data policies, no international treaties or guidelines "mandate a legal set of approaches towards space traffic management."⁵⁹ Only liability resulting from collisions is presently addressed by international law. The Outer Space Treaty of 1967, the Liability Convention of 1972, and the Registration Convention of 1976 make it clear that both intergovernmental organizations and state parties are liable for damages caused by their space objects (including their components) whether on the ground or in the air or outer space. Unfortunately, the treaties are silent on the issues of debris management or removal. If debris happens to be involved in a collision, the Registration Convention obligates nations with space surveillance systems to assist to the greatest extent feasible in identifying the origin of the space object.⁶⁰ To address this problem, the State Department's deputy director of space policy is looking "at ways to protect critical government and commercial space infrastructure against orbital debris" and improve SSA at the 2010 United Nations (UN) Conference on Disarmament.⁶¹

If a global service is required to avoid satellite collisions, is there precedence for such a service? We next look at three global services operating today, some of which have been in use for more than a century.

Precedents for Global Services

Three existing services could be models for a global service.⁶² These include a free US-operated service and international services that would help to manage the global commons on behalf of their members.

The Global Positioning System (GPS) demonstrates the first type of global service, one provided free by the United States. Today, GPS is used by virtually the entire world for positioning, navigation, and timing. According to senior US State Department officials, although its genesis was military uses, GPS evolved into a global utility and a centerpiece of US diplomacy. In 1983 President Reagan offered free civilian access to GPS to help enhance aviation safety around the world. President Clinton in 1996 expanded the policy to ensure the worldwide availability of the service for peaceful civil, commercial, and scientific purposes, free of user fees. In 2004 President Bush furthered the policy to ensure that the GPS meet the increasing and varied domestic and global requirements. These successive policies "helped unleash the power of free markets and private enterprise for the good of all users worldwide."⁶³ Clearly, this type of service is a likely candidate. With the largest, most comprehensive space surveillance system in the world, the United States is uniquely poised to offer another free service to the world.

A second precedent for a global utility is the International Telecommunication Union (ITU), a specialized UN agency based in Geneva, Switzerland. The ITU manages the worldwide radio spectrum usage and slot allocation for GEO satellites on behalf of its members. The ITU currently consists of 191 member states (nations), 574 sector members (commercial companies), and 150 associates (commercial companies). The members underwrite operations and participate in its decision making.⁶⁴ The ITU ensures the rational, equitable, efficient, and economical use of radio frequencies and orbital slots—both of which are finite resources—and creates the conditions that harmonize development of systems, taking into account all parties involved. According to the director of its Radio-communication Bureau, the ITU "plays a vital role in the global management of the radio-frequency spectrum and satellite orbits."⁶⁵

The third example of a global service is the International Civil Aviation Organization (ICAO). Founded in 1947, it governs the international civil aviation system. With the rise in aircraft use during World War II, the United States and others saw the need for a global aviation system. According to the ICAO, "A vast network of passenger and freight carriage was set up, but in order for air transport to support and benefit the world at peace there were many political and technical obstacles to overcome. In those early days of 1944, the Government

of the United States conducted exploratory discussions with other allied nations to develop an effective strategy.”⁶⁶ The ICAO is now a specialized UN agency with 190 member states that have voluntarily entered into its conventions. These conventions established the rules, procedures, requirements, and techniques to govern the movement of international civil aviation. Although each nation governs air traffic within its own sovereign territory, the ICAO successfully established protocols and procedures for the operations of international traffic, the transition of aircraft from one nation to the next, and the operation of aircraft over global commons, such as the high seas.



Photograph courtesy of the ICAO

In November 1944, under the leadership of the United States, 54 nations met in Chicago, resulting in a Convention on International Civil Aviation. In 1947 the ICAO became permanent.

Possible Solutions

Which model is most appropriate for the management of a global space-traffic-control service? One USAF general advocates a unilateral solution for protecting global utilities. “Having the Air Force assume responsibility for global satellite protection as an extension of its existing space-control responsibilities seems the most feasible option. Since the Air Force is tasked with controlling space, placing global utilities under the protective umbrella of space control would be a matter of policy—not an expansion of technology or costs.”⁶⁷ On the other hand, the State Department’s International Security Advisory Board proposes a multilateral solution and recommends that the

United States "seek to enlist allies and friendly nations in cooperative efforts to improve situational awareness."⁶⁸ The following examines four possible constructs and their pros and cons.

The first conceptual model is a US-owned-and-operated service akin to GPS. There are many compelling reasons why the US government could do this. First, it is probably the most expedient avenue to establish a global service because it could quickly leverage the existing SSN infrastructure and nascent CFE program. Second, the United States, as the leading spacefaring nation and the only nation with the necessary resources, has treaty obligations to ensure safety of space operations in the global commons. Lastly, as matter of national interest, the United States has the most at stake and most to gain. As the world's superpower benefiting from globalization, maintaining international institutions and their associated systems that contribute to the current world order is paramount to its economic security. Moreover, a global space-traffic-control service would enhance military space security as a defensive system.

Many believe there is a significant drawback to this type of service; that is, a utility provided by a single nation with the power to turn it off. For example, despite US public law, presidential policy, and diplomatic engagement, many nations are still wary of US intentions with the GPS and are pursuing their own navigational systems. The Europeans, Russians, and Chinese all have satellite programs that aim to implement organic capabilities. With respect to SSA, it's much the same. ESA's director-general articulated Europe's worry of being "blind" and wholly dependent on US-supplied data.⁶⁹ Despite these reservations, the United States could leverage this opportunity and promote US leadership and diplomacy just as it has done with space-based navigation applications.⁷⁰

A second model could involve a multinational cooperative service, as "it takes a village to build a (good) catalog."⁷¹ This could be a bilateral or multilateral arrangement among the United States, Russia, China, and/or the European Union. Significant diplomatic negotiations would be required to establish such an alliance, but the benefits could be significant. Doug Messier suggests that "the key benefit to international participation in SSA is greater capability for relatively low cost, by combining existing sensor and data sources."⁷² This model would also align with President Obama's anticipated space policy focusing on international cooperation.⁷³ Another benefit of cooperation is that each nation would have access to the same space operating picture, thus lowering mutual suspicion and increasing international security.

This construct does have several flaws. Data sharing could be sticky—especially information about defense satellites that each na-

tion would want to protect.⁷⁴ As stated earlier, Russia and China currently do not share their catalogs, and the Europeans have already expressed reluctance to share theirs. Equitable cost sharing associated with the operations, maintenance, and upgrades of this service would also need to be negotiated, probably not an easy matter. The service could disintegrate if one or more of the cooperating nations decided to withdraw from the arrangement.

The third model could be a commercial utility with clients—nations or private sector—that would pay for the service. A fledgling operation similar to this, the Space Data Association, is already in planning stages. The association plans to compile satellite positional data from its members' satellite telemetry feeds. A benefit to this kind of service is the built-in perception that it is independent from any one state or member. The association also aspires to be more nimble, timely, and responsive compared to the current US CFE paradigm.⁷⁵ However, without a robust, organic space surveillance system, its situational awareness will be limited to the collective knowledge of its members, and it would not be able to globally track nonmember satellites or debris unless a government augments the data.

The last model examined is an international global utility similar to ICAO. Advocates for this model include Dr. Ailor and the Secure World Foundation, a space-policy think tank. They propose a nonprofit space-operations clearinghouse with a board of governors and members drawn from governments of spacefaring nations and major non-governmental satellite owners "to establish common standards and practices."⁷⁶ This service would have the benefit of being recognized as legitimate and unbiased by nations and private-sector interests alike. The purpose and aims of such an organization could be orchestrated to parallel existing international laws and customs, such as the Outer Space Treaty and US space policy. This organization would also provide a forum for substantive discussions on debris control and unimpeded, safe access to the global commons. One drawback to such an arrangement would be that its members would be subject to rulings from an international body. However, this is no different than what already happens today with the ITU and ICAO.

Because an ICAO-like service has the most advantages and is more likely to enjoy international support, it is most likely to succeed. Pursuing this model would constructively leverage existing SSA infrastructures and capabilities as well as international cooperation while also suppressing mutual suspicions. The United States, as the leading spacefaring nation in the world, would additionally benefit indirectly in terms of diplomatic leadership and international prestige. It would also benefit directly, as would the world, from improved mili-

tary and economic security via improved space control and a safer environment for commerce.

Findings and Recommendations

Based on this research, this paper identifies five critical findings. First, the big sky theory for safe operations is no longer valid. Space is becoming congested and prone to collisions. It will only get worse with time. Second, the global economy and international security are in part dependent upon space systems. Consequently, safe operation of satellites is essential. Third, no governmental, international, or nongovernmental organization is ultimately responsible for global space-traffic control. Some governments, namely the United States, and several nongovernmental organizations have taken nascent steps to address this problem. However, these efforts are not synchronized or comprehensive. Fourth, an international consensus is building for improved SSA and space-traffic control.⁷⁷ Finally, the United States is the world's premier source for SSA. However, even with its future planned hardware upgrades, the United States is not configured to meet the needs of global space-traffic control, especially in terms of timely high-precision data analysis, data sharing, and policy.⁷⁸

These findings coalesce into a need for a global space-traffic-control service. This paper recommends first, as in 1944, that the US Department of State, in concert with applicable US agencies and departments, convene an international conference with the purpose of establishing a global space-traffic-control service. Within the next two years, the United States should engage spacefaring nations and interested private-sector companies in exploratory discussions to develop an effective strategy for such a service. Second, AFSPC, in concert with USSTRATCOM, should upgrade its antiquated software and databases utilized to track and catalog space objects. Although the planned Space Fence and Space Based Surveillance System will greatly expand data available, these hardware upgrades by themselves do not fundamentally bridge the processing gap required for timely, accurate collision mitigation.

As revealed by the fourth documented collision in space and the increasing orbital congestion, the need for global space-traffic-control service is clear. Ignoring the issue will not ease the problem. Within the US government, the USAF, NASA, STRATCOM, the State Department, and Congress all have stated the need to improve SSA and mitigate orbital collisions. Outside the US government, the ESA, the Secure World Foundation, and private industry have also advocated the need. What is missing is a comprehensive, synchronized plan to

addresses the problem in its entirety. As a matter of national prestige, leadership, and security, the US government should endeavor to establish an international institution to govern global space traffic.

Notes

1. Secure World Foundation, "Iridium 33-Cosmos 2251 Collision," fact sheet, 13 February 2009, http://www.secureworldfoundation.org/siteadmin/images/files/file_273.pdf; and Liz DeCastro, "Update on Iridium Satellite Constellation," 11 February 2009, <http://iridium.mediaroom.com/index.php?s=43&item=885>.

2. William Ailor, director, Center for Orbital and Reentry Debris Studies, The Aerospace Corporation, briefing, subject: Space Traffic Control and Space Debris, 8 May 2009, slide 5, https://www.mcgill.ca/files/iasl/Session_5_William_Ailor.pdf.

3. Statement of Lt Gen Larry James, commander, Joint Functional Component Command for Space, before the Subcommittee on Space and Aeronautics of the House Committee on Science and Technology, "Keeping the Space Environment Safe for Civil and Commercial Users," 28 April 2009, <http://gop.science.house.gov/Media/hearings/Space09/april28/james.pdf> (accessed 16 September 2009).

4. "Big sky" theory, borrowed from the aviation community, proposes that space is so large the probability of a collision is infinitesimally small. Some also use the term "big space."

5. Tony Reichhardt, "Satellite Smashers: Space-faring nations: Cleanup low Earth orbit or you're grounded," *Air and Space Magazine*, 1 March 2008; and Ailor, briefing, slide 5.

6. Ailor, briefing, slide 5.

7. Reichhardt, "Satellite Smashers."

8. *Ibid.*; and Ailor, briefing, slide 5.

9. James, "Keeping the Space Environment Safe," 3.

10. House, Committee on Science and Technology, Subcommittee on Space and Aeronautics, Hearing Charter, *Keeping the Space Environment Safe for Civil and Commercial Users*, 28 April 2009, http://democrats.science.house.gov/Media/file/Comm_docs/hearings/2009/Space/28apr/Hearing_Charter.pdf (accessed 16 September 2009).

11. NASA, briefing, subject: The Threat of Orbital Debris and Protecting NASA Space Assets from Satellite Collisions, 28 April 2009, www.secureworldfoundation.org/siteadmin/images/files/file_308.pdf. Although space debris mitigation, by physical means, policy, or international agreement, is an important topic unto itself, it has been extensively discussed by others and is not addressed in this paper.

12. Nicholas Johnson and Jer-Chyi Liou, "Risks in Space from Orbiting Debris," *Science Magazine* 311, no. 5759 (January 2006): 340; and Reichhardt, "Satellite Smashers."

13. NASA, briefing.

14. Doug Messier, "Secure World Foundation Proposes Global Space Debris Tracking System," *Parabolic Arc*, 29 April 2009, <http://www.parabolicarc.com/2009/04/29/secure-world-foundation-proposes-global-space-debris-tracking-system> (accessed 17 September 2009).

15. Warren Ferster, "GeoEye Dodging Space Junk with Increasing Frequency," *Space News*, 4 November 2009, http://www.spacenews.com/earth_observations/091104-geoeye-dodging-space-junk.html.

16. Richard Abbot and Timothy Wallace, "Decision Support in Space Situational Awareness," *Lincoln Laboratory Journal* 16, no. 2 (2007): 313.

17. Gen Kevin P. Chilton (address, Strategic Space and Defense Conference, Offutt AFB, NE, 4 November 2009). In this speech, General Chilton refers to "big sky" as "big space."

18. James, "Keeping the Space Environment Safe," 3. The number of active payloads cited in literature varies from 900 to 1,300. For consistency, this paper uses 1,300 payloads cited by General James during his 2009 congressional testimony. The math for the number of objects reported in public forums by the USAF does not add up in a straightforward manner either. For example, 6,000 objects are tracked but not cataloged because the launching country cannot be determined.

19. Ibid.

20. US Congress, Office of Technology Assessment, *Orbiting Debris: A Space Environmental Problem—Background Paper*, OTA-BP-ISC-72 (Washington, DC: US Government Printing Office, September 1990).

21. For this paper, *space environment* is narrowly defined to be just the man-made space objects and associated debris orbiting the earth. It does not include space weather commonly included in the definition of space environment.

22. The United States, in a nonroutine, limited fashion, maneuvers some of its high-priority satellites to avoid collisions. But the United States does this only for its own satellites. A global service that could direct space traffic for all satellites irrespective of their origin (governmental or nongovernmental) does not exist. The CFE program (discussed later in this paper) does provide some collision avoidance warnings for non-US government entities, but these warnings lack sufficient accuracy for collision avoidance maneuvers. The Air Force only passively warns and makes suggestions; it does not recommend maneuvers or enforce maneuvers for collision avoidance. In fact, the Air Force cautions the users to use the information at their own risk. See Space-track.org, "User Agreement," www.space-track.org/perl/new_account.pl.

23. James, "Keeping the Space Environment Safe," 3.

24. Jim Hodges, "Space Fence Reinvented," *C4ISR Journal*, October 2008, 37.

25. LEO is defined as an orbit less than 2,000 kilometers (km) in altitude.

26. GEO is defined as an orbit 36,000 km above the earth. The medium Earth orbit (MEO) region, although containing some important constellations such as the Global Positioning System, currently is at low risk for collisions and is not discussed at length in this paper.

27. Abbot and Wallace, "Decision Support in Space Situational Awareness," 306.

28. USSTRATCOM, "Space Control and Space Surveillance," fact sheet, 19 February 2008, http://www.stratcom.mil/files/STRATCOM_Space_and%20Control_Fact_Sheet-25_Feb_08.doc (accessed 18 September 2009).

29. Committee on Space Debris, *Orbital Debris: A Technical Assessment* (Washington, DC: National Academy Press, 1995), 12.

30. US Congress, *Orbiting Debris*, 2; and Committee on Space Debris, *Orbital Debris*, 22.

31. James, "Keeping the Space Environment Safe," 3; and NASA, briefing, slide 5.

32. Johnson and Liou, "Risks in Space from Orbiting Debris," 340; and Reichhardt, "Satellite Smashers."

33. Committee on Space Debris, *Orbital Debris*, 32.

34. Brian Weeden, "The Numbers Game: What's in Earth Orbit and How Do We Know?" *Space Review*, 13 July 2009, <http://www.the-spacereview.com/article/1417/1> (accessed 16 September 2009).

35. Committee on Space Debris, *Orbital Debris*, 32.

36. USSTRATCOM, "Space Control and Space Surveillance."

37. The US military uses two different mathematical models to describe orbits and conduct its analyses. The first is general perturbations; it describes orbits with two-

line element (TLE) sets compatible with the Simplified General Perturbation computer model; these are made public. The second method—far more accurate and complex—is special perturbation, which uses state vectors with double-precision positions and velocity vectors. It is only used for high-priority mission support on a case-by-case basis. State vectors are available only to the US government and are not shared with the public like TLE sets. See US Space Command Instruction 10-5, *DOD, Commercial, Civil and Foreign Space Support*, 1 April 2002, 2, 9.

38. Committee on Space Debris, *Orbital Debris*, 32.

39. Quoted in Peter B. De Selding, "Despite SSA Collaboration, Europe Leery of U.S. Intentions," *Space News*, 19 January 2009, 6.

40. *Ibid.*

41. Lt Col Charles Spillar, interview by the author, 24 September 2009, Peterson AFB, CO; Lt Col Charles Spillar, USAF Space Command/A3CN, briefing, subject: Commercial and Foreign Entities (CFE) & U.S. Government (USG) SSA Sharing, 24 September 2009.

42. Space-track.org, "User Agreement," www.space-track.org/perl/new_account.pl (accessed 17 November 2009).

43. Weeden, "Numbers Game?"

44. Peter B. De Selding, "Satellite Firms Moving Ahead on Orbital Database," *Space News*, 18 November 2009, http://spacenews.com/satellite_telecom/091118-satellite-firms-moving-ahead-orbital-database.htm (accessed 22 November 2009).

45. Abbot and Wallace, "Decision Support in Space Situational Awareness," 307–13.

46. Lt Gen John Campbell, USAF, retired, et al., *Examining Codes and Rules for Space*, Forum on National Security Space (Washington, DC: George Marshall Institute, 27 June 2007), <http://www.marshall.org/pdf/materials/554.pdf>, 17; and T. S. Kelso and S. Alfano, "Satellite Orbital Conjunction Reports Assessing Threatening Encounters in Space (SOCRATES)" (address, 2005 American Astronautical Society/American Institute of Aeronautics and Astronautics Space Flight Mechanics Conference, 23–27 January 2005), <http://celestrack.com/publications/AAS/05-124>.

47. James, "Keeping the Space Environment Safe," 8.

48. Jeremy Singer, "Air Force Seeks to Triple Funding for Space Surveillance," *Space News*, 7 April 2008, 50.

49. James, "Keeping the Space Environment Safe," 8.

50. Author's personal experience and knowledge.

51. Weeden, "Numbers Game?"

52. Spillar, interview.

53. In addition to its antiquated data processing and orbit prediction software, the associated Air Force databases are also archaic. Currently, the database is hard coded to handle only a limited number of objects, so it will also need to be upgraded. "Out of the 69,999 entries allocated for cataloged objects, about half are already used and growth is accelerating every year. Compounding this situation are the plans to add new sensors to the SSN in the near future that will greatly expand the number of objects tracked." Refer to Weeden's article, "Numbers Game?"

54. Iridium Satellite LLC, "Iridium Provides Update on Satellite Constellation," 9 March 2009, <http://www.iridium.com>; and De Selding, "Satellite Firms Moving Ahead on Orbital Database."

55. Edward O'Hara, *Space Situational Awareness*, Technological and Aerospace Committee, European Security and Defense Assembly, Assembly of Western European Union, Document C/2035, 6 May 2009, 6.

56. Quoted in "ESA Approves Space Situational Awareness Program," *C4ISR Journal*, 7–8 July 2008, 8.

57. Campbell et al., *Examining Codes and Rules for Space*, 17.

58. Ailor, briefing, slide 7.
59. House, Hearing Charter, *Keeping the Space Environment Safe*, 28 April 2009, 20.
60. US Congress, *Orbiting Debris*, 28–31.
61. Amy Klamper, "Obama Space Policy to Focus on International Cooperation," *Defense News*, 7 December 2009, 44.
62. This paper does not attempt to analyze these services in detail in terms of structure, cost, or degree to which they provide totally comprehensive solutions—only as appropriate examples to consider.
63. Alice A. Wong and Raye E. Clore, "Promoting International Civil GNSS Cooperation through Diplomacy," *High Frontier* 4, no. 3 (May 2008): 25–27.
64. ITU membership overview, <http://www.itu.int/members/index.html> (accessed 21 November 2009).
65. Valerie Timofeev, "Welcome to ITU-R," International Telecommunication Union Web site, <http://www.itu.int/ITU-R/index.asp?category=information&mlink=itur-welcome&lang=en>.
66. International Civil Aviation Organization, "Memorandum on ICAO," <http://www.icao.int/icao/en/pub/memo.pdf>.
67. Gen Bruce Carlson, "Protecting Global Utilities: Safeguarding the Next Millennium's Space-Based Public Service," *Air and Space Power Journal* 14, no. 2 (Summer 2000): 37–41.
68. US Department of State, International Security Advisory Board, "Report on U.S. Space Policy," Washington, DC, 25 April 2007, <http://www.state.gov/documents/organization/85263.pdf> (accessed 16 September 2009).
69. De Selding, "Despite SSA Collaboration, Europe Leery of U.S. Intentions," 6.
70. Wong and Clore, "Promoting International Civil GNSS Cooperation," 25–27.
71. Weeden, "Numbers Game?"
72. Messier, "Secure World Foundation."
73. Klamper, "Obama Space Policy," 44.
74. Edward O'Hara, *Space Situational Awareness*, Technological and Aerospace Committee, European Security and Defense Assembly, Assembly of Western European Union, Document C/2035, 6 May 2009, 10.
75. De Selding, "Satellite Firms Moving Ahead on Orbital Database."
76. Peter N. Spotts, "Does Space Need Air Traffic Control? As More Countries Race to Launch Satellites and Manned Craft, Some Warn of a Space Jam," *Christian Science Monitor*, 14 March 2008, <http://www.csmonitor.com/2008/0314/p01s02-usgn.html>. See also Ailor, briefing; and Doug Messier, "Space Traffic Control Conference to be Held Next Week in DC," *Parabolic Arc*, 20 March 2009, <http://www.parabolicarc.com/2009/03/20/space-traffic-control-conferences-held-week-dc>.
77. Ailor, briefing; Spotts, "Does Space Need Air Traffic Control?"; Messier, "Space Traffic Control Conference"; De Selding, "Satellite Firms Moving Ahead on Orbital Database"; Messier, "Secure World Foundation"; and Space.com staff, "Out There: Space Traffic Control System Needed," *Space.com*, 9 November 2008, <http://www.space.com/new/081109-space-traffic.html>.
78. Albert Glassman, "The Growing Threat of Space Debris," *IEEE-USA Today's Engineer online*, July 2009, http://www.todaysengineer.org/2009/jul/space_debris.asp.

Abbreviations

AFSPC	Air Force Space Command
CFE	commercial and foreign entity
DOD	Department of Defense
ESA	European Space Agency
GEO	geosynchronous Earth orbit
GMWS	Geosynchronous Monitoring and Warning System
GPS	Global Positioning System
ICAO	International Civil Aviation Organization
ITU	International Telecommunication Union
JSpOC	Joint Space Operations Center
km	kilometer
LEO	low Earth orbit
MEO	medium Earth orbit
NASA	National Aeronautics and Space Administration
SOCRATES	Satellite Orbital Conjunction Reports Assessing Threatening Encounters in Space
SSA	space situational awareness
SSN	space surveillance network
SSS	space surveillance system
TLE	two-line element
UN	United Nations
USSTRATCOM	United States Strategic Command

Ready or Not?

Repeal of "Don't Ask, Don't Tell"

*Col Julie C. Boitt, USAF**

I will end "don't ask, don't tell."

—Pres. Barack Obama

Throughout his presidential campaign and again as recently as the 2010 State of the Union address, Pres. Barack Obama reinforced his commitment to lift the ban on homosexuals serving openly in the US military.¹ Although he cannot lift the ban on his own—only the legislative branch has that authority—the president's clear stance and the Democratic Party's majority in Congress point to a repeal of the "Don't Ask, Don't Tell" (DADT) policy in the nearer term.[†] In fact, bills have already been introduced, and some Democrats in Congress are posturing to include a repeal in their versions of the defense authorization bill this year.² Moreover, in congressional testimony, Adm Michael G. Mullen, chairman of the Joint Chiefs of Staff (JCS), stated that it was his "personal belief that allowing gays and lesbians to serve openly would be the right thing to do."³ These facts make a repeal of DADT more likely than not—therefore, the Department of Defense (DOD) should begin preparing now to manage prospective impacts to its forces.

The US military, with its ban on the open display of homosexuality, stands with 11 other countries, but this list does not include countries where homosexuality is "banned outright, such as Iran, Saudi Arabia, and several other nations in the Middle East."⁴ However, other key allies, including the United Kingdom, Canada, Australia, and Israel, have already lifted the ban on homosexuals serving in their militaries. In fact, 24 foreign militaries now have no ban on gay service members, and many of these allies provide critical support to the North Atlantic Treaty Organization (NATO) International Security Assistance Force in Afghanistan.⁵ These "combat-tested fighting forces" are "critical partners in the American defense strategy" and can pro-

*Dr. Stefan Eisen, USAF civilian, was the essay advisor for this paper.

†The author finalized this paper in fall 2009 with the intent to better prepare the DOD for the eventual repeal of DADT. In March 2010, the secretary of defense directed establishment of the Comprehensive Review Working Group, which examined many of the issues outlined in this paper. In December 2010, Congress repealed DADT; the DOD is now in the process of implementing the new nondiscriminatory policy.

vide insight to the United States as it prepares for its own policy change regarding homosexuals.⁶

This paper briefly discusses the history and current policy under DADT and outlines proposed legislation currently in the US House of Representatives and Senate. Given the likelihood of repeal sooner rather than later, this paper then focuses on specific policy implementation recommendations for the DOD—and who should be involved. This paper does not argue the “rightness” or “wrongness” of any alteration to DADT. It does, however, show that to successfully execute the potential new law in the US military work environment, the DOD must involve key stakeholders and take multiple actions *now* to mitigate potential impacts. Such steps include being proactive, emphasizing professional conduct, top-down implementation, training and education, and consideration of manpower, facility, and other internal policy concerns.

Recent History and the Current Law

Those serving in the US military in the early 1990s remember the charged political debates and presidential campaign promises of Gov. Bill Clinton that eventually led to 10 *United States Code* 654, *Policy Concerning Homosexuality in the Armed Forces*, commonly known as DADT. While Clinton promised to lift the ban entirely, §654, enacted in 1993, was essentially a compromise based on fierce resistance by influential congressional members and senior US military officers.⁷ In the law, Congress reasserted its unique discretion to “establish qualifications for and conditions of service in the Armed Forces,” reaffirmed the “prohibition against homosexual conduct,” and reemphasized its authority to “regulate a [service] member’s life for 24 hours each day.”⁸

Basically, the law allows a homosexual to serve in the armed forces as long as that person does not engage (or intend to engage) in homosexual conduct, which includes homosexual acts, statements, marriage (or attempted marriage) to a person known to be of the same biological sex.⁹ Since implementation, from fiscal years 1994 through 2009, 13,167 service members have been discharged from the US military under §654.¹⁰ This paper uses DADT and the general term *policy* to refer to restrictions against open homosexuals in accordance with the 1993 statute, as well as the accompanying US government policy and implementing directives.

Proposed Legislation

The Military Readiness Enhancement Act of 2009, introduced in the House of Representatives and in subcommittee in March 2009, proposes to repeal the current law and the DOD policy concerning

homosexuality. As written, it "prohibits the Secretary of Defense, and Secretary of Homeland Security with respect to the Coast Guard when it is not operating as a service in the Navy, from discriminating on the basis of sexual orientation against any member of the Armed Forces or any person seeking to become a member."¹¹ The proposed legislation also "authorizes the re-accession into the Armed Forces of otherwise qualified individuals previously separated for homosexuality, bisexuality, or homosexual conduct."¹² The secretaries may also "not establish, implement, or apply any personnel or administrative policy, or take any personnel or administrative action (including any policy or action relating to promotions, demotions, evaluations, selections for awards, selections for duty assignments, transfers, or separations) in whole or in part on the basis of sexual orientation."¹³ A similarly worded and entitled bill was also introduced in the Senate, and it is currently in committee as of March 2010.¹⁴

Note that since repeal could affect family member benefits, section 5 of each bill states "[n]othing in this act . . . shall be construed to require the furnishing of dependent benefits in violation of section 7 of title 1, U.S. Code (relating to the definitions of 'marriage' and 'spouse' and referred to as the 'Defense of Marriage Act')."¹⁵ Unless changed, the federal definition of marriage will continue to be a "legal union between a man and a woman" and a spouse still "refers only to a person of the opposite sex who is a husband or a wife."¹⁶ In other words, unless the Defense of Marriage Act is altered or the proposed DADT repeal legislation is amended, spousal and dependent benefits should not be an *immediate* issue for the DOD.

Working the Interfaces—Who Should Be Involved?

Having people from all levels involved brings in multiple perspectives, identifies unexpected problems, and can generate innovative ideas and solutions.

—Wayne Turk
"Be Willing to Make Changes"

Repealing DADT must involve numerous stakeholders to ensure effective implementation and full consideration of unintended consequences. Participative involvement from all levels can also create buy-in and help "overcome resistance and make changes succeed."¹⁷ To determine who should be involved, figure 1 provides a proposed interest map for the DOD's use as it prepares for repeal.

Steven Cohen's interest map concept can be useful to visualize the different agencies with an interest in the outcome.¹⁸ For example, the

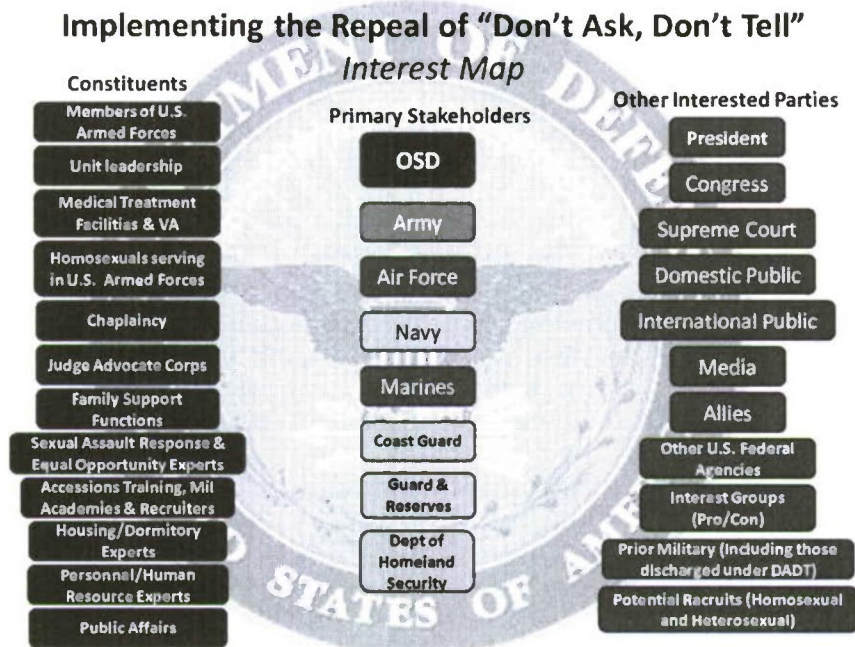


Figure 1. Implementing the repeal of “don’t ask, don’t tell” interest map. (Created by the author.)

primary stakeholders clearly have an interest if DADT is repealed, as they will be the primary implementers. The constituents, such as military members and agencies within the DOD, have a direct relationship and will be directly affected by the implementation plan approved by the department. Other interested parties (OIP) may or may not have a direct relationship with the DOD, but OIPs certainly have interests in the outcome—and might make decisions or take action based on that outcome. As Cohen suggests, these stakeholders’ interests may appear remote. However, “If we ignore them . . . they may come back to haunt us when we are least expecting it.”¹⁹ Moreover, note the overlapping interests, multiple ties, and connections among *all* of the parties on the map, even though these connections are not shown in the graphic.

To illustrate the recommended thought process, note that OIPs include the American public, the media, and US allies. Making a concerted effort to reach out and communicate strategically with the American public through the media before, during, and after implementation can go a long way towards ensuring transparency and maintaining public trust. Strategic communication should also target US allies, especially since many of them no longer have a ban on openly

serving homosexuals. Coalition partners must understand the change and the DOD's efforts to smoothly implement the repeal. In fact, many allies can offer potential "lessons learned" from their personnel policies, as will be discussed later. The key is to engage the right internal and external organizations from the start and to realize that others outside the US military are also impacted by a repeal of the DADT policy.

Policy Implementation Recommendations

If elected officials change the military's homosexual policy, the DOD must appropriately implement and adhere to the new law to minimize negative impacts to its forces. Armed with the background and proposed legislation above, several recommendations, outlined in figure 2, should assist the DOD in executing the new law's details.

Recommendations for DOD	
1. Be Proactive	– Consult Foreign Militaries – Review prior DOD Integration efforts
2. Emphasize Professional Conduct	– Create "code of professional conduct"
3. Top-Down Implementation	– Message must come from DOD senior leadership
4. Training & Education	– Not sensitivity training, but education on new law/standards
5. Manpower Considerations	– Temporary augmentation of Equal Opportunity (EO), Sexual Assault Response Coordinators (SARC), Chaplaincy, & Medical Corps – Posture for reinstatement of formerly discharged members – Prepare for potential "mass exodus" (senior officer/NCO leaders)
6. Facility Issues	– Consider, but be wary of special treatment/benefits
7. Other Internal Policy Considerations	– Revision of directives, regulations, <i>Uniform Code of Military Justice (UCMJ)</i>, and personnel policies – Posture for potential litigation
8. Immediate Implementation (versus Gradual Change)	

Figure 2. Implementing repeal of DADT—recommendations for the DOD. (Created by the author.)

Be Proactive

The DOD must be proactive and act now to involve such key players as those recommended in figure 1. The initial intent is to begin the dialogue among the stakeholders to determine what *they* think the issues will be and follow their suggestions by establishing specific action plans to deal with those issues. While the DOD may be concerned that leaning too far forward would signal acceptance or desire for the change, it may find that waiting until the change occurs risks failure—and is inconsistent with the military culture of planning ahead.

Part of a proactive approach should include consultations with allies who have lifted their bans to garner lessons learned. While such nations as Canada, Israel, Britain, and Australia did not experience the difficulties initially anticipated²⁰—and for Britain and Australia, lifting the ban was an “absolute non-event”²¹—there are still insights to be gained. Perhaps by consulting with Britain, for example, the United States can ascertain how none of the fears about “harassment, discord, blackmail, bullying or an erosion of unit cohesion or military effectiveness” materialized for its all-volunteer force.²² Despite size and cultural differences, an opportunity exists to extrapolate from allied experiences what might happen for the United States.

Regardless of these insights, the American military should still expect internal resistance; attitudes, social norms, and religious beliefs differ in the United States. For example, US military concerns regarding service of open homosexuals include undermining of unit cohesion, violence or abuse towards gays, violation of religious and moral beliefs, lack of respect for homosexual leaders, and the sharing of close quarters (such as foxholes, latrines, and operational spaces) between heterosexuals and open homosexuals.²³

A 2009 survey of Iraq and Afghanistan war veterans with specific questions about the concerns listed above suggests that “the strong support for the policy when it was created [in 1993] has shifted somewhat toward the direction of uncertainty or opposition,” indicating less internal resistance to a repeal.²⁴ Furthermore, the ratings indicated that the quality of leaders, equipment, and training is the critical factor associated with unit cohesion and readiness.²⁵ This is relevant since concerns about unit cohesion and readiness are the most cited reasons for opposition to any repeal of the gay ban.²⁶ Despite this, some current military members might view any change to the current policy as “coercive interference in their way of life.”²⁷ Therefore, the United States must prepare for this if the law changes.

Finally, while this change may not exactly mirror previous integration efforts in the US military, the DOD should still consult lessons

learned surrounding integration of African Americans and women for use during this effort. Consulting historical lessons can provide an essential base of knowledge leading to a successful transition. At a minimum, these experiences can provide insights into the military's adaptability to change. As RAND stated, "Experience shows that it is possible to change how troops behave towards previously excluded (and despised) minority groups, even if underlying attitudes towards these groups change very little."²⁸

Emphasis on Professional Conduct

Gay service personnel know that they have the code of conduct to back them up in the event of harassment or bullying. And all servicemembers know that they have recourse to complain if they witness inappropriate comments or actions.

—Aaron Belkin and R. L. Evans
*The Effects of Including Gay and Lesbian
 Soldiers in the British Armed Forces*

One successful implementation strategy used in the United Kingdom's transition in 2000 was the establishment of a code of social conduct modeled after the Australian armed forces.²⁹ The code, referenced in the quote above, places the focus on professional conduct and behavior for *all*, regardless of sexual orientation. Homosexuals and heterosexuals are "prohibited from engaging in social behavior that undermines, or may potentially undermine the trust, cohesion, and therefore the operational effectiveness, of the Services."³⁰ Existing policies, such as "zero tolerance for harassment, discrimination and bullying," complemented the code, which enumerated inappropriate behavior that included unwelcome physical or verbal sexual attention, displaying affection which might cause offense to others, and taking sexual advantage of subordinates.³¹ The key was the code avoided dealing with attitudes and beliefs that are often difficult to change. Instead, it addressed behavior, which can be more directly influenced.

Using such a code tailored for the United States may work. If the DOD adopts this approach, the first step would be to create a guiding coalition of senior leadership across the DOD with enough power and vision to lead the change.³² The second step would be to involve such key stakeholders as those illustrated in figure 1 to create a similar code that would apply to all US service members. The new conduct code should also be as *simple* as possible to enhance understanding.

Additionally, the stakeholder team should specifically address public displays of affection (PDA), since challenges in implementation may occur if heterosexuals and homosexuals have different standards in this regard. The team developing the code must realize that if PDA for a heterosexual couple is acceptable, the same standard should apply to homosexuals. In sum, an emphasis on professional conduct will be critical to successful implementation—and long-term adherence—to the proposed law.

Top-Down Implementation

It must be clear to the troops that behavioral dissent from the policy will not be tolerated.

—RAND Research Brief RB-7537, 2000

To effectively implement the DADT repeal, DOD officials must issue a consistent message from the top. DOD-wide talking points and senior leadership support and training must be central to this policy conversion. In addition to the message within the quote above, DOD guidance should include reminders that the US military is subject to civilian authority and that the DOD must make the change successful.

At all levels, commanders and their senior enlisted leaders must be the messengers, leading from the front rather than using the equal opportunity (EO) or sexual assault response coordinator (SARC) offices to deliver the news. Because the military is already under significant stress in Iraq and Afghanistan, leaders must also send messages of reassurance to the force, “convey[ing] that this policy is not a challenge to traditional military values.”³³ While potentially difficult to execute (depending on the personal views of each leader), the policy, coming directly from senior levels, can set the tone for a positive transition across the services.³⁴

Training and Education

Any enterprise-wide change requires training and education to ensure the initial roll out is implemented appropriately and to ensure the message is reinforced as new members enter. This change will be no exception. Using the code of conduct and talking points described earlier provide a great start. However, the training should *not* resemble sensitivity training, as has been suggested by other recent articles.³⁵ As RAND advises, “[E]mphasis should be placed on conduct, not on teaching tolerance or sensitivity. For those who believe that homo-

sexuality is primarily a moral issue, efforts to teach tolerance would simply breed more resentment."³⁶

Instead, the focus should center on establishing "clear norms that sexual orientation is irrelevant to performing one's duty and that everyone should be judged on his or her own merits."³⁷ Moreover, training should emphasize "all sexual harassment is unacceptable regardless of the genders or sexual orientations of the individuals involved."³⁸ Furthermore, training should include other specific guidelines—such as Britain's implementation guidance that advised "a person's sexual orientation is to be considered a private matter, and every servicemember has a right to personal privacy"—reminding personnel to "[r]espect that right, and do not try to make their private business your concern."³⁹ Educational efforts should also include clear direction and a focus on professional conduct by all. Finally, in anticipation of potential violence against known homosexuals in the military, training should emphasize that perpetrators of violence of any kind will be punished quickly and appropriately. In sum, training and education must clearly (and simply) communicate the new policy's expectations and explain what it means to each military member, focusing on characteristics that unite, rather than what separates.

Manpower Considerations

Although our allies did not experience great difficulties within their militaries and data from a 2006 survey of US, Iraq, and Afghanistan war veterans shows "declining support" for the homosexual ban, it is still prudent to plan for internal resistance.⁴⁰ To this end, the DOD should consider several resource issues. For example, the DOD's EO and SARC programs may require augmentation to deal with the potential increase in sexual harassment and EO-related complaints resulting from homosexuals serving openly. While homosexual-related complaints occur now, it is realistic to anticipate a temporary increase once the threat of involuntary discharge is lifted. As an integral part of change implementation, these organizations can appropriately deal with any lapses in performance by service members (both homosexual and heterosexual), and these functions can also provide critical commander support if adequately staffed.

Furthermore, such support agencies as the chaplaincy and medical community could require help depending on the reaction of the force. Although the DOD approach should emphasize behavioral issues, this topic has spiritual and moral implications that need consideration. In terms of religious counseling, even though a chaplain "would not be required to preach something that he did not believe as a part

of remaining in the chaplaincy, this community could face significant challenges as it seeks to minister to members of the force.”⁴¹ Additionally, frequency of homosexual-related medical issues may cause an uptick in readiness challenges if homosexual conduct is no longer prohibited. While HIV testing is already a part of medical screening for service members, a new nondiscriminatory homosexual policy could still have a negative impact. In response, additional screening, targeted medical care, and additional HIV medications may be required—and the medical community should be manned accordingly.

Another important issue deals with reinstatement of individuals previously discharged under the current DADT law, particularly since the proposed legislation calls for “re-accession of otherwise qualified persons.”⁴² Given this, the services should examine homosexual discharge cases since 1993 and begin determining personnel procedures for reinstatement immediately. The services should also begin collecting data regarding career fields in which these individuals served and begin formulating where and how they can be utilized to benefit both the service and the returning service member. The DOD should note that Britain successfully invited, integrated, and reaccessed previously separated members. After ensuring the individual’s qualifications, security clearance, and fitness for duty, the candidate was reinstated in fields where military personnel were needed. In addition, on-the-job or other training programs were used to establish job currency.⁴³

Finally, the DOD cannot ignore the possibility of a “mass exodus”—or at least a significant number of currently serving personnel deciding to separate or retire early because of the policy change. Other foreign militaries expected it based on vocal resistance before implementation. Even though it did not materialize, the United States could certainly be different, particularly in the higher ranks of its military. In fact, 1,152 retired flag and general officers have communicated concerns regarding DADT repeal, which could indicate significant resistance in *current* leadership as well.⁴⁴ To manage this risk, DOD leaders must communicate with the entire force early and often and reiterate such themes as fair and equitable standards for all and DOD-wide expectations for professional conduct. Focusing on leadership support at the intermediate level and what it means to them professionally is also important, for the “next layer of leaders, those who actually must implement the new rules, [must] come to identify their enforcement of the new policy *with their own self-interest* as institutional leaders” (emphasis added).⁴⁵ Interestingly, in addition to a concerted effort by military leadership to prevent any mass exodus, the presently weakened economy may actually be an asset in dealing with the repeal of the DADT policy. Even though RAND warned of

negative impacts on recruiting and retention, it is realistic to predict current economic concerns could mitigate those effects, not to mention those who *do* resign or choose not to reenlist are more easily replaced during record enlistment resulting from the new post-9/11 Government Issue bill, a steady paycheck, training, and other benefits.⁴⁶ Moreover, those retained will likely adhere to the new rules rather than risk discharge or disciplinary action, particularly given the fear of unemployment in the currently challenging job market.

However, a potential still exists that members may depart because their belief system will not allow them to adjust to the new policy, or they may depart to make a statement. The DOD should be prepared for this possibility, but such departures should not change an approach that incorporates an emphasis on professional conduct.

Facility Considerations

Another resource consideration mentioned in other literature stated that "dorm and facility upgrades would be needed."⁴⁷ While such upgrades would certainly be worth *considering*, since the most common concern for heterosexuals is related to sharing with homosexuals such accommodations as showers, bathrooms, and dormitories, the significant monetary costs and potential fairness concerns make it critical to look carefully at all sides.⁴⁸

For example, note that the United Kingdom chose *not* to make any facility adaptations to accommodate homosexuals and that the negative reaction was only short term.⁴⁹ Additionally, in Israel, rather than alter facilities, "gay soldiers are assigned to open bases, allowing them to commute to and from home and sleep at their own homes rather than in barracks."⁵⁰

In this regard, the US military must be particularly wary of special treatment—if homosexuals receive better facilities or special accommodations, it would only exacerbate potentially contentious integration issues and undermine cohesion and morale. Moreover, creating separate facilities or special quarters policies for homosexuals would theoretically require homosexuals to declare their orientation—a concept directly contrary to the proposed law's intent. In addition to cautions about special treatment, one could argue that current US military facilities are already adequate. With the exception of Navy ships and some Marine Corps bases, most enlisted dormitories are at (or projected for) the "1+1 standard," which includes separate living quarters with a shared bathroom and kitchen.⁵¹ Also, most locations, even in Iraq and Afghanistan, already use such privacy measures as stalls to separate common-use showers and bathrooms.

Lastly, it is accepted as factual that *homosexuals already serve in today's armed forces* and that there are no issues with the facilities currently available. Nor is there "valid scientific evidence to indicate that gay men and lesbians are less able than heterosexuals to control their sexual or romantic urges" or that "acknowledged homosexuals very seldom challenge the norms and customs of their organizations."⁵² Given this, if facilities are not an issue now, they should not be after the ban is lifted. However, if just *knowing* someone is homosexual, or if the real issue is that heterosexuals simply do not like or are threatened by homosexuals, perhaps the right way to deal with such discomfort or any resulting inappropriate behavior is through sexual harassment or educational channels and the chain of command. Within such channels, it remains an issue of professional behavior, not special accommodation.

In summary, good order and discipline, ensured through leadership, are what will make the transition work—much more than walls and stalls. Consequently, repeal of the DADT policy should not necessarily require special facilities accommodations—particularly given the enormous costs—but the DOD should look closely to consider all sides of the argument.

Internal Process Changes and Other Policy Considerations

Upon the ban's repeal, the DOD's most obvious internal tasks are to rewrite or adjust directives, instructions, and regulations and task subordinate services to do the same. In fact, proposed legislation already includes a blanket statement to this effect: "Not later than 90 days after the date of the enactment of this Act, the Secretary of Defense shall revise Department of Defense regulations" and each military department must revise its regulations "not later than 180 days after the date of enactment."⁵³ This relatively short timeline makes it prudent for the DOD to take stock of documents requiring edits now—while the repeal is being debated. This easy step enables a timely plan of action.

Note that the proposed bill does *not* address a revision of the punitive articles of the *Uniform Code of Military Justice (UCMJ)*. The congressionally mandated *UCMJ* requires the president to implement the *UCMJ*. The president does this through an executive order known as the Manual for Courts Martial. If Congress passes the DADT repeal bill, it follows that Article 125 ("Sodomy"), Article 133 ("Conduct Unbecoming an Officer and Gentleman"), and Article 134-4 ("General Article-Assault") would need to be aligned with the new law, since

arguably these articles could no longer be legitimately enforced under a homosexual antidiscrimination policy.

Another internal consideration is to prepare for possible lawsuits from separated homosexual service members. An increase in litigation is especially realistic if the DOD continues to discharge military members while the DADT policy is under review. Interestingly, the British Ministry of Defence discharged its last homosexual three days before lifting of its ban in 2000, resulting in additional negative press and litigation.⁵⁴ Thus, the United States should consider immediately whether to place on hold current discharge cases to preclude issues after repeal.

In addition to the considerations above, a broad range of personnel policies must be reviewed in the wake of the DADT policy repeal to determine if any other policies include discriminatory language. For example, service fraternization policies appear to remain relevant in any post-DADT world, with the exception of those paragraphs specifically addressing the current homosexual policy.⁵⁵ However, with regards to assignment policies, while military members could argue that homosexuals should be restricted from serving in certain career fields more likely to experience austere or close-knit living conditions (e.g., infantry, ranger, or Marine units), the proposed bill specifically prohibits any personnel policy, including selections for duty assignments, on the basis of sexual orientation in whole or in part.⁵⁶ Finally, if the proposed bill is altered to include dependent benefits, given that some states allow same-sex marriages, several other recommendations will need to be considered at some point, including medical benefits, insurance, and survivor benefits.⁵⁷ Even though the federal government is not bound by such state laws, repeal could just be a foot in the door and lead to dependent benefits as the next step of legislation. Either way, the DOD should at least consider this possibility, since the monetary and policy impacts would be significant. In sum, the DOD must undertake an enterprise-wide review of its policies to ensure they meet the new law's intent—and consider possible challenges.

Implementation Timeline

I think it's important, as we look to this change, that it be done in a way that doesn't disrupt the force at a time where it's under a lot of stress. And that, to me, means in a measured, deliberate way, over some time—to be determined.

—Adm Michael G. Mullen
Chairman, JCS

While some could argue that a gradual change may be more palatable because of current operations tempo (as the chairman states above) or because military culture does not change quickly and its customs are formed over generations, note that it has already been more than 16 years since the DADT policy was implemented. In other words, in a way, it has already been a gradual change.

Regardless, if the homosexual ban is lifted, the DOD may not have a choice in its implementation. The law may be directive and specific—the proposed bill's regulation rewrite timelines are a case in point. But even if there is a choice, most change experts recommend establishing a "sense of urgency" as the organization embarks on change and puts together its vision and strategy for implementation.⁵⁸ RAND also recommended immediate rather than gradual implementation as "any sense of experimentation or uncertainty invites those opposed to change to continue to resist it."⁵⁹ Since military members may feel like their turf is being invaded, leaders at all levels need to understand these concerns and communicate the policy change benefits to heterosexuals too, because it hinges on the professional standard of conduct for all. Still, leaders should *not* expect fundamental attitude changes towards homosexuals (or homosexuality) regardless of the timeline—even well after the change is implemented—but they must insist on an adherence to the new rules and a display of professional behavior from all service members.

Lastly, to ensure implementation is progressing as planned, the DOD must solicit feedback through hotlines, climate surveys, unit assessments, and possibly DOD-hosted conferences to identify and address issues during implementation. The DOD must also closely monitor retention and recruiting trends to determine the policy change's impact, if any.

Conclusion

Today's integrated force is the product of many years of effort, constant monitoring, and the sustained commitment of civilian and military leaders.

—RAND Research Brief RB-7537, 2000

The US military is the strongest force in the world, and if required by law, it is capable of integrating homosexuals as other countries have successfully done. The key in implementing a DADT policy repeal will be for the DOD to plan now and smartly implement any change to the existing policy by being proactive, emphasizing profes-

sional conduct, implementing the change with visible support from senior leaders, utilizing robust training and education programs, considering manpower and facility ramifications, and leaning forward to make policy and regulatory changes required by the new law. Doing these things, particularly with a sustained leadership commitment mentioned in the quote above, will help to ensure that US military readiness and cohesion remains intact in the midst of such a significant change. With a repeal of the DADT policy likely in the not-too-distant future, the DOD must be *more* ready than not—the American people and its government expects and deserves nothing less.

Notes

1. Pres. Barack Obama stated, "This year, I will work with Congress and our military to finally repeal the law that denies gay Americans the right to serve the country they love because of who they are." See Pres. Barack Obama, State of the Union Address (White House, Washington, DC, 27 January 2010), <http://stateoftheunionaddress.org> (accessed 28 January 2010).

2. Ed O'Keefe and Paul Kane, "Congressman Vows Repeal Effort in 2010," *Washington Post*, 12 November 2009, 6.

3. JCS Web site, "Testimony Regarding DOD 'Don't Ask, Don't Tell' Policy," as delivered by Secretary of Defense Robert M. Gates and Adm Mike Mullen, chairman, JCS, 2 February 2010, <http://www.jcs.mil/speech.aspx?id=1322> (accessed 8 February 2010).

4. Other countries with homosexual bans include Argentina, Belarus, Brazil, Croatia, Greece, Poland, Peru, Portugal, Russia, Turkey, and Venezuela. See Nathaniel Frank, *Unfriendly Fire: How the Gay Ban Undermines the Military and Weakens America* (New York: St. Martin's Press, 2009), 137.

5. *Ibid.*, 137, 158. Other countries without homosexual bans include Australia, Austria, Bahamas, Belgium, Great Britain, Canada, Czech Republic, Denmark, Estonia, Finland, France, Ireland, Israel, Italy, Lithuania, Luxembourg, Netherlands, New Zealand, Norway, Slovenia, South Africa, Spain, Sweden, and Switzerland.

6. *Ibid.*, 158.

7. Statements presented by members of Congress indicated resistance. See US House, Committee on Armed Services, *Policy Implications of Lifting the Ban on Homosexuals in the Military*, 103d Cong., 1st sess., May 1993. For information on resistance from the JCS, see Colin Powell, *My American Journey*, ed. Joseph Perisco (New York: Random House, 1995), 556–57.

8. "Policy Concerning Homosexuality in the Armed Forces," *US Code*, Title 10, sec. 654.

9. *Ibid.*

10. JCS Web site, "Testimony Regarding DOD 'Don't Ask, Don't Tell' Policy"; and Lt Col Greg A. Brown (USAF, Office of the Secretary of Defense for Personnel and Readiness), interview by the author, 13 October 2009.

11. House, *Military Readiness Enhancement Act of 2009*, 111th Cong., 1st sess., HR 1283, in *Congressional Record*, 3 March 2009; and Senate, *Military Readiness Enhancement Act of 2010*, 111th Cong., 2d sess., S. 3065, in *Congressional Record*, 3 March 2010.

12. House, *Military Readiness Enhancement Act of 2009*.

13. Ibid.
14. Senate, Military Readiness Enhancement Act of 2010.
15. Ibid.; and House, *Military Readiness Enhancement Act of 2009*.
16. *Defense of Marriage Act, Definition of Marriage and Spouse*, US Code, 104th Cong., 2d sess., 3 January 1996.
17. Wayne Turk, "Be Willing to Make Changes: But Not Change for Change's Sake," *Defense AT & L*, 1 May 2009, 2, http://www.thefreelibrary.com/_/print/PrintArticle.aspx?id=201622652.
18. Discussed in detail by Steven P. Cohen, *Negotiating Skills for Managers and Everyone Else* (New York: McGraw-Hill Co., 2002).
19. Ibid., 71.
20. Frank, *Unfriendly Fire*, 147.
21. Aaron Belkin, "Don't Ask, Don't Tell: Is the Gay Ban Based on Military Necessity?" *Parameters* 33, no. 2 (Summer 2003): 110; and Group Captain Raymond Goodall (Royal Air Force, Air War College instructor), interview by the author, 14 October 2009. See also Frank, *Unfriendly Fire*, 147; Sarah Lyall, "Gay Britons Serve in Military with Little Fuss, as Predicted Discord Does Not Occur," *New York Times*, 21 May 2007; Craig Jones (lieutenant commander, Royal Navy, retired), interview by the author, 19 January 2010; and "Gays in the Military: The UK and US Compared," *BBC News*, <http://news.bbc.co.uk/2/hi/americas/8493888.stm> (accessed 14 February 2010).
22. Lyall, "Gay Britons Serve in Military with Little Fuss."
23. Bonnie Moradi and Laura Miller, "Attitudes of Iraq and Afghanistan War Veterans towards Gay and Lesbian Service Members," *Armed Forces and Society*, 29 October 2009, <http://afs.sagepub.com/cgi/rapidpdf/0095327X09352960v1> (accessed 13 December 2009).
24. Ibid., 19.
25. Ibid., 1.
26. Rowan Scarborough, "Marine Leads 'Don't Ask, Don't Tell' Fight," *Washington Times*, 2 November 2009, 1.
27. Frank, *Unfriendly Fire*, 143.
28. "Changing the Policy toward Homosexuals in the U.S. Military," RAND Research Brief, RB-7537, 2000, http://www.rand.org/pubs/research_briefs/RB7537/index1.html.
29. Aaron Belkin and R. L. Evans, *The Effects of Including Gay and Lesbian Soldiers in the British Armed Forces: Appraising the Evidence* (University of California-Santa Barbara: The Center for the Study of Sexual Minorities in the Military, 2000), 27, 33.
30. Ibid., 26.
31. Ibid.
32. John P. Kotter, *Leading Change* (Boston: Harvard Business School Press, 1996), 21.
33. "Changing the Policy toward Homosexuals in the U.S. Military."
34. Some leaders may view homosexuality as wrong—for example, former chairman of the Joint Chiefs, Gen Peter Pace, "believe[d] that homosexual acts are immoral." Quoted in "Top General: Remarks on Gays Were 'Personal Moral Views,'" *CNN.com*, 14 March 2007, <http://www.cnn.com/2007/US/03/13/gays.military/index.html> (accessed 14 December 2009).
35. See Om Prakash, "The Efficacy of Don't Ask, Don't Tell," *Joint Forces Quarterly* 55 (October–December 2009): 88–94.
36. "Changing the Policy toward Homosexuals in the U.S. Military."
37. House, *Policy Implications of Lifting the Ban on Homosexuals in the Military*, 247.
38. Ibid.
39. Belkin and Evans, *Effects of Including Gay and Lesbian Soldiers*, 27.
40. Moradi and Miller, "Attitudes of Iraq and Afghanistan War Veterans."
41. House, *Policy Implications of Lifting the Ban on Homosexuals in the Military*, 170.

42. House, *Military Readiness Enhancement Act of 2009*.
43. Jones, interview.
44. "Flag and General Officers for the Military: Supporting the 1993 Law That Protects Morale and Readiness," <http://www.flagandgeneralofficersforthemilitary.com> (accessed 8 February 2010). For example, current Marine Corps commandant, Gen James T. Conway, has been the "most outspoken opponent" of repeal. See Scarborough, "Marine Leads 'Don't Ask, Don't Tell' Fight."
45. Frank, *Unfriendly Fire*, 166.
46. Lizette Alvarez, "More Americans Joining Military as Jobs Dwindle," *New York Times*, 18 January 2009, <http://www.nytimes.com/2009/01/19/us/19recruits.html> (accessed 14 December 2009).
47. Prakash, "Efficacy of Don't Ask, Don't Tell."
48. Belkin and Evans, *Effects of Including Gay and Lesbian Soldiers*, 38.
49. *ibid.*, 39.
50. Aaron Belkin and Melissa Levitt, "Homosexuality and the Israel Defense Forces: Did Lifting the Gay Ban Undermine Military Performance?" *Armed Forces & Society* 27, no. 4 (Summer 2001): 553.
51. "Base Housing: Barracks and Dormitories," *Army Times.com*. http://www.armytimes.com/benefits/housing/online_hbml08_housing_barracks/ (accessed 14 February 2010).
52. House, *Policy Implications of Lifting the Ban on Homosexuals in the Military*, 245; and "Changing the Policy toward Homosexuals in the U.S. Military."
53. House, *Military Readiness Enhancement Act of 2009*.
54. Brown, interview.
55. *Ibid.*
56. House, *Military Readiness Enhancement Act of 2009*.
57. Massachusetts, Connecticut, California, Iowa, Vermont, and New Hampshire issue marriage licenses to same-sex couples; Rhode Island, New York, and the District of Columbia recognize same-sex marriages from other states; and New Jersey allows civil unions. See National Conference of State Legislatures, "Same Sex Marriage, Civil Unions and Domestic Partnerships," <http://www.ncsl.org/issuesResearch/HumanServices/SameSexMarriage/tabid/16430/Default.aspx> (accessed 8 February 2010).
58. Kotter, *Leading Change*, 21.
59. "Changing the Policy toward Homosexuals in the U.S. Military."

Abbreviations

DADT	"don't ask, don't tell"
DOD	Department of Defense
EO	Equal Opportunity
JCS	Joint Chiefs of Staff
NATO	North Atlantic Treaty Organization
OIP	other interested party
PDA	public display of affection
SARC	sexual assault response coordinator
UCMJ	<i>Uniform Code of Military Justice</i>

Science and Technology Intellectual Capital

A Critical US Asset

*Col Stella T. Smith, USAF**

The potential for losing intellectual dominance in science and technology is a major threat to the ability of the United States to maintain national security and economic superiority. The United States must ensure it exercises the best possible options to grow, attract, and maintain enough qualified individuals to stay ahead of all adversaries. In addition to expanding the base of technology-educated individuals, the United States must counter threats to the intellectual capital base to secure its ability to deter the actions of adversaries. The primary measure of intellectual capital development is the number of undergraduate and graduate degrees earned in science, technology, engineering, and mathematics (STEM). The United States must focus now on doing what is necessary to maintain educational excellence and post-education opportunities to ensure that the US knowledge base in science and technology will remain the strongest in the world.

The following discussion examines many variables influencing the future of US intellectual capital. I first review the strategic importance of growing, attracting, and retaining graduate-level STEM professionals. This includes the first-, second-, and third-order effects of having, or conversely losing, US intellectual capacity. I next address current trends and, specifically, the importance of benefiting from foreign-born students and workers. This analysis includes statistics regarding graduate degrees granted in the United States to both citizens and noncitizens. Subsequently, I review initiatives to ensure that the United States will have a robust technology-educated core in future years. Finally, the discussion lays out potential impacts of developing technology on deterrence. I specifically focus on the United States' ability to stay at the cutting edge of innovation and the correlation of maintaining STEM intellectual capacity to countering or deterring technically advanced threats.

The exponential growth of technology combined with rapid globalization points to a future that requires the United States to have an advantage in science and technology intellectual capital. Without this

*Mr. Theodore Halles, USAF civilian, was the essay advisor for this paper.

resource, the United States will be at a disadvantage in many areas, including national security and economic stability. To best prepare for future threats, the United States needs to prioritize growing, attracting, and maintaining graduate-level technical capacity.

The Importance of STEM Intellectual Capital

A loss of leadership in S&T [science and technology] could hurt the U.S. economy, living standards, and national security.

—Titus Galama and James Hosek
*Perspectives on U.S. Competitiveness
in Science and Technology*

The United States earned and has maintained the preeminent place on the world's science and technology stage because of a robust higher education system and a pervasive culture of innovation. This advantage contributed to successes in all sectors and is a perishable resource worthy of attention and preservation. Exponential growth in technological change combined with rapid globalization increases the criticality of creating, recruiting, and maintaining science and technology intellectual capital.

STEM intellectual capital is the group of individuals with education and prowess in science and technology who use those talents to benefit the nation. This definition includes both American-born individuals and immigrants. Historically, the technological and scientific knowledge needed for US national security has not been a function of only domestic scientific talent.¹ While the Manhattan Project was overseen by a general and a chief scientist who were both US born and educated, over half the key scientists involved were foreign born.² The two scientists most responsible for the hydrogen bomb were born and educated abroad, one in Hungary and the other in what is now the Ukraine.³ Similarly, when the "space race" began with the Soviet Union launching *Sputnik I*, the United States responded by recruiting Wernher von Braun, born in Poland. He became known as the "father of the U.S. space program."⁴ These examples illustrate that throughout American history, when faced with a threat, the United States found the requisite talent wherever available. This has been, in breadth and depth, a uniquely American approach, one that has created diversity and strength in many fields. To maintain and increase intellectual capital, the United States must continue to seek, recruit, and retain foreign immigrants with science and engineering (S&E) capabilities.

Retaining or increasing the advantage of dominant intellectual capacity in science and technology is critical to the United States' staying

at the forefront of innovation and has potential second- and third-order economic, political, military, and social effects. Potential first-order effects include producing new forms of energy, responding to diseases, protecting the environment, stimulating further interest and excitement in students to study science and technology, sparking the next technological revolution, and enhancing security.⁵ Currently, the United States is the leader in many of these areas, and a change in that position could alter the world's economic, social, and security balance. Possible second-order effects of STEM capability include innovation, economic growth, military superiority, and the ability to detect and counter threats. All these elements support the broad US national strategy of promoting peace and prosperity. Third-order effects could include global social changes which alter the balance of power. These effects are amplified by globalization.

As an example, the National Academy of Engineering published an in-depth analysis of the impact of globalization on technical advancement. In part, it stated that "the United States must develop the necessary human, financial, physical, regulatory and institutional infrastructures to compare more advantageously with other nations in attracting the technical, managerial, and financial resources of globally active private corporations or individuals."⁶ In a globalized world, additional opportunities exist for individuals worldwide to gain expertise and use it in many locations for a variety of motivations. Where a person earns a degree may have less influence on where he or she will work in the future. Likewise, in a globalized world, where a highly educated worker lives will put less of a limit on whose interest he or she supports. This illustrates the importance of growing and recruiting individual intellectual capital working specifically in the interest of the United States.

One second-order effect of intellectual capital superiority is the national security activity of deterrence—influencing adversary leadership decisions away from actions deleterious to the United States. This endeavor requires an understanding of the actions an adversary is capable of taking, including threats based on emerging technologies. A decreasing science and technology intellectual base is likely to diminish the United States' ability to deter these threats. More simply stated, brainpower itself provides deterrence capability. If the adversary knows the United States has the intellectual ability to understand and counter threats, the chance of achieving his desired effect decreases. This change in the adversary's decision equation deters him from acting. Likewise, existing weapons are a key component of the US deterrent posture, and those weapons also require individuals with the intellectual capability to keep them viable. According to one

estimate, the Pentagon is at risk of running out of scientists to operate and upgrade the nation's arsenal of intercontinental nuclear and conventional missiles.⁷

As technology advances exponentially, risk increases due to dependence on vulnerable major networks such as the electrical grid and the Internet. Not only are more aspects of human endeavors relying heavily on these networks, but as time goes on, the United States is losing the necessary knowledge base required to revert to previous ways of doing business in a crisis. This increased dependence on high-value systems is a compelling reason why maintaining a robust pool of people with critical STEM knowledge is essential to successfully deterring adversaries.

If the United States does not take the actions necessary to stay at least even, if not ahead, in science and technology, there will be significant and very negative impacts. No other nation is its equal in scientific and technological accomplishments, but this does not make the United States invulnerable. The globalized world requires that the United States be at least on par with all potential adversaries in every technology field so not even one adversary can get an advantage by an outpacing advance in one area. If an adversary were to develop an advantage in a technology beyond what the United States could deter or counter, that would cause a change in the balance of world power. For this reason, the United States must stay even or ahead in all areas or be prepared to exist in a world where it is not the number one power.

Current Status and Trends

The number of university degrees a nation awards in S&E is an indicator of a nation's capacity to innovate in those arenas. S&E graduate enrollment in the United States declined in the latter half of the 1990s but has increased steadily since 1999. The most recent data, published by the National Science Foundation in 2010, shows that the number of bachelor's degrees awarded in 2007 increased in most technical fields, except computer sciences.⁸ Although it is difficult to determine the specific number of degrees required to keep an advantage, a positive trend is promising and far better than the alternative.

Students in the United States on temporary visas earned only 4 percent of the technical bachelor's degrees awarded in 2007, but foreign students make up a much higher proportion of the master's and doctoral degree recipients. In 2007 foreign students earned 24 percent of S&E master's degrees and 33 percent of doctoral degrees, bringing the total number of doctorates earned by foreign students to 13,700—a new peak.⁹ The United States should encourage these stu-

dents to stay and work for US interests. John Smart, preeminent scholar on the future of technology and founder of the Acceleration Studies Foundation, points to the US culture of innovation and the ability to do valuable research as advantages foreign students see for studying in the United States.¹⁰ The next step must be recruiting and retaining individuals in the high-skill work force.

Foreign-born intellectual capital is a critical asset. The United States has depended on the diversity, competition, and personal drive contributed by foreign students both during their education and afterwards in the highly skilled work force. Fortunately, through 2007 the trend of foreign-born students choosing to study in the United States is positive, as is the trend of foreign-born graduates who intend to stay here after graduation (fig. 1).

The United States is still the destination of the largest number of foreign students, but the numbers are trending downward. The US share in 2000 was 25 percent, but in 2006 it had fallen to 20 percent. The United Kingdom, Germany, and France are the other top destinations.¹¹ This is a trend worthy of close attention because attracting foreign students is a primary way of recruiting foreign talent for the

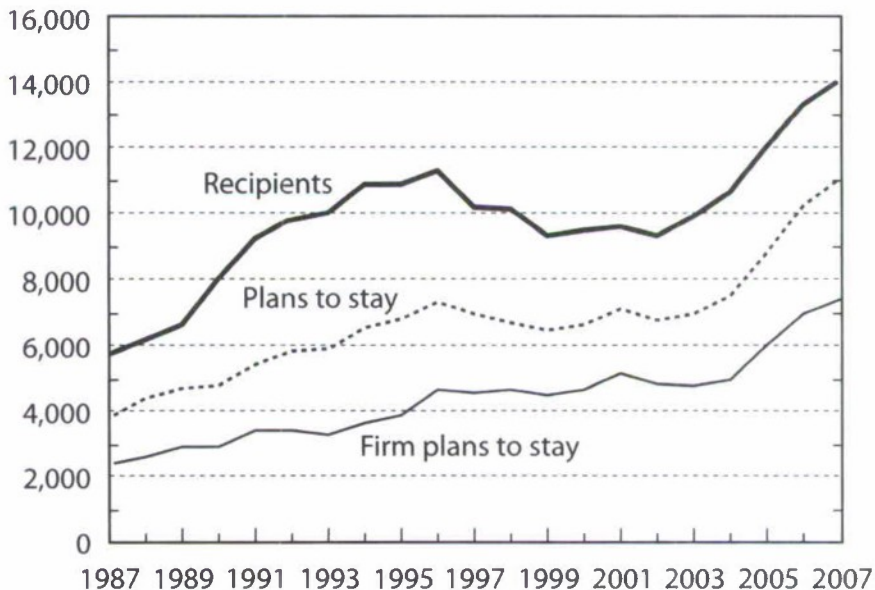


Figure 1. Plans of foreign recipients of US S&E doctorates to stay in the United States: 1987–2007. (Adapted from National Science Foundation, "Survey of Earned Doctorates," special tabulations, 2009.)

long term. Historically, graduate-level science and technology programs in US universities have been the world's benchmark. This acknowledged excellence, combined with the US culture of innovation, made degrees from US universities attractive to both US-born and international students. The secondary effect of attracting foreign students to US universities is that many of the international students have historically remained in the United States after graduation, increasing the intellectual resources available to US educational institutions, private companies, and government institutions.

Increased competition from other countries expanding their recruitment efforts is not the only threat to the United States attracting foreign students. Several trends threaten to decrease the US advantage in attracting foreign talent between now and 2035. First, US security concerns have increased greatly since the terrorist attacks of 9/11; as a result, visa procedures are more daunting, including those for foreign students and for foreign graduates of US universities who wish to stay in the United States to work. Second, at the same time that US policies are making it more difficult for foreigners to stay, improving conditions in many competitor nations are making it more attractive for foreigners educated in the United States to return home. The knee-jerk reaction to 9/11, which tightened visa policies, created a two-year decline in the number of foreign students in the United States. This trend later reversed, with the number of foreign S&E graduate students in US institutions increasing in the fall of 2006.¹² The number of student and exchange-visitor visas issued in 2006 was higher than ever before, and the sum of the other high-skill-related visa categories was near the 2001 high, suggesting the United States continues to attract those with advanced education.¹³ This improvement bodes well for recovery in the areas of recruiting and retaining intellectual capital, but the dip must be heeded as a warning of how easily the trend can be reversed. The foiled terrorist attack on a Northwest Airlines flight to Detroit on Christmas Day 2009 returned national attention to visas for foreigners. US policy makers must understand that any tightening of visa restrictions may seem to provide short-term improvements in security, but it could result in a long-term decrease in the capability to deter the very threats we are bracing against.

Finally, the pervasive interconnectedness or "flattening" of the world is a trend that has made it more possible and palatable for foreign-born graduates who do stay in the United States to still commit all or part of their efforts to interests in their countries of origin rather than using them to benefit the United States.¹⁴ The United States must develop a strategic plan now to continue to ensure adequate science and technology skills for 2035 and beyond.

Attracting foreign students is only the first step in securing foreign-born intellectual capital for the United States. Obtaining student visas is not the only issue. After graduation, many foreign graduates have difficulty obtaining visas to stay in the United States. In a study of approaches to strengthening scientific technology, Col Walter Juzukonis pointed out that the United States provides fast-track citizenship for foreign nationals who serve in the US military and proposes a similar fast-track approach for foreign nationals who have earned doctorate degrees in fields we need to bolster.¹⁵

Historically the United States has benefited from "brain drain"—when highly skilled immigrants contribute educational and economic assets to a country that hosts them for extended periods or permanently.¹⁶ The brain drain from foreign countries is created by a lack of opportunity for individuals to be innovative in their home countries. The United States provides attractive opportunities in a culture of innovation, and the brain drain for other nations in turn becomes a brain surge for the United States. A 2006 report on Brazilian, Chinese, and Italian students in the United States showed that social responsibility and perceived opportunities in their home countries were strong factors in their decision to stay in the United States or return to their country of origin.¹⁷ The United States can increase the potential for foreign graduates to stay here by providing incentives that outweigh their desire to return to their home countries. Investing resources and creativity in influencing these decisions will provide payback if it means the United States retains STEM-educated, innovative individuals.

In today's environment, the United States must recognize and prepare for multiple levels of external threats. Easy access to information increases the possibility of high-tech threats being wielded not only by nation-states but also by groups and individuals. Some see this as an impetus for tighter restrictions on visas and the naturalization policy. Ironically, these same policies make it more difficult to expand the pool of individuals with technology and science skills needed to counter those threats. National policy makers must work these issues aggressively and recognize that keeping science- and technology-educated individuals out of the United States is a prescription for increased external threats and decreased capability to deter or counter them.¹⁸

T. A. Frank, an Irvine Fellow at the New America Foundation, proposes that one way to regain our dominance in the tech sector would be to get more of the brightest people in the world to move here. He contends that because roughly a quarter of US technology and engineering start-ups have founders who were born abroad, it would benefit

the United States to encourage more talent to come here and stay here. Frank supports a plan whereby any student with an advanced degree in science, technology, engineering, or math would be offered a reasonable chance at permanent residency in the United States, with the requirement of employment in that field. A bill presented by Republican senator John Cornyn in 2007 would have removed caps on employment-based green cards for workers with advanced degrees. The bill did not pass, and neither did a similar one presented by Senator Arlen Specter. The aim should be to prevent an exodus of the people educated in the United States. Some think this policy will hurt low-income Americans. Historically, this is not true because an increase in high-skill workers tends to create additional jobs, not take them.¹⁹

Existing Initiatives

Many ongoing initiatives are encouraging the future growth of technological expertise. Great examples already exist of politicians and educators focusing on this important venture. President Obama made STEM education a national priority by putting emphasis on science and technology early in his administration. Prior to that, initiatives already were underway at lower levels in the United States, driven by the efforts of interest groups, states, and individual politicians.

Even before his inauguration, President Obama recognized that science and technology need to be reinvigorated.²⁰ The president made an early announcement that physicist John Holdren would serve as assistant to the president for science and technology and director of the White House Office of Science and Technology Policy. In addition to putting a priority on filling this key position, President Obama started talking publicly about improving education in STEM areas. In remarks to the National Academy of Sciences, President Obama quoted Abraham Lincoln's statement regarding his purpose in creating that organization—to add “the fuel of interest to the fire of genius in the discovery of new and useful things.”²¹ President Obama stated, “Science is more essential for our prosperity, our security, our health, our environment, and our quality of life than it has ever been before.”²² In his remarks, he committed to use policies and incentives to exceed the level of research and development the United States achieved at the height of the space race. He also committed to improve education in math and science. The president pointed out that more than 20 percent of high school students in math and more than 60 percent in chemistry and physics are taught by teachers without expertise in those fields. He created an incentive for states making commitments to math and science education to compete for additional

funds. Further, in response to the United States' trailing other nations in creating scientists and engineers, he set a goal for America to have the highest proportion of college graduates in the world by 2020. He also pledged to triple the number of National Science Foundation graduate research fellowships.²³ The tone of his entire speech was one of dedication to reinvigorating the nation's commitment to science and technology to stay competitive academically and economically.

President Obama is doing more than just talking about improving technology education—he included substantial funding in the proposed fiscal year (FY) 2011 budget specifically targeted at creating the next generation of scientists and engineers who can help drive economic growth in the coming decades. The budget provides \$300 million in new grants for states to develop and implement instructional practices and improve teaching and learning in science and math. The Investing in Innovation Fund totals \$500 million and includes \$150 million for competitive grants for school districts, nonprofits, and other organizations to test, validate, and scale promising strategies to improve teaching and accelerate student learning in STEM subjects. The budget also directs the Department of Education to work with the National Science Foundation and other federal agencies to identify the most effective interventions that can help states, schools, and teachers improve STEM outcomes.²⁴ Setting the goal for 2020 and providing funding for initiatives show the administration's dedication to the future of science and technology brainpower. These are all good concepts but only become of value if implemented. The current fiscal crisis in the United States puts all such programs at risk, and the political environment may not be conducive to supporting such expenditures for both fiscal and nationalistic reasons. Advocates must continue to make arguments for science and technology education that strongly illustrate the long-term advantages of increasing the current STEM capabilities.

The administration is not alone in attempting to reinvigorate science and technology education in the United States. In 2005 a coalition of 15 business-oriented organizations, Tapping America's Potential, set a challenge to double the number of American graduates with bachelor's degrees in science, technology, engineering, and mathematics from 200,000 to 400,000 by 2015. The number increased each year through 2006, but not enough to meet the goal. Falling short of the target may not be statistically relevant because the target was chosen based on the professional judgment of business people, rather than the needs of the nation. However, the fact that business leaders are giving the issue specific attention is a positive indicator that experts understand the importance of intellectual capital.

Colorado provides one outstanding example of a state-level project to invigorate technology education. Four institutions—the Metropolitan State College of Denver, Colorado School of Mines, Community College of Denver, and Cherry Creek School District—have formed an unprecedented alliance called the Colorado Academy for the Development of STEM-Related Careers (ADSC). It is designed to position the state as a leader in STEM education and to ensure that its students, from kindergarten through graduate level, are connected to cutting-edge innovation. Colorado's governor, Bill Ritter, has embraced and supported ADSC's vision. The academy's initial focus will be on air and space—providing education, scholarships, internships, career guidance, and mentoring to students desiring skills needed to build air and space careers. The Colorado ADSC will provide educational certifications and specialized training that connect its targeted learning communities from kindergarten to doctoral programs to ensure job readiness and career enhancement. It will also collaborate with Colorado Workforce Centers, which will facilitate training and assist in job placement.²⁵ This program could be used as a model for other states and, if leveraged properly, could educate and inspire a whole generation of US students.

Individual politicians have also recognized the importance of STEM education. Republican congressman Randy Forbes (VA) obtained a National Science Foundation grant of \$989,747 for Virginia State University to target minority students to increase the pool of STEM students. In the United States, this segment of the population has been underrepresented in the STEM fields, and tapping into that resource is another potential method to increase the intellectual capital for the future. The money will fund a three-year study aimed at improving test scores for minority students in STEM fields. Forbes hopes the study can become an education model. He said that it “is about more than just advancing test scores and equality in education; it is about economic advancement and ensuring that the United States retains its edge in the math, science and technology fields—a critically important requirement in today's global economy.”²⁶ While the intent is good and should be supported, it does have the scent of “pork” politics, so proper arguments need to accompany such proposals to defend them in the political arena.

The issues of creating and maintaining intellectual capital are complex and require a multifaceted approach. The initiatives listed above merely provide examples of methods which could yield benefits. Globalization increases competition for intellectual capital and makes it critical for all levels of US government, business, and education to

find innovative, effective ways to encourage STEM education and attract and retain STEM-educated researchers and workers.

Implications for Deterrence in 2035

All indications are that technology will continue to develop at an increasing rate and that globalization will continue to "flatten" the world. The world of 2035 will benefit from positive technology innovations which improve health care, information availability, energy sources, and human performance. The technologies that will make these improvements possible will also offer adversaries opportunities to use them for negative purposes. As always, US national security in 2035 will depend upon the ability to deter adversaries. Intellectual capital in STEM professions, whether residing in US- or foreign-born individuals, is the foundation of any deterrence. STEM knowledge is an enabler for deterrence.

Deterrence is dependent upon a potential adversary determining that an action on his part will either fail to get the result he seeks or will create an intolerably high cost or risk.²⁷ The United States relies on deterrence as a major element of national security strategy and, to keep it viable, must stay aware of developing technological advances. This can only be accomplished if the United States harnesses the capabilities of individuals who can understand and competitively operate in the fields of nuclear weaponry, cyber warfare, chemistry, molecular biology, nanotechnology, directed energy, and the space domain. In addition to understanding evolving technologies, the United States must maintain existing deterrence options, like nuclear and conventional weapons, while developing new offensive and defensive weapons. Deterrence is crucially dependent on science and technology.

Space as a Case Study: The United States May Not Have an Advantage in 2035

There will be many areas of concern for deterrence in 2035. Primary among these will be threats in cyber, nuclear, biological, directed energy, nano, and space technologies. The space domain provides a valuable example as a critical area in which the United States must be prepared to deter threats in the future. It also provides a good example of second-order effects because space is an industry which drives economic growth. According to *The Space Report 2009*, "It is unclear whether the U.S. education system can drive growth in the number of new skilled science and technology graduates, espe-

cially those with advanced degrees, needed to replace veteran U.S. space workers who are retiring.”²⁸ The number of bachelor’s degrees awarded in “space critical” fields—Earth and atmospheric sciences, mathematics, computer science, and engineering—dropped by 8 percent between 1986 and 2006.²⁹

These trends do not bode well for the future of the space industry or for national security interests in the space domain. The demand for key space industry occupations is projected to grow over the next 10 years, and unless the number of space-critical graduates increases or the United States is able to recruit foreign talent, jobs will go unfilled.³⁰ As *The Space Report 2009* notes, “The key to maintaining US technology preeminence is to encourage and develop skilled scientists and engineers who strengthen the space industry.”³¹ The US space industry is just one example of a domain in which the United States may not maintain intellectual dominance through 2035.³² Each area of potential threat must be evaluated individually; space provides just one clear example of the criticality of maintaining intellectual dominance.

Conclusion

Maintaining the advantage in science and technology intellectual capital is critical to the future of US security. Current trends are positive, and initiatives are underway to grow, attract, and maintain enough qualified individuals to stay ahead of adversaries. However, the past decade has shown that these trends are vulnerable to sudden change. The tightening of visa processes after 9/11 demonstrated that the inflow of foreign students and experts can drop quickly. Although keeping terrorists out is vital, the federal government must also recognize the ramifications of impeding one source of technical expertise. In the near term, the United States likely will continue to rely on foreign-born individuals to maintain its science and technology advantage. If the United States chooses to reduce its historic dependence on foreign-born brainpower, there must be a corresponding increase in homegrown expertise. The most robust pool of individuals can be amassed both by attracting foreign-born students and experts and by increasing the presence of US-born personnel who are highly educated in the technology arena.

President Obama has said that improving science and technology education is a matter of national importance, and he included substantial funding in the proposed FY 2011 budget. Industry, state, and local initiatives are also in place to provide educational opportunities to increase the number of US-born students earning technology de-

grees. Adjusting visa and immigration laws to enable the United States to attract and retain even more talent from other nations will reduce the threat of the United States falling behind in the capability to lead innovation in science and technology. Its lead in technology is crucial to deterring adversaries, whether they are nation-states, non-state actors, or individuals.

If the United States does not maintain the lead in critical technologies like nuclear weaponry, biological warfare, nanotechnology, cyber warfare, directed energy, and space technology, one or more adversaries likely will take advantage of areas of weakness. Current deterrence depends on the adversary believing that the United States has the capability to deter and the will to take decisive action. The capability is created by those who understand cutting-edge technology. If an adversary did not think the United States could act decisively, he would be more likely to take offensive action. A cyber attack could interfere with almost any US data system and could potentially disrupt most US military operations. A space attack could eliminate access to the global positioning system (GPS), which, at a minimum, would make navigation nearly impossible and disrupt banking worldwide. A biological attack could eradicate a vast portion of the US population. These are examples of events that, undeterred and uncountered, could change the balance of power and threaten the American way of life. Current intellectual capacity makes deterrence viable and supports development of methods to recover if one of these attacks should occur. Without qualified scientists and engineers, the United States could not replace or establish a workable alternative for the GPS after a space attack. Likewise, vaccinations and antidotes would not be available to counter or minimize the impact of a biological attack. These are just two examples of a plethora of possible threats if the United States does not maintain intellectual superiority.

The United States enjoys its position as the one remaining superpower in large part because of its broad spectrum of intellectual expertise in technology fields. In his February 2010 State of the Union address, President Obama stated that the United States is not going to be "number 2." Maintaining the position as "number 1" means more than maintaining national security. As the leader of technology development, the United States also gets to set policy. This has worldwide implications for areas like human genome mapping, nuclear weaponry, and biological warfare. As the leader in these areas, the United States can best influence international treaties, bans, and agreements. Intellectual capital is a critical national security resource that cannot be regained rapidly if it is allowed to deteriorate. Keeping the advantage is a wise investment in the future.

Notes

1. Paul Oyer, "Some Thoughts on the 'Gathering Storm,' National Security, and the Global Market for Scientific Talent," in *Perspectives on U.S. Competitiveness in Science and Technology*, eds. Titus Galama and James Hosek (Santa Monica, CA: RAND, 2007), 115.
2. Ibid., 114.
3. Ibid.
4. Ibid.
5. Thomas Kalil, "Planning for US Science Policy in 2009," *Nature* 443 (19 October 2006): 751–52.
6. Thomas Lee and Proctor P. Reid, eds., *National Interests in an Age of Global Technology* (Washington, DC: National Academy Press, 1991), 5.
7. Matt Kelley, "Report: U.S. Missile Science Slumping," *USA Today*, 23 March 2006.
8. National Science Board, "Key Science and Engineering Indicators: 2010 Digest," <http://www.nsf.gov/statistics/digest10> (accessed 22 January 2010).
9. Ibid.
10. Acceleration Watch, Web site, www.accelerationwatch.com (accessed 20 January 2010); and John Smart, briefing, Air War College, Maxwell AFB, AL, 28 October 2009.
11. Ibid.
12. National Science Board, "Key Science and Engineering Indicators: 2010 Digest."
13. National Science Board, "Digest of Key Science and Engineering Indicators 2008," <http://www.nsf.gov/statistics/digest08> (accessed 13 December 2009).
14. Thomas Friedman, *The World Is Flat* (New York: Farrar, Straus and Giroux, 2005).
15. Walter Alan Juzukonis, *Strengthening the Scientific Capacity Available to Serve the Nation* (Carlisle Barracks, PA: US Army War College, 2009).
16. Katalin Szelényi, "Students without Borders? Migratory Decision-Making among International Graduate Students in the U.S.," *Knowledge, Technology, and Policy* 19, no. 3 (September 2006): 5.
17. Ibid., 4.
18. Ibid.
19. T. A. Frank, "Green Cards for Grads," *Washington Monthly*, May/June 2009, A7–8.
20. Alan I. Leshner, "A Wake-Up Call for Science Education," *Boston Globe*, 12 January 2009, A11.
21. Barack Obama, "Remarks at the National Academy of Sciences," *Daily Compilation of Presidential Documents*, 28 April 2009, 1.
22. Ibid., 2.
23. Ibid.
24. Office of Management and Budget, "The President's Budget for Fiscal Year 2011," <http://www.whitehouse.gov/omb/budget> (accessed 28 July 2010).
25. "8th Continent Project: Four Colorado Institutions Launch Statewide Science and Technology Education Collaborative," *Defense and Aerospace Week* 44 (July 2009): 44.
26. "Rep Forbes Announces Funding to Advance Math, Science, Technology Education for Minority Students," US Fed News Service, 10 October 2009.
27. Christopher Kinnan, briefing, subject: Deterrence Operations, to Blue Horizons students, Air War College, Maxwell AFB, AL, November 2009.
28. Space Foundation, *The Space Report 2009: The Authoritative Guide to Global Space Activity* (Colorado Springs, CO: Space Foundation, 2009), 88.

29. Ibid.
30. Ibid., 99.
31. Ibid.
32. Smart, briefing.