VOLUME TWO

# IN SUPPORT OF THE COMMON DEFENSE

## A HOMELAND DEFENSE AND SECURITY JOURNAL

Editors:
Professor Bert B. Tussing, Dr. Brian Nussbaum,
Colonel Thomas Keegan, Colonel Karl Bopp
and Ritchie Dion

U.S. ARMY WAR COLLEGE PRESS
Carlisle Barracks, PA

CENTER for STRATEGIC LEADERSHIP and DEVELOPMENT
CSLD
U.S. ARMY WAR COLLEGE

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **JUN 2013** | | **00-00-2013 to 00-00-2013** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **In Support of the Common Defense: A Homeland Defense and Security Journal. Volume 2** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br>**U.S. Army War College,Center for Strategic Leadership and Development,650 Wright Avenue,Carlisle,PA,17013-5049** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | **Same as Report (SAR)** | **192** | |

# In Support of the Common Defense

## A Homeland Defense and Security Journal


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

# IN SUPPORT OF THE COMMON DEFENSE

## A Homeland Defense and Security Journal

**Volume Two**

**Editors:**

**Professor Bert B. Tussing, Dr. Brian Nussbaum, Colonel Thomas Keegan, Colonel Karl Bopp and Ritchie Dion**

**In Support of the Common Defense**

*A Homeland Defense and Security Journal*

**Volume Two**

**June 2013**

**Executive Agent for this publication:**
**United States Army War College**



**This publication is available on line at:**

**http://www.csl.army.mil/AllPublications.aspx**

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

# Contents


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

# Foreword

**Douglas B. Campbell**
Director, Center for Strategic Leadership and Development

One of the enduring missions of the Department of Defense, and the United States Army, has been to defend the United States homeland from foreign aggression and those threats that might endanger its sovereignty, its infrastructure, or its citizens. From the American Revolution to "Superstorm Sandy," the United States Army has played a key role is safeguarding not just American interests around the world, but the American people at home. While Strategic Landpower – one of the U.S. Army's defining focuses – is often viewed narrowly as focused solely on war-fighting, a quick look at the history of the United States shows that it has been applied selectively to suppress insurrection, to respond to disaster, and to otherwise support civil authorities – all in ways that are well within the authorities, legal framework, and intent set forth by our founders. Strategic leaders across the federal interagency, and within the U.S. Army, are well served by having a strong understanding of the threats facing the U.S. homeland, the capabilities that exist to respond to such threats, and the challenges and emerging issues that face the United States in this realm.

We at the United States Army War College have long recognized this priority, and have had the good fortune to play a role in expanding the knowledge of the various issues surrounding homeland defense and homeland security. Through the Homeland Defense and Security Issues group (HDSI) of the Center for Strategic Leadership and Development (CSLD), we have sought to foster dialogue, support research, and educate strategic leaders on these subjects. CSLD has a long history of sponsoring research, developing courses, hosting forums, and conducting strategic level exercises on issues surrounding homeland defense and homeland security.

The increased focus on homeland defense and homeland security missions since the tragic attacks of September 2001 might offer the misleading sense that such missions are novel, rather than part of a

long tradition that included missions surrounding civil defense, consequence management, and Defense Support of Civil Authorities (DSCA). While the responses to recent events like Hurricane Katrina and Hurricane Sandy stand out in our minds, it is worth remembering historic actions taken by the Army in support of civil authorities in cases like the Mississippi River floods of 1882 or the Great San Francisco Earthquake of 1906. Protecting the United States homeland and people from external threats, and from the consequences of disasters and catastrophes, is not a new mission.

Homeland defense, homeland security, and DSCA are not new mission sets, nor are they ones that can be undertaken lightly. Much like war-fighting they demand thoughtful planning processes, informed leadership, force structure, supplies and logistics, and other institutional focus to be done well; because like war-fighting, they too are often matters of life and death. It is with these needs in mind, that we at CSLD present the following collection of research articles on issues of concern to those interested, and those charged, with understanding homeland defense and homeland security.

# Section One

## Recommitting Against Complacency


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

# Introduction

**Professor Bert B. Tussing**

Homeland Defense and Security Issues Group
Center for Strategic Leadership and Development
U.S. Army War College

When members of the United States Army War College's class of 2012 began their Strategic Research Projects (the dreaded SRP's), few, if any of them were cognizant or concerned over what has led us to the edge of a fiscal cliff, seemingly destined to tumble into sequestration. Most, however, would be predicting a continued drawdown in Afghanistan, which would accompany actions already having taken place in Iraq. Those predictions, of course, would lead to pervasive discussions over cuts in resources – including, for the Army, that most precious and measurable resource – manpower.

That inevitability looms exponentially over the military with the specter of sequestration. Even without the additional impetus, there is no doubt that what we hopefully see as the waning hours of two wars will deliver the kinds of cutbacks that have historically come at the ends of our conflicts. Those historic reductions, however, have not always proven to be the wisest. Consider, for instance, the massive cuts in the National Guard that heralded the "peace dividend" at the end of the 20th Century…just in time for the unprecedented increases in operational tempo for these same National Guard units that began steady play through Bosnia-Herzegovina, Kosovo, Afghanistan and Iraq. Cuts, of course, were not borne solely by the Guard; but given that the focus of this volume is Homeland Defense and Civil Support, it is appropriate that we spotlight those reductions in anticipation of the vulnerabilities a new set of reductions will engender.

An old American Indian tale reminds us that it is easy to discern the programs and missions that are most important to us: they are the ones that we feed. Now this preference can come directly in funding, but it is also displayed in our strategies, our focus on doctrine, and the

alignment (or realignment) of our forces. The United States military, for instance, has made unprecedented commitments to domestic civil security missions in the development of the Chemical, Biological, Radiological and Nuclear and High Explosive Yield (CBRNE) enterprise; on the other hand, the paucity of forces actually assigned to the United States Northern Command (USNORTHCOM) still leaves some questioning the actual commitment of the of the Department of Defense (DoD) in terms of the active component. In his paper, Lieutenant Colonel Harry Culclasure correctly notes that Defense Support of Civil Authorities (DSCA) as a mission had gained steadily in prominence up until the 2010 Quadrennial Defense Review. But will that focus be sustained? Is there, for instance, a message conveyed in the *Defense Strategic Planning Guidance*,[1] released less than two years later, wherein of the ten "primary missions of the U.S. Armed Forces," homeland defense and support to civil authorities is listed seventh?

This is hardly meant to decry or demean the progress that has taken place in homeland defense and civil support. The establishment, nourishment and maturation of USNORTHCOM and the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs are clear signs of commitment from the DoD to these ends. The recent addition of the Chief of the National Guard Bureau to the Joint Chiefs of Staff was likewise reflective of a new revitalization toward domestic security in the Pentagon.

Moreover, the partnership efforts supported, stimulated, and even initiated by the DoD in deference to its civil masters stands as testimony to an enhanced commitment. The growth of the CBRNE enterprise has seen a remarkable transition that saw deliberate plans and resources coming out of a Department that had heretofore stood firmly against specified expenditures for purely "domestic" ends. In a steady progression – from Weapons of Mass Destruction Civil Support Teams (WMD-CST), through CBRNE Emergency Response Force Packages (CERF-P), through the evolution of the CBRNE Consequence Management Response Forces (CCMRF) to the current Defense CBRN Response Force (DCRF), and finally the Homeland Response Forces (HRF) associated with each FEMA region – the active

and reserve components of our military have made commitments well beyond just words (or even acronyms).

Likewise, those commitments have taken form across both interagency and intergovernmental partnerships. DoD's commitment to its support role in the interagency process has been demonstrated from planning through execution. Scores of detailees from the Department were instrumental in standing up its civil security counterpart, the Department of Homeland Security (DHS), and many continue to serve there in both permanent and adjunct functions. Operationally, through the auspices of the Economy Act, the Department routinely participates in taskings in support of DHS, the Department of Justice, and other members of the federal interagency.

Beyond this type of interagency cooperation are intergovernmental initiatives that have resulted in far greater alignment between the DoD and state and territorial governments. Seeking to emulate the long established ties held by the states and territories and their respective National Guards, the USNORTHCOM and the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs have actively pursued measures to achieve greater unity of effort. Notable among these cooperative efforts is the Joint Action Plan formulated between the Department and the President's Council of Governors,[2] that has provided for significant gains in terms of crises planning; shared situational awareness; logistic mobilization, staging and distribution; and preparing mission assignments ahead of events requirements in order to expedite response when the crises arise. Perhaps most notable, however, is the cooperative effort that has resulted in the training, designation, and employment of Dual Status Commanders. These general officers, appointed and approved in memoranda reached between the President and the states, are a mechanism by which active duty forces, service reserves and their National Guard counterparts may be brought under a single commander to most efficiently coordinate a "total force" response to the states when conditions demand it. Application of the concept has already been put to the test in 2011 in response to Hurricane Irene, and 2012 with Hurricane Sandy.

Taken together then, the progress achieved by the DoD in civil support is both remarkable and admirable. But the threats and hazards which

served as impetus for these improvements leave no room for a new sense of complacency. Manmade threats to the security of our people, from within and without, pepper both the media and our intelligence reports. Natural phenomena of extraordinary frequency and severity have levied new demands against the whole of the nation's government, to the extent that the outgoing Secretary of Defense has declared climate change and its effects have had and continue to make "a dramatic impact on national security."[3] In these affairs, taking a strategic pause is inviting strategic failure.

The authors of the papers in this section have made note of the improvements in the military's stance for response and recovery, but are each calling for improvements, as well as greater commitments in terms of prevention and preparedness. Lieutenant Colonel Culclasure decries the "seam of uncertainty" that remains between the missions of law enforcement and defense, as exercised predominantly by the DoD and Homeland Security. He suggests that great gains could be made towards closing these seams if unnecessary obstacles between the varied stakeholders in the "homeland security enterprise" were removed. Chief among these, Culclasure contends, are obstructions against integration and interoperability, such as restrictions in information sharing born of over-classification, overly restrictive security clearances, and other governance issues. He reminds the reader that, for the enterprise to truly be responsive, it requires the ability to access and share information not just "horizontally," across the federal interagency; but likewise "vertically," across frequent barriers between federal, state and local governments.

Lieutenant Colonel Brian A. Barthel continues the theme of information exchange, but this time not so much in method as in mechanism. Beginning with a review of current national policies, procedures, and technologies for managing large-scale emergencies, he offers challenges to the same, and identifies opportunities for improvement. Central in his approach for enhancing the government's response in times of crises is a call for implementing a nationwide interoperable communications system to facilitate a "common operating picture" for first responders – both civil and military. Taken alongside a call for integrating "all-hazard" planning across every level of government and the private

sector, Barthel contends that a concerted civil-military effort in both preparedness and response could rise above pitfalls that too frequently characterize operations in our imperfectly coordinated federalist state.

Perhaps the most controversial among the proposals in this section are those offered by Lieutenant Colonel Michael Bentley, who suggests that in times of crises, augmentation forces from the active component of the U.S. military should be placed under the "tactical command" of the governors of the states receiving their assistance. Bentley's proposal has a logical development through the lens of ultimate responsibility for the immediate response to a disaster – and perhaps even more when viewed against the longer view of recovery from the same. But the proposal is sure to stir debate in an environment that has already made steps towards these apparent ends through measures like the Dual Status Commander concept. Nevertheless, the position may add to the persistent debate over the most appropriate application of the federal component of military power in the sovereign states, as it plays out through discussions surrounding the Posse Comitatus Act, the Insurrection Act, and the regulations pertaining to the same. Moreover, it may force the debate toward clarification of how restrictive these laws and regulations are in fact, as opposed to popular perception.

The trend against shrinking from controversy continues in the final paper of this section, offered by Colonel Tim Lawson of the Wisconsin National Guard. Against growing concerns over variable threats against our borders, Colonel Lawson suggests establishing a permanent presence of the National Guard as an augmenting force to DHS's Customs and Border Protection (CBP). Lawson argues that the last two Administrations' commitment of the Guard in support of CBP along the southwest border of the United States is proof enough of the requirement, while acknowledging that said support was deliberately limited to assisting the force in intelligence, surveillance, reconnaissance and infrastructure development. But pointing to the sustained requirement there, along with the frequently overlooked border with Canada, he suggests that the piecemeal approach that has characterized the Guard's employment to date is wanting. As commitments in Iraq and Afghanistan approach an end, Lawson suggests that this new mission could serve as a means of sustaining the hard-gained levels of

proficiency now enjoyed by so much of the National Guard, and make a vital contribution to an interagency commitment to our nation's security in the process.

There is far more nuance, detail, and insight contained in these research papers than this introduction is intended to provide, of course. But hopefully this prologue will serve to contribute to the authors' combined goal of maintaining a focus on homeland defense. That focus may be in danger of a dual diversion: first, against what many believe is a growing atmosphere of complacency; and second, against rising concerns over budgetary cuts to the "global commitment." The military is right to continue to think of its obligation to the nation's security as a "defense in depth." But we should not lose sight of the fact that the depth of our concerns begins at home.

# Homeland Security and Homeland Defense: The Seam of Uncertainty Unstitched

**Lieutenant Colonel Harry Culclasure**
United States Army

> *…we will not be able to deter or prevent every single threat. That is why we must also enhance our resilience—the ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.*
>
> —President Barack Obama[1]

Following the tragic events of September 11th 2001, the United States embarked on a series of efforts to combat terrorism, including the establishment of the United States Northern Command in 2002 and the Department of Homeland Security (DHS) in 2003. In 2005, Hurricane Katrina caused unprecedented damage across multiple state and local governments, challenged our emergency preparedness, and ultimately demonstrated how quickly our civilian and military first responders could be over-extended in large natural disasters. These two separate events became the focal response incidents on which to base our national response enterprise for the federal government. In the past ten years the government established or combined multiple agencies and vertical layers to improve our planning, execution, and recovery from disasters. The Department of Defense (DoD), playing a supporting role in Defense Support of Civil Authorities (DSCA), also established a new command to assist in natural and man-made disasters. DSCA adds a second mission space apart from DoD's Homeland Defense mission and the protection of U.S. sovereignty and territory. This paper intends to study the ends, ways, and means and identify shortcomings where the seams between Homeland Security and Homeland Defense become apparent in preventing, protecting, responding to, and recovering from natural and manmade disasters. Current strategic policies represent our desired ends; the policies' application represents the ways; and the agencies and

units required to accomplish the Chemical, Biological, Radiological and Nuclear and High Explosive Yield (CBRNE) response mission represent the means. After reviewing the response enterprise from the top down the paper intends to identify the capability gaps that still remain in the enterprise and make recommendations for their improvement.

## The New York Example

As one of the most targeted cities for terrorism, New York City (NYC) invested more than $3 billion dollars to address the terrorism threat and make it a difficult target for future acts. In a *60 Minutes* interview aired on 25 September 2011, Raymond Kelly, the NYC Police Commissioner, reviewed the personnel, equipment, and tactics the city uses to deter and respond to emergencies. The city employs over 35,000 uniformed police officers, maintains well over 2,000 cameras, and uses swarming techniques to take over city blocks. It constantly monitors the harbor and vehicles entering the city with sensitive radiological detectors and software that recognizes potential hazards on the streets. To gather intelligence on emerging threats, the city employs linguists in sixty languages across the world.[2] These linguists report back to the city's counter-terrorism group, where their information is used to develop estimates on activities. Intercepted phone calls from potential terrorists have confirmed that these techniques are effective. To date it appears the city's deterrence methods are working and would-be terrorists need to look elsewhere at less capable cities.

New York City stands as an example of how coordination, information sharing, and response units, when used together, close the seams between "prevent, prepare, respond and recover." NYC is one of the few cities in the United States which commands a budget large enough to afford these capabilities, and can respond with little help from outside agencies. Other U.S. cities and communities do not have the funds (or the constant terrorist threat), and will require assistance when man-made or natural disasters occur. For them, as suggested by New York's example, the answer is a multi-layered and partnered response. That answer is written throughout the documents discussed in this paper, but enacting the collaboration, information sharing, and capabilities of the players needed to execute that answer remains elusive.

## The Ends: Interagency and Department of Defense Objectives for Emergency Response

The strategy for Homeland Security and Homeland Defense begins with national-level objectives designed to communicate and promote collaboration within the government. These documents set the stage for combined strategy to protect the homeland and nest all the way down to the response level – or means – contained in the civil and military components of our Nation's government.

The National Security Strategy (NSS) identifies threats at home in the United States that include terrorism, natural disasters, cyber-attacks, and pandemics.[3] It provides the federal government's objectives – or ends – based on current U.S. priorities. The strategy calls for enhancing security at home and effectively managing emergencies through all levels of the government and the private sector. It calls for "individual and community preparedness and resilience through frequent engagement" that supplies clear information to the public.[4] As noted in the NSS, the United States cannot expect to prevent or deter the potential damage caused by every terrorist plot or natural disaster.[5] To reduce an event's effect, the NSS calls for investment in preparedness throughout all levels of government to include planning, equipping, and information sharing and collaboration across all response elements.

To build upon the guidance in the NSS, President Obama issued *Presidential Policy Directive 8: National Preparedness,* which established the national preparedness system. The system allows the nation "to track the progress of our ability to build and improve the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from those threats that pose the greatest risk to the… Nation."[6] It looks into risks trends all over the nation and "include[s] concrete, measureable, and prioritized objectives to mitigate the risk."[7] The risk data is placed in frameworks coordinated under a "unified system with a common terminology" and built upon "basic plans that support an all-hazards approach to preparedness."[8]

As a supporting document to the NSS, the 2010 Quadrennial Homeland Security Review (QHSR) report effectively replaced the 2007 National Strategy for Homeland Security (NSHS). The

QHSR was the first document to look at Homeland security as an "enterprise…the collective efforts and shared responsibilities of Federal, State, local tribal, territorial, non-governmental, and private sector partners—as well as individuals, families, and communities…"[9] It stresses homeland security missions are not solely the responsibility of DHS, but are "*enterprise-wide*" and everyone has the responsibility for executing homeland security missions.[10] It expands a focus frequently limited to response and recovery, to incorporate mitigation and preparedness.[11] This shift in direction requires less of a "top-down emergency management" approach, and engages all stakeholders from the state down to local government, nongovernmental organizations (NGOs), private sector, communities, and individuals.[12] At the core of response is the use of the National Response Framework (NRF) and the National Incident Management System (NIMS) which provide roles, responsibilities, and effective response mechanisms during disasters.

There are numerous gaps between local, state and federal governments (to include DoD) pertaining to information sharing and protocols needed to improve situational awareness during an incident. The QHSR addresses these shortfalls and calls for "greater real-time shared threat information and situational awareness.…avoid[ing] stovepipes that hinder appropriate information sharing and analysis…"[13] Additionally, it recognizes that in order to share information the entire homeland security enterprise "must use compatible information architecture and data standards" which avoids duplication and enhances preparedness.[14]

Homeland Security Presidential Directive 5 (HSPD-5), *Management of Domestic Incidents*, tasked the Secretary of Homeland Security to develop NIMS to close the gaps between federal, state and local entities. The objective was to "provide a consistent nationwide approach for Federal, State, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity."[15] It solidified the DoD's support to civil authorities and tasked the Secretary of Defense and Secretary of Homeland Security to establish "appropriate relationships and mechanisms for cooperation and coordination between their two departments."[16] HSPD-5 also established the National Response Plan (NRP), updated as the National Response Framework (NRF), and

defined the roles and responsibilities of government in terms of an "all hazards" plan. These two documents, the NIMS and the NRF, are the synthesis to provide a unity of effort between the military and the civilian sector. The relationship and coordination between DoD and the rest of the Interagency is crucial to response, and is emphasized in the 2010 QHSR. It stresses the need to "strengthen unity of effort between military and civilian activities.…and revise strategy and doctrine accordingly."[17] The 2010 QHSR was the first document to place a strong emphasis on this relationship and call for a unity of effort for disaster response from federal, state, and local levels.

The DoD Quadrennial Defense Review (QDR) report emphasizes DoD contribution in Defense Support of Civil Authorities (DSCA), a role that "has steadily gained prominence."[18] It explains the Department's role in DSCA, in support of DHS as the lead federal agency, and/or in support of a governor's request under Title 32.[19] The QDR reviewed the force capabilities and identified areas where DoD could most affect the DSCA mission. Among the recommendations that emerged from the review was a call for more capable CBRNE Consequence Management Response Forces (CCMRF). The CCMRF is a Title 10 force consisting of 4,700 soldiers in three brigade sized units – two from the National Guard and one from the Active component – with operations, aviation, medical and other specialized units. Its primary mission is to "augment the consequence management efforts of the first responders."[20]

The QDR directed the reorganization of the CBRNE Response Enterprise. The CCMRF that had been stood up prior to the QDR's direction effectively became three units: the Defense CBRN Response Force (DCRF) and the two Command and Control CBRN Response Elements (C2CRE). Plans for the two National Guard CCMRFs were replaced with what have become ten Homeland Response Force (HRF) units, each aligned with a FEMA region. DoD introduced all of these changes in order to create a more flexible force with quicker response times, and to increase its ability to respond to simultaneous events. This new structure intends to capitalize on planning and coordination with FEMA in each of the regions.

The DoD and the rest of the Interagency produced clear guidance in the documents discussed and targeted similar ends to construct a layered approach to protect the homeland. For the Interagency to succeed in prevention, protection, mitigation, response, and recovery, it requires a forcing function to provide the whole of government response. The Goldwater-Nichols Act achieved "jointness" in the military; a similar act could assist the rest of the Interagency.

**The Ways: The Interagency Application of the Means**

DHS began operations in 2003 with the mission to prevent terrorist attacks, reduce our vulnerability, and minimize the damage if an attack occurs.[21] In the past ten years DHS grew to the third largest federal government agency with over 200,000 employees and $50 billion dollar budget. As previously noted, HSPD-5 tasked DHS to develop the NIMS and the NRP, which evolved to become the NRF.

The NIMS provides a proactive approach to organize the government, NGOs, and the private sector to respond to and recover from disasters. It is based on the premise that the use of a common, "incident management framework will give emergency management/ response personnel a flexible but standardized system for emergency management and incident response activities."[22] The system is based on five components: preparedness, communications and information management, resource management, command and management, and management and maintenance. The components concentrate on the ability to manage emergency personnel and equipment, maintain a common operating picture and interoperability, manage resources, and maintain command structure. It strives to produce a unified command where all players in a disaster work seamlessly toward a common goal to reduce the loss of life and property. The NIMS makes it clear that it is neither a response nor a communications plan, but a "comprehensive, nationwide, systematic approach to incident management, including the Incident Command System, Multiagency Coordination Systems, and Public Information."[23]

The NRF, a companion document to the NIMS, "is a guide to how the Nation conducts all-hazards response.…built upon *scalable, flexible and adaptable coordinating structures* to align key roles and responsibilities

*across the nation*."[24] To coordinate response and provide support, the Federal Emergency Management Agency (FEMA) organized its response capability into 15 Emergency Support Functions (ESF), such as firefighting, communications and transportation. The ESFs "bundle and funnel resources and capabilities to local, tribal, State, and other responders."[25] The application of the ESFs helps provide organized support to communities in need.

DoD produced three joint documents related to its Homeland Defense/ Civil Support mission in the 2006-2007 timeframe. Joint Publications 3-27, 3-28, and 3-41 each explain the critical missions tasked to the Department in Homeland Defense and Civil Support. All three reference the strategic documents mentioned earlier in this paper, and DoD's relationship to Homeland Security. They explain DoD's "place" in NRF and NIMS, and under what authorities it responds to crises in the homeland.

Joint Publication (JP) 3-27, *Homeland Defense*, gives an overall view of the homeland defense mission but also explains the relationships with other agencies in the government to achieve mission success. It acknowledges the communication gaps during the events of 9/11 and stresses the transition from a "'need to know' to a 'need to share' culture."[26] In JP 3-28, *Civil Support*, DoD explains the mission of Civil Support (CS), the Request for Assistance (RFA) process, and the roles of Title 10 and Title 32 forces in the homeland, informed by lessons learned from Hurricane Katrina. It reinforces the need to share information during a disaster because "information sharing and the interaction with agency liaison personnel prior to and during CS exercises and operations significantly enhance real-time information sharing and coordination activities and improve CS related response capabilities."[27] Finally, JP 3-41, *Chemical, Biological, Radiological Nuclear and High-Yield Explosives Consequence Management*, takes a close look at the CBRNE response capabilities in DoD. The publication challenges its commanders and staffs to understand the NRF and the NIMS, and know where their units fit in the overall response framework.[28] The document educates DoD members on the formation of the Joint Field Office where officials work to achieve unity of effort when dealing with a threat or hazard.

The three DoD documents discussed in this section give a clear guidance on the varying missions under Homeland Defense and Civil Support. Each uses the nation's strategic documents and reiterates the necessity to understand the NIMS and NRP and where DoD fits in it. Finally, they take the lessons learned from 9/11 and Hurricane Katrina to reinforce the need to share information across the response enterprise.

**The Means: DoD and DHS Resources in the Response Enterprise**

DHS and DoD work together during a domestic incident through FEMA and the United States Northern Command (USNORTHCOM). USNORTHCOM is responsible for the CBRNE Response Enterprise and supports the Primary Federal Agency in the event of a CBRNE event. It responds to RFAs according to the NRF when directed by the President or the Secretary of Defense. FEMA is responsible for coordinating federal response to disasters. Both USNORTHCOM and FEMA use the NIMS and the NRF to coordinate support for incident response. This section will explore the roles and responsibilities of each and the resources available to respond and recover from incidents.

FEMA became a part of DHS in 2003 with the mission to "support citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards."[29] With roughly 7,500 employees in 10 Regions throughout the United States, FEMA acknowledges it is not the "the team, but part of a team" that includes federal partners, state and local officials, and the private sector.[30]

To meet the demands for incident response, FEMA organized itself into the aforementioned regions to integrate disaster preparedness, incident management, emergency communications, and logistics. They rely upon existing community emergency response personnel and combine them into teams to respond to an event. These teams include capabilities such as Urban Search and Rescue and mobile communications to affected communities. The FEMA employees report to Regional Response Coordination Centers (RRCC). In the event of an emergency FEMA coordination is accomplished through the Joint Field Office (JFO) which coordinates all disaster response.

The direction of the DoD response enterprise changed in 2010 with the Quadrennial Defense Review. Prior to 2010 the enterprise basically consisted of the National Guard Weapons of Mass Destruction Civil Support Teams (WMD CST) and the CBRNE Enhanced Response Force Packages (CERFP). Three CBRNE Consequence Management Response Force (CCMRF) packages had been planned for: two from the Guard and one from the Active Component. As previously alluded to, only one CCMRF unit was ever stood up; plans for the other two were abandoned with the QDR's objectives.

To increase its ability to respond more quickly to disasters the QDR instructed DoD to restructure the CBRN Enterprise, with a particular focus on lifesaving capability, flexibility, and response times."[31] This direction resulted in the development of ten Homeland Response Forces (one in each FEMA region); a Defense CBRN Response Force; and two Command and Control CBRN Response Elements (C2CRE). The envisioned response time improved with the HRF response to no later than N+12, as compared to the old CCMRF at N+48.[32] The HRF's positioning in their respective FEMA region, under the governor's control, places them in a better geographical location to respond to crises. They are not as large as the prior mentioned CCMRF units. On the other hand their dispersed locations allow them an opportunity to work and train with FEMA thereby increasing their awareness and response time. All ten HRFs are currently manned and undergoing certification.

The CBRNE Response Enterprise actually began with the Civil Support Teams (CSTs). There are currently 57 CSTs with at least one in each of the states and territories (there are two each in New York, Florida and California). The teams consist of 22 active Guard personnel serving under Title 32 authority. The teams respond to state and territorial governors for the identification and survey of suspected chemical, biological, and radiological events. The teams deploy within 3 hours of notification with a mobile laboratory and a communications vehicle capable of classified communications and some limited voice and data (internet) communications with civilian first responders.[33]

The next tier in the response enterprise is the NG CERFP. There are currently 17 units consisting of 186 personnel, with a small number of Title 32 members (normally less than 25%). Their mission is to

conduct search and extraction, search and recovery, decontamination of affected personnel, and initial triage. CERFP units can deploy within 6 hours' notification.[34] Unlike the CSTs, the CERFP does not have a robust communications capability.

The Homeland Response Force (HRF) consists of 566 personnel in each FEMA region for a total of 5,660. The force maintains no more than 25% of its element in Title 32 status. Its mission is much like the CERFP; but it also contains a command and control element, security, and additional triage and treatment. The HRFs are required to deploy within 6-12 hours after notification.[35]

The CSTs, CERFPs, and HRFs are the first three echelons, other than civilian first responders, available to respond to a CBRN event. These elements remain under the command and control of a given state or territory's governor unless federalized. If the units respond to another state with the approval of the respective governor, the supported governor assumes tactical control of the unit.[36] This is accomplished through interstate agreements, the most notable of which is the Emergency Management Assistance Compact (EMAC). This mutual assistance agreement provides support to "any emergency disaster that is duly declared by the Governor of the affected state" and includes events such as "natural disaster, technological hazard, man-made disaster, civil emergency aspects of resources shortages, community disorders, insurgency, or enemy attack."[37] The EMAC is granted under public law by Congress.

The Defense CBRN Response Force (DCRF) and the Command and Control CBRN Response Elements (C2CRE) are the first Active Component response forces in the enterprise allocated to USNORTHCOM. The DCRF is primarily an active duty force but can contain Reserve and National Guard elements. It consists of 5,200 personnel: 2,100 in Force Package 1 (FP1) and 3,100 in Force Package 2 (FP2). FP 1 is required to deploy within 24 hours of notification and FP 2 within 48 hours. The DCRF is the first unit to bring rotary wing aircraft for patient evacuation, as well as level III medical care. The C2CRE A and B packages provide an additional 1,500 personnel from the Active and Reserve Forces. They have capability similar to the DCRF, but are composed of smaller units. National Guard CSTs,

CERFPs, and HRFs from unaffected areas can be federalized to provide additional capability to the DCRF. The C2CRE is required to deploy in 96 hours.[38]

The events of 9/11 and the lessons learned from hurricanes and other natural disasters forced the federal government to review its response enterprise to garner a more robust response. The United States now has a very capable, well trained, and equipped response force for disasters, but there are numerous limitations to its current configuration. These limitations include proposed response times, common operating pictures, and general knowledge of and between DHS and USNORTHCOM. These themes are common throughout all the documents previously explored in this paper.

**Limitations to the Response Enterprise**

While the United States adjusted the size and locations of units responsible for emergencies, the most important traits are rapid response, life-saving capabilities, the ability to share information, and the capacity to make timely decisions during a crisis. This section explores some of the limitations in the processes and the response forces.

Military first responders such as the CSTs, CERFP, and HRF are controlled by the state governor, who in most cases, places them on State Active Duty (SAD) for response. The CSTs are the only unit in the Guard on active duty for immediate response to a Chemical, Biological, Radiological and Nuclear event. The CERFP are the first to respond with lifesaving capabilities but have only 25 percent of their force on Title 32 status at any one time; only 45 of the 186 personnel are available for an unanticipated emergency event. This is not a criticism of the Guard or the training level of the CERFP, but one example of time factors that can limit response. The six hour assembly time for the CERFP, combined with the travel time to the incident site, is crucial when an unanticipated event occurs. This time lag limits the initial assessments sent to the governor, and adds more time to the decision-making process if additional forces are needed for response.

The HRF is in a similar position. Even with a response capability within twelve hours, the HRF faces a shortcoming by only maintaining 25% of its personnel in Title 32 operational status.[39] The HRF cannot assemble and deploy until the governor places them in SAD. In an unanticipated event the HRF has 141 personnel immediately available for response, and some of those may not be part of the lifesaving capability. Even with the quick assembly time for the HRF, they can still expect to travel up to 500 miles to the incident site. Multiple incidents in the same FEMA region or on state borders can cause even greater problems. Governors may hesitate to acknowledge an EMAC as they assess the damage and danger to their particular state. All of these considerations add precious time to the lifesaving capability the CERFP deliver.

The DCRF faces a greater challenge in relation to time. Domestic response, as with all DSCA, is driven by the RFA process from civil authorities.[40] The President or the Secretary of Defense direct the response to an RFA. It is forwarded to USNORTHCOM in accordance with the NRF to support a primary agency, e.g., FEMA.[41] Once USNORTHCOM receives the order it may take up to 24 hours for the DCRF to begin movement to the incident site. The availability of air transport and proximity to the incident play a large factor on the success of the response. The initial 96 hours after an event offer the greatest opportunity to save lives and poses one of the greatest challenges.[42] A USNORTHCOM CBRN Response Enterprise brief to its Senior Steering Group, dated 23 September 2011, emphasized the time involved in HRF and DCRF deployments. The brief called out the number one concern as "can we get there in time?"[43] To address the deployment timelines USNORTHCOM utilizes Deployment Readiness Exercises (DRE) as the key to measure a unit's ability to deploy and its installation's capability to support a deployment.[44]

The notion of time also permeates the decisions state, local, municipal, and tribal leadership consider during an emergency. After an incident occurs it is imperative the leadership in the community or state receives the best timely information to make informed decisions. According to the NRF, "incidents must be managed at the lowest possible jurisdictional level and supported by capabilities when needed."[45] Immediately following an unanticipated event the ability to receive

accurate information can prove challenging. While the local authorities and first responders react to the event they may not know if the incident exceeds their capabilities. As the NRF states, "it is not always obvious at the outset whether a seemingly minor event might be the initial phase of a larger, rapidly growing threat."[46] Once the community requests assistance from the state more time is used to assess what resources are needed at the state level. If the governor expects the incident to exceed the state's capability he/she may request assistance from other states via EMAC or other agreements. If the event overwhelms or is anticipated to overwhelm the state's capability, the governor may request assistance from the federal government. To request this assistance the governor can request assistance under the Stafford Disaster Relief Act. The Stafford Act authorizes the President to "provide financial and other assistance…certain private nonprofit organizations, and individuals to support response, recovery, and mitigation efforts."[47]

Most events do not warrant the use of a Presidential declaration, but when necessary the governor must ensure all state functions are potentially overwhelmed and issue a formal request to the President. The governor's request for a Presidential declaration must include a survey of the area, a joint damage assessment with FEMA, and a consultation with the regional FEMA administrator for eligibility.[48] This process takes up precious time needed to activate response forces and for them to move to the incident site.

The NRF does allow for a proactive response to unanticipated events, such as CBRNE threats, that can cause catastrophic loss of life and property. The NRF provides an ability to pre-position federal assets "in anticipation of a formal request from the state for federal assistance," allowing for a proactive means to provide support.[49] The notion of a proactive response makes the need for information sharing even more important. There are too many time variables involved in domestic response from the local to state to federal which depend upon accurate, timely information. A local government can quickly become overwhelmed in an incident which then adds time to the state and additional time to the Federal response. These times only improve when the whole of government shares intelligence and response information in the form of a common operating picture (COP), the "overview of

an incident created by collating and gathering information…from agencies/organizations in order to support decisionmaking."[50]

The 2010 QHSR underscores the necessity to shorten the information sharing process through the entire enterprise, and not just within DHS. It stresses the need to "avoid stovepipes that hinder appropriate information sharing and analysis, and foster greater information sharing"from a "top-down command and control model to a more bottom-up approach."[51] Information sharing throughout the enterprise can unquestionably improve response times from the local, to the state, and up to the federal level. While the solution is easily recognized, achieving the end state is much more complicated. Gaps still exist within the intelligence community and DHS due to an inability to supply a single enterprise information system that meets the requirements for all.

The enterprise suffers from several factors that inhibit its information sharing and networking. Security clearances, over classification, and governance issues all contribute to a lack of integration and interoperability. For the enterprise to truly be responsive it requires the ability to access and share information not just vertically but horizontally.

One of the most critical factors that hamper information sharing in the intelligence community is the governance issue. DHS as it operates now "is poorly positioned to receive intelligence from the intelligence community agencies because it does not do intelligence collection on its own."[52] Without political support from the Congress and control of a budget, the Director of National Intelligence (DNI) cannot break down the stove pipes and the resistance to reform that exists in the intelligence communities.[53] No one in the intelligence community has the ability to collect and process all the available information into actionable intelligence.[54] To remedy this shortfall and transform the community the DNI needs to establish a new community based on collaboration and abolish the current rivalries. The Goldwater-Nichols Act of 1986 is an example of reform that streamlined the command structure within DoD. It created a "unified military establishment and, among other things, laid the foundations for a 'joint' military."[55] A similar act from the Congress could establish a more collective intelligence environment. The act could break down the barriers of

the "need to know" culture past the "need to share" and into a mindset of "responsibility to provide."[56] These communities need to overcome past biases and provide threat information across the enterprise while protecting the source.

Before any intelligence is provided the community must also confront security clearance issues. There is an "inability or unwillingness on the part of DHS and FBI to work effectively together" on this issue.[57] Many states and some major metropolitan areas maintain fusion centers, a central repository on intelligence mainly tied to law enforcement, with "a higher degree of vertical (federal intelligence community) and horizontal (state/local) collaboration."[58] These fusion center operators require security clearances to receive, analyze, store, and disseminate this classified information. There are reported cases where the FBI did not accept DHS security clearances; and others where DHS required verification from fusion centers that personnel possessed an FBI clearance, certified to DHS from the FBI.[59] These occurrences frustrate the state fusion centers, which are not funded through federal dollars but by the individual states.

Even if the fusion center personnel receive the clearances, a problem still exists with the over-classification of intelligence. The Interagency lacks an overarching policy on Sensitive but Unclassified (SBU) documents, which doubled since 2001, and procedures that deal with the designation of these documents.[60] The SBU documents are of "particular importance to homeland security," but the designations are "misapplied and disjointed."[61] This lack of understanding on classifying material is a serious impediment to sharing information. According to the 2006 Government Accountability Office Report 06-385, the government used fifty-six different SBU designations and applied them on information that did not warrant classification.[62] This misuse of classification denies state and local fusion centers the ability to act on intelligence that may affect their community or even add their own information and build upon it. If a cleared operator in a fusion center receives classified information they cannot declassify and share it with others. Even with an emphasis in our strategic documents on information sharing, "making information available to participants

(people, processes, or systems)," there is still a tendency for agencies to limit their dissemination procedures with one another.[63]

Finally, in order to share information across the enterprise the government needs a network where all communities can collaborate. The solution for this requirement is a network that addresses "user needs and concerns at all levels….Just as important as the ability to share information is the willingness on the part of emergency managers to share information."[64] In 2004, DHS launched the Homeland Security Information Network (HSIN) as the primary means for the whole of government to share information. Unfortunately, DHS launched the system without studying the current environment and evaluating the systems used by the states and local communities.[65] They failed to consider the existence of other systems already used in the field by law enforcement, such as the Regional Information Sharing System (RISS), the Joint Regional Information Exchange System (JRIES), Law Enforcement Online (LEO), and an oversight mechanism incorporating these systems.[66] HSIN not only overlooked law enforcement systems, it failed to consider the more than fifteen different Emergency Operating Center (EOC) software options used in the states.[67] The oversights highlighted the fact that the system lacked integration with state EOCs.[68] In addition, studies indicated it had privacy issues, was not user friendly, and did not handle all events expected.[69] As a result of these pronounced shortcomings, DHS saw a requirement to establish a Homeland Security Information Network Advisory Committee (HSINAC).[70]

The HSINAC meets to gather information on the HSIN, and works to enhance and promote information sharing. The committee recognized its main obstacles to be "cross boundary and cultural issues… across jurisdictions, levels, and functions of government."[71] DHS acknowledges the existence of duplicative systems, but has no authority to enforce the use of HSIN. When questioned on law enforcement use of HSIN, the HSINAC admitted most of those agencies use LEO and RISS systems, and there would not be a change for the next few years.[72] Law enforcement's concern with HSIN was information overload with duplicative systems, and the need for the Department of Justice and DHS to work together to eliminate competing systems

for state and local users.[73] The primary DoD HSIN user, the National Guard, only posts to HSIN when it is approved by leadership, due to authentication, security concerns, and systems access.[74] These limiting factors of the HSIN challenge the preparedness of the nation to share intelligence and respond to a natural or manmade disaster.

## Conclusion

Since the terrorist events of 2001 and Hurricane Katrina in 2005, the Federal government focused efforts, "aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the nation."[75] National preparedness not only involves response but a whole of government collaboration focused on "prevention, protection, mitigation, response, and recovery."[76] USNORTHCOM plans to train and equip smaller, more responsive units, which are more closely tied to the civil agencies they support. While the government is better prepared for natural and man-made disasters, it still lacks the information and intelligence sharing capability needed to prevent and respond to these events. There is still a substantial gap between the intelligence community and DHS, and their ability to collaborate with local law enforcement and fusion centers in the states. Incidents begin and end locally, but to achieve true success there is a need to involve "multiple jurisdictions, levels of government, functional agencies, and/or emergency responder disciplines."[77] There is a "seam of uncertainty" in the response enterprise, but it appears to be in collaboration, not in mission overlap. In the past ten years the government identified and closed seams in response and recovery by establishing DHS, USNORTHCOM, and their associated units. The remaining seams involve our information sharing capacity and collaboration.


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

# 9/11 Ten Years After: Command, Control, Communications Remain An Issue

**Lieutenant Colonel Brian A. Barthel**
United States Air Force

> *One of the most critical things in a major operation like this [response to 9/11 attacks on New York City's Twin Towers] is to have information. We didn't receive any reports of what was seen from the [NY Police Department] helicopters. It was impossible to know how much damage was done on the upper floors, whether the stairwells were intact or not.*[1]
>
> —Fire Chief, New York City Fire Department

The 9/11 terrorist attacks were a watershed event for the United States of America. They opened the nation's eyes, bringing the realization that this powerful nation is not immune to asymmetric attacks from non-state actors. They also painfully revealed the need to improve homeland security, specifically response efforts. The magnitude of these attacks required responses from all levels of government, local, state, and federal, as well as private and non-governmental support. The devastating problems arising in these responses brought to light significant command, control, and communication (C3) shortfalls, not only among responding organizations, but also within them and across all levels.

The *2010 National Security Strategy* (NSS) cites the security of the United States and its citizens as an enduring national interest.[2] It further stipulates the requirement to strengthen security and resilience at home to counter the full range of threats, from natural disasters to terrorist attacks. The primary NSS goal is to prevent these dangers. However, if deterrence fails, national security requires effective rapid response and recovery operations.[3] To meet this challenge, the United

States must integrate its all-hazard planning through collaboration at all levels of government and with the private sector. To assure such collaboration the nation must invest in a reliable, interoperable, survivable communications system for first responders.[4]

This paper reviews the nation's current capabilities to respond to significant incidents, both natural and manmade. To respond effectively, multiple agencies (from local, state, and federal government to the private sector) must manage their collective assets and provide critical support as a cohesive team. They include the broad range of first responders, fire, medical, and police. The unity of effort needed to provide timely, efficient, and integrated responses can only be achieved through effective C3 within and among responding forces. To effectively support the 2010 NSS, responders need interoperable communications among all agencies, a mechanism to track personnel, and share a common operating picture (COP). This paper reviews current national policies, procedures, and technologies for responding to national emergencies. It identifies challenges and opportunities for improvement. It concludes with recommendations for implementing a nationwide interoperable communications system that, along with an effective tracking system, will facilitate the formulation of a COP for first responders.

## Background

The events of 9/11 were surely eye-opening. But this was not the first event, manmade or natural, to reveal the need for better integration of first responders. The December 1993 terrorist bombing of the World Trade Center (WTC) revealed significant C3 issues. Responding forces were dispatched by different control centers and were not operating on the same radio frequencies, so they could not communicate with one another.[5] Even when leaders of different responders were collocated, they often used different terminology. For example, "fire" could mean a blaze or a gunshot. Lastly, as experienced during 9/11, communication was lost with responding forces inside the WTC; radios could not penetrate the numerous steel and concrete floors; and too many units using the same point-to-point channel rendered communications ineffective.[6]

These issues impeded emergency agencies from rapidly and comprehensively responding to the incident and from effectively performing their primary mission to protect the public.

As a result of the 1993 WTC bombing, the New York/New Jersey Port Authority (responsible agency for the WTC) invested $100M to make physical, technological, and structural improvements, and to improve fire safety plans and procedures.[7] They upgraded the facilities emergency power, installed redundant alarms, posted a 24/7 alarm monitor, and established a fire warden program, among other upgrades.[8] Despite these improvements, the 9/11 attacks clearly reveal that much work still needed to be done regarding first responder C3 capabilities.

Since 9/11, a number of statutes, strategies and directives have been enacted to provide specific legal authority for both cross-sector and sector-specific protection and guidance. These directives have been crafted to the NSS mandate to protect the homeland of the United States. The *2002 Homeland Security Act* established a cabinet-level department headed by a cabinet Secretary of Homeland Security with the mandate and legal authority to protect the American people from terrorist threats.[9] Congress has assigned the Department of Homeland Security (DHS) the primary mission of minimizing damage and assisting in the recovery from terrorist attacks.[10] This Act further directs DHS to develop a comprehensive national plan for securing the nation's critical infrastructure and key resources. One of these cited key resources is an emergency preparedness *communication* system.

Similarly, the *Robert T. Stafford Disaster Relief and Emergency Assistance Act* provides detailed authority for response to emergencies and major disasters.[11] The federal government is granted specific authority to provide assistance to state and local entities for disaster preparation and for emergency assistance to mitigate the damage of major disasters.[12] This assistance includes, among other things, resources and such services as emergency *communications*, emergency transport, and assistance in fighting fires.

Additionally, there are two Homeland Security Presidential Directives (HSPD) which address preparedness and response. HSPD 5, *Management of Domestic Incidents*, and HSPD 8, *National Preparedness*,

establish a national approach to managing domestic incidents that ensures effective coordination among all levels of government and among government and non-government and private agencies.[13] They empower the Secretary of Homeland Security to coordinate federal resources used for prevention, preparedness, response, and recovery from terrorist attacks, major disasters, or other large-scale emergencies.[14] They further mandate development of emergency preparedness training, planning, equipment, and exercises.[15] Finally, they direct all involved parties to adhere to the same standards.

These legislative acts and presidential directives have led to the implementation of various DHS planning documents. Several seminal documents pertain to response planning and execution: the *National Infrastructure Protection Plan* (NIPP), the *National Incident Management System* (NIMS), the *National Response Framework* (NRF), the *National Emergency Communications Plan* (NECP), and the *Emergency Services Sector Specific Plan* (SSP).

The NIPP provides a unified structure for integration and unity of effort at the national level. Its primary goal is to, "build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating terrorists' attempts to destroy or incapacitate our nation's critical infrastructure and key resources (CIKR)."[16] Additionally, it aims to "strengthen national preparedness, timely responses, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency."[17] The DHS has designated emergency services as a key resource sector.

The NIMS is the national template designed to enable federal, state, local, tribal, private, and non-government agencies to work together efficiently to prevent, protect, respond, and recover from incidents.[18] It provides the doctrine for command, control, and incident management across all agencies, levels, and disciplines. It also provides the concepts, principles, terminology, and processes for collaborative incident management – *common operating picture*, *interoperable communications*, and information management.[19] The NRF builds on the NIMS and provides the "structure for implementing a nationwide response policy and for operational coordination of responses to all types of domestic incidents."[20]

The NECP is designed to "ensure operability, interoperability, and continuity of communications."[21] Its goal is to establish nationwide *interoperable* emergency communications.[22] Additionally, this plan seeks to develop a COP that will enhance responders' situational awareness and provide timely and consistent information during a crisis.[23] Lastly, the Emergency Services SSP sets prioritized goals and objectives which support the overarching goal of the NIPP. It is designed to protect, among other things, personnel from both operational risk and risk from attackers, and to ensure timely, coordinated all-hazards emergency response.[24] This sector is comprised of law enforcement, fire and emergency services, emergency medical assistance, emergency management, and public works and constitutes the nation's first line of defense against a concerted terrorist attack.

**Analysis**

These policies, directives, and plans have substantially improved the nation's emergency response capabilities. Specifically, they provide the basic framework for agencies at all levels of government, for non-government assets, and for the private sector across all disciplines to share a common foundation for coordinating, planning, and responding to national emergencies. Collectively, they now share a common terminology for first responder communications; they clearly articulate goals; and they pursue specific objectives to meet those goals – interoperable communications, COP, etc. They also now have an incident command structure and know who is in charge based on the nature of the situation.

However, these documents, do not yet assure optimal and integrated responses. Federal policies and guidance are just that, guidance. As a result of our federalist system, the federal government lacks the authority to direct necessary measures to ensure effective response to major incidents. Response is an inherent function and responsibility of each state; effective responses require close coordination with private and non-profit entities to provide goods, services, and research and development.[25] Improvements come only when local and state governments, in collaboration with the private sector, voluntarily comply with the federal guidance.

DHS has taken further measures to improve communication capabilities. For example, the National Communications System provides a number of communication services for qualifying federal, state, local, and non-profit agencies that provide emergency services. The Government Emergency Telecommunications Service (GETS) provides emergency priority and access to segments of the public switch wireline network, using a special dialing plan and unique personal identification number.[26] GETS is designed to make maximum use of available communication lines. Similarly, Wireless Priority Service (WPS) provides access and priority to cellular networks over non-WPS subscribers.[27] To improve the probability of successfully completing a call during an emergency, DHS recommends using WPS in conjunction with GETS. But this is not an ideal situation: Telecommunication providers are not required to offer this service and do not guarantee call completion.[28] Additionally, access to the service requires WPS-enabled cell phones, and users are charged a fee on a pay-as-you-go basis.[29]

Statewide Communications Interoperability Plans (SCIP) represent significant progress. With the assistance of the DHS Office of Emergency Communications, all states and territories have drafted department-approved plans.[30] These plans specify how states will communicate within the state across agencies, disciplines, and jurisdictions, as well as with other states and federal agencies. They provide a mechanism and process for communicating with disparate agencies, but not the means. So they do not assure genuine interoperability. Lastly, federal grant programs have helped improve communications capabilities across the emergency services sector. The Federal Emergency Management Agency (FEMA) administers the interoperable emergency communications grant program. This program provides states, territories, and local governments with funds for governance, planning, training, and exercises to achieve interoperable communications.[31] In fiscal year 2009 and again in 2010, the federal government distributed $48M each year in support of SCIP.[32]

Despite the great strides made in policy and funding to improve communications and increase situational awareness among and across state and federal jurisdictions, more needs to be done. America still

does not have, but needs, a nationwide interoperable communications system, an effective way to track responding personnel and assets, and a coherent mechanism to capture all relevant data into a shared COP.

### *Interoperable Communications*

First and foremost, an effective C3 system begins with interoperable communications. This is the backbone for the other elements, enabling a response force tracking capability and a COP. The NIMS defines interoperable communications as the ability of emergency response personnel to communicate within and across agencies and jurisdictions by voice, data, and video.[33] Today, in most locales, communications rely on a number of archaic methods; swapping radios, radio/phone patches, use of liaisons, information relayed by dispatchers/control centers, shared channels, or trunked systems.[34] All of these methods fall short of providing effective interoperable communications.

As previously stated, many cornerstone homeland security documents, and real world events have revealed the need and requirement for interoperable communications. For example, the NECP purports that emergency response agencies require interoperable and seamless communications to manage response, to control response partners, and to maintain a common operating picture.[35] But the lack of interoperable wireless communication among first responders diminishes this capability. The 9/11 Commission recommended dedicating a portion of radio spectrum to create a coast-to-coast, interoperable digital emergency communications network.[36] Accordingly, *Homeland Security Act 2002* and *Homeland Security Appropriation Act 2007* legislate the creation of a nationwide emergency communications capability.

This legislation is being implemented by means of the NECP, the NIMS, and various emergency management working groups. However, Congress has yet to resolve issues of frequency spectrum allocation and licensing. Nor has it appropriated sufficient funds to build a Public Safety Broadband Network (PSBN). Finally, Congress has not addressed governance concerns of both the public safety and commercial sectors, nor have they granted PSBN the D Block radio frequency spectrum.[37] This frequency band is contiguous to existing PSBN spectrum and is needed to meet emergency responders' day-to-

day communications needs.[38] The *2005 Deficit Reduction Act* stipulates that this frequency band will be auctioned to the highest bidder.[39] Congress must amend this Act to assure that PSBN has an adequate radio frequency spectrum. Likewise, Congress must allocate sufficient funds for construction of this system, which is estimated in the tens of billions of dollars.[40]

Currently three primary options are being discussed. The first option is to continue to advocate for local stakeholders to find their own solutions within the construct established by the DHS. This option assumes that stakeholders have the greatest understanding of their particular issues and concerns, so they are in the best position to decide what is needed. Under this option, the system will develop incrementally along a continuum established by an agency designated in the NECP.[41]

While this approach offers benefits to the local community, history reveals two significant drawbacks in this bottom-up approach. First, these systems are generally proprietary, tailored to the local market; therefore, they are not interoperable across jurisdictions or regions. Second, it is costly to purchase, install, operate and maintain them. In the past nine years, the federal government has expended $13B on emergency communications, and the estimated cost to upgrade existing equipment is another $18B.[42] But these upgrades do not guarantee interoperability. This option exposes both the general public and first responders to increased and unnecessary risk.

The second option is to build a dedicated, nationwide, interoperable wireless network for public safety. To fully reach this goal, 10MHz of spectrum from the D Block must be reallocated to the PSBN to assure public safety.[43] This will provide first responders with twice the current spectrum and twice the capability for current and evolving communications requirements; data, voice, and video.[44] Additionally, the system will provide 4G technology, which is 10 times faster than the current high-speed wireless services. It will also provide wider service to 98% of the population.[45] Lastly, it provides priority access to a self-governed dedicated system to meet both day-to-day operational needs and to respond to large-scale contingencies. There are, however, two major concerns with this proposal: First, Congress must amend current legislation that requires auctioning off the D Block frequency

spectrum. Second, the Federal Communications Commission (FCC) estimates this network's initial cost to be approximately $15.7B.[46] Finally, to build and operate this system over the next 10 years will cost approximately $34-47B.[47]

The third option is to develop a public-private partnership between public safety agencies and wireless carriers; these partners will share joint responsibility for decision-making. This partnership will build a nationwide network that meets the express needs of first responders for robust interoperable communications. Theoretically, this shared infrastructure and capability will provide economies of scale, new sources of funding, continuous technological improvements, and access to additional spectrum during large scale incidents.[48] There are significant concerns about this option. Public safety proponents fear they will have insufficient influence over access and operations of the system. Specifically, they would have to compete with the private sector during incidents for more bandwidth (an issue during 9/11 and Hurricane Katrina). They fear that commercial carriers will not be willing to push paying customers off the network at critical times. Additionally, during major crises like 9/11, public networks were overwhelmed and rendered virtually ineffective. Furthermore, the proposed network would provide only video and data capabilities. It does not address the requirement for voice, which is the first responders' most needed capability. Lastly, the FCC estimates this system will cost approximately $12-16B, while the public estimate is $18-40B.[49]

First responders must be able to effectively communicate across disciplines and jurisdictional lines and to swiftly respond to and resolve issues. Without this capability, the public's safety and the lives of first responders and of all U.S. citizens remain at risk. No matter which of the above options is chosen, our national leaders must commit to providing an effective system of interoperable communications for our responders to national emergencies.

### *Response Force Tracking*

The second area requiring attention is a means to track personnel and resources. The ability to effectively communicate during a crisis is crucial; however, the ability to track the location of first responders is

equally important. The NIMS identifies accountability of resources as essential during incident response operations.[50]

Furthermore it cites the need for unity of command, for personnel accountability, and tracking resources. The lack of effective tracking of equipment and especially personnel, during 9/11 impaired C3 response capabilities. During the initial 9/11 response, the fire chief lost radio communications with fire fighters inside each tower.[51]

This greatly inhibited his ability to command the situation and his ability to effectively allocate additional resources. If tracking devices had been available, the fire chief would have known what floor his personnel were on. And he would have had a fairly good idea how the evacuation was proceeding. Tragically, many fire fighters died on 9/11 because they never got the word, via radio or mouth, to evacuate the building. Armed with tracking technology, runners could have pinpointed first responders' locations and verbally ordered units to evacuate. Unfortunately, the methods for tracking personnel have not changed much since 9/11. Agencies still rely on listening to land mobile radio communication, radio status checks, and plotting boards.

But effective and proven tracking technology now exists. Over the past 10 years, the U.S. military has conducted extensive research, development, and tests on tracking devices, and has fielded "Blue Force Tracking" (BFT). This system uses a global positioning system (GPS) beaconing instrument that provides point-to-point, peer-to-peer and/or point-to-command center tracking.[52] The system provides position location, an identification function, a transceiver, a communications network, and a user interface.[53] It provides near real-time information that transmits the exact location of personnel, vehicles, and assets.[54] This information is displayed on a portable or fixed monitor that depicts friendly forces on an easy-to-read digitized geospatial map. The number of assets being tracked directly determines how much bandwidth is required. This is why emergency management needs a dedicated nationwide wireless network that includes the additional 10 MHz of spectrum.

BFT has been used extensively in Iraq and Afghanistan; it has proven effective in both rural and urban terrain. When BFT is properly

integrated with other data feeds, it provides enhanced situational awareness and a COP that optimizes command and control (C2). This system can be adapted for civilian use to track critical equipment, key assets, and responding forces.

This technology has proliferated to the private sector. Wireless providers, Verizon, AT&T, and Sprint, offer applications that can track the precise location of individual cell phones. Additionally, New York City emergency management agencies are acutely aware of the benefits of this technology and have begun outfitting all their fire trucks and ambulances with GPS tracking devices.[55] It enables them to instantly dispatch the nearest unit to an incident scene: reducing response time means more lives saved.

To track their personnel, the New York City Fire Department (FDNY) is in the process of fielding the Electronic Fireground Accountability System (EFAS). This system, like BFT, uses GPS technology and geographic information system mapping to graphically display firefighters in flaming structures; it can track personnel in high-rise buildings or in the subways.[56] Handheld radios carried by FDNY personnel transmit GPS locations on both mobile and fixed platforms; this system tracks personnel individually by fire company and position.[57] Moreover, it transmits distress signals and conducts electronic roll calls. Armed with this information, Incident Commanders (IC) can better deploy, employ, command, and control responding forces. Then they can effectively send search teams to locate dead, missing, or injured comrades.

EFAS has already been tested in four units across the boroughs with positive results.[58] Consequently, FDNY leaders are expanding the program to other units citywide. This system will provide better situational awareness for the ICs, improve their ability to effectively C2 responding forces, and quickly deliver aid to distressed first responders.

### *Common Operating Picture*

The third C3 element, COP, builds on or is the culmination of the other two. It can be fully realized only after a dedicated nationwide communication system has been established, along with an effective means to track responding personnel, vehicles, equipment, and assets.

As with interoperable communications, there are many definitions of COP. For purposes of this paper, the following NIMS definition will be used: "COP provides an overview of an incident created by collating and gathering information, such as traffic, weather, actual damage, and resource availability, of any type (voice, data, etc.) from agencies and organizations in order to support decision-making."[59]

The need for a COP for the first responders was born out of 9/11. All national-level policies identify COP, at a minimum, as a desired end-state to be achieved through procedures, agreements, and eventual integration of systems. For example, the NIPP advocates a networked approach for information-sharing, and the NRF contends that in order to have an effective, unified effort, response agencies (governmental and non-governmental organizations) must gain and maintain situational awareness by continually monitoring relevant information.[60] Likewise, the Emergency Services SSP cites COP as the primary national strategic goal for the national critical infrastructure sector.[61] Fundamentally, the COP provides the right information, at the right time, in a user-friendly format to support effective decision-making.

Currently, responders rely on a number of disjointed methods to get a COP. At the national level a 24/7 National Operation Center (NOC) acts as a hub for fusing law enforcement, intelligence, emergency response, and private sector reporting.[62] Its primary function is to maintain situational awareness and provide operational coordination across the federal government for incident management.[63] This is largely accomplished through standardized reporting procedures, delivered telephonically or electronically, set forth in the previously mentioned national policy documents. Additionally, the NOC seeks to sustain situational awareness by means of the Homeland Security Information Network, a web-based communications platform that enables federal, state, local, and partner agencies to obtain, analyze, and share information.[64] The NOC thereby facilitates collaboration among members and assists with providing real-time connectivity between states and the NOC.

At the state and local levels, COP is generally achieved through emergency operation centers, which may or may not be operated 24/7. A COP can also be derived from coordinating information from first-

responder control centers.[65] These centers serve as the nerve system for multiagency coordination. During an incident, these centers provide inter- and intra-agency coordination, communication, resource allocation, and information collection, analysis, and dissemination.

While common language and command structure protocols have been established via NIMS and the Incident Command System, there is no single standard COP in use across all levels of emergency response, jurisdiction, and disciplines.

There are however, a number of government and commercial programs available and in use throughout the country. However, these systems are usually not networked. Once again, because of the very nature and complexity of war, the military has long recognized the benefits of having an integrated C2 suite. Accordingly, it has developed and implemented the Global Command and Control System (GCCS). This system-of-systems provides a foundation for dominant battlespace awareness by providing an integrated, near real-time picture that facilitates conduct of combined, ground, air, and naval operations.[66] GCCS fuses selected C2 capabilities (satellite imagery, BFT, radar, camera feeds, etc.) into a comprehensive, interoperable system through exchange of operational and planning information.[67] This architecture shows promise for wider use, both within the military and the civilian sector, but its current utility is limited by the fact that the system only operates at the "secret" classification level. Its users must access the Secure Internet Protocol Router Network, which many emergency management agencies do not have access to.

In the public sector, New York City (NYC) developed a systematic approach to incident management called CIMS (Citywide Incident Management System). It is very similar to and complies with the NIMS construct; it establishes roles and responsibilities, directs how incidents will be managed, and offers a means for integrating regional, state, and federal agencies into a NYC response.[68] Under the CIMS umbrella are a variety of systems designed to improve situational awareness. Overall they provide a COP. These systems rely on geographic information to link maps with databases; they enable users to visualize, manipulate, analyze, and display spatial data.[69] One of these incident management

systems is E-Team, which enables responders to collaborate and manage efforts across multiple organizations sharing a single identical display.[70]

Another CIMS tool, CALMS (Citywide Asset and Logistics Management System), integrates multiple resource management systems. This web-based system captures information on resources commonly used during disaster response (personnel, vehicles, equipment, and supplies) from local, state, federal, and private partners.[71] It graphically depicts the location of evacuation centers, special use equipment, and facility blueprints.[72] Also it provides rosters of skilled craftsmen. FDNY is currently testing and fielding a number of systems to improve situational awareness and incident management, most notably EFAS.

**Recommendation**

Many changes have been made in the past 10 years to improve interoperable communications and to create a COP for our nation's first responders. However, more work is needed to truly meet the spirit and intent of published guidance and, more importantly, to meet the needs of our nation. To fully achieve viable interoperable communications, tracking, and a meaningful COP, the nation needs enabling legislation, improved compliance with established policies, clearly articulated technical standards, and a coherent funding strategy. As a critical first step, the federal government must commit to fund and build a dedicated, nationwide, interoperable wireless network. The other options are too risky and too limited. Local stakeholders can only provide ad hoc communications and public-private partnerships leave many questions unanswered regarding dedicated bandwidth and overall governance of the system.

A dedicated public safety system will assure effective emergency communications. This system is affordable over time. It will benefit from economy-of- scale and provide better service through access to and competition from the commercial sector for cutting-edge technology. Benefitting from the upgrade of 4G technologies, the public safety community will benefit from a quantum leap in access to state-of-the-art capabilities, which will enable them to better protect themselves, and the homeland.[73]

To build this system, Congress must amend legislation and dedicate the D Block to the existing public safety frequency spectrum. This new legislation will provide the domestic security community with twice the current bandwidth and much greater capacity for current and future needs.[74] This additional bandwidth is required, as proven during a recent test in San Francisco, to take full advantage of video, data, and eventually voice capabilities. Based on the results of this public safety broad-band network test, at least 20 MHz of continuous spectrum is needed to fulfill emergency responder's day-to-day voice, data, and video needs.[75]

To pay for this upgrade, the federal government should use proceeds from the upcoming auction of frequency spectrum already identified by the FCC. The initial sales are projected to generate approximately $24B in revenue, which more than covers the estimated $15.7B cost to implement this network.[76]

Once there is a dedicated nationwide network, then work can begin on effectively integrating the disparate systems. The DHS needs to establish a bonafide communications roadmap. The DHS Science and Technology (S&T) Division is a logical choice to lead this effort. S&T must develop a consolidated list of approved technologies (radios, software, and COP systems) predicated on robust research and development followed by extensive testing and evaluation. This menu of items should be sufficiently varied to meet the diverse needs of emergency management agencies both large and small, both urban and rural, all disciplines, and at all organizational levels. These systems should operate intuitively, perform to standards, be dependable, and be fully interoperable. Additionally, well-defined requirements must be established for data, imagery, voice, video, back-up capabilities, display functions/icons, etc.

Approved systems must be able to fuse data from the myriad of sources and systems. An effective COP should depict the geographical locations of responding elements, available assets, specialized equipment and vehicles, key facilities, critical infrastructure, and specialized teams. The military's GCCS or NYC's CIMS are examples of systems that integrate alarms, videos, CALMs, and EFAS. Whenever it is practical, these new systems should accommodate legacy equipment.[77] The goal

is to create a suite of systems that are compatible in a plug-and-play fashion, regardless of their hardware and/or software manufacturers.

While our federalist system cannot mandate compliance with existing and emerging standards, state and local agencies can be encouraged to comply with shared standards through funding. For example, when federal funds pay for radios, they should be purchased off the S&T approved list and be loaded with the appropriate national emergency frequency.[78] Despite the fact that emergency response efforts and funding are state and local responsibilities, DHS must work with all levels of governmental and non-governmental agencies to develop a comprehensive funding strategy. The nation needs an objective, standardized framework to identify and assess nationwide emergency management communications capabilities in order to prioritize where limited funds are most needed.[79] Emergency management leaders should identify funding sources (federal, state, local, and private) and develop a prioritized funding strategy predicated on compliance with established guidance (NECP), risk (number of people impacted), and need (current capability and financial). For example, a small rural town that needs 3 or 4G technology and lacks the financial means to acquire this capability should be able to consult DHS to determine what funding sources are available and whether they can pay for the needed technology. In addition to the established grant programs – Homeland Security Grant Program, Public Safety Interoperable Grant Program, etc. – the federal government should provide incentives for commercial carriers to share the costs of building a nationwide network. For example, the frequency bandwidth currently slated for sale could be offered at a reduced cost with the caveat that the private carrier expands 3 or 4G capability to rural areas and allows the public sector to use existing infrastructure, i.e., communication towers.[80]

Finally, there is no reason to reinvent the wheel. Available technology can facilitate interoperable communications, can track assets, and can produce shared COP. Through the various working groups like Regional Emergency Communications Coordination Working Group, DHS can do a better job of improving communications among the various agencies within the emergency management sector. DHS should capture best practices from the field, evaluate the process,

develop procedures, and identify proven technology and make all of these available to the emergency response community.[81] For example, DHS could test and evaluate NYC's solutions, determine which pieces have utility across the sector, and add the specific hardware and/or software to the approved technology list for other agencies to use.

**Conclusion**

To meet the national security objective of protecting the homeland and people, first responders need new and better tools. Watershed events like 9/11 have exposed vulnerabilities in first responders' communication capabilities. Effective and efficient emergency response C3 requires such capabilities in order to mitigate the damages of catastrophic terrorist attacks and to respond to major natural disasters or other emergencies.

To improve their capability to protect our great nation, first and foremost responders need a dedicated, interoperable, nationwide wireless network. Such a network will facilitate integration, synchronization, and unity of effort from all levels of government; non-government agencies; and all disciplines. After this network is created, further enhancements can be realized to track and provide a "true" COP that is shared, viewed, and used by all echelons of emergency response leadership. This capability will provide incident command teams with the ability to pinpoint equipment, locate key facilities and infrastructure, and effectively track emergency response personnel. All of this will expedite, improve, and synchronize critical response and recovery efforts. Most of all, it will save lives and assure the best use of critical national resources.

Despite improvements made in first responder communications, there is still a great deal of work left to be done. For example, Congress needs to act quickly to dedicate spectrum to public safety and fund a nationwide wireless network. The time to act is now, before the next major catastrophic event, natural or man-made, takes more innocent lives. Our nation, our people, and our emergency responders deserve and demand protection. Our elected leadership must act decisively to ensure homeland security through better policy and appropriate funding.


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

# The Role of Military Forces in Disaster Response: Remove The Impediments

**Lieutenant Colonel Michael Bentley**
United States Army

*A lot of ink was shed cataloguing lessons from Katrina, 9-11, and other disasters in reports by the House, Senate, White House, countless think tanks, and Commissions, including the Commission on the National Guard and Reserves. So it is fair to ask here today, did we learn the lessons of 9-11 and those other tragedies: Are we ready? Or maybe more precisely, are we as ready as we need to be for the next "big one"…? Either you are ready, or you are not. Unfortunately, the answer is – we are not ready. The yardstick here is not how far we have come and the progress we have made. It is how far we have to go.*[1]

—Major General Arnold L. Punaro,
U.S. Marine Corps (Ret.)

In March 2011 an earthquake registering a 9.0 on the Richter scale struck off the coast of Japan. It was one of the four most powerful earthquakes in the world since earthquake data has been recorded.[2] This earthquake and the resultant massive tsunamis led to enormous loss of life and property in the impacted zones. The Japanese government's response was tremendously complicated as this natural disaster quickly overwhelmed first responders and developed into a nuclear and radiological event that required follow-on responders to cope with the meltdown of three of Japan's nuclear reactors. Although this catastrophe occurred thousands of miles from the shores of the United States, our nation is not immune to this type of event. An earthquake with a magnitude 7.0 or higher on the Richter scale along the New Madrid seismic zone in the midwest United States would be catastrophic. It would require a response far greater than that mounted for Hurricane Katrina.

In his testimony before the Senate Committee on Homeland Security, William Carwile III, Associate Administrator for Response and Recovery for the Federal Emergency Management Agency (FEMA), described the potential impacts of an earthquake along the New Madrid fault line:

> *A rough estimate of the damage would include…nearly 715,000 buildings…damaged in the eight-state study region. Damage to critical infrastructure…could be substantial in the 140 impacted counties, including 3,500 damaged bridges…2.6 million households could be without power. Nearly 86,000 injuries and fatalities could result and nearly 130 hospitals may be damaged. Three days after the earthquake, 7.2 million people could be displaced, with 2 million seeking temporary shelter.*[3]

This fault line is among the most active in the United States; it is the site of more than 200 measured events per year.[4] Although many of these events can be felt across the seismic zone, most are nuisances that require no responses. However, a future major earthquake along this zone would be catastrophic, with the potential for flooding, structural damage, and radiological complications, like those that recently struck Japan. There are 15 nuclear power plants located in the New Madrid Seismic Zone,[5] and a severe earthquake could severely damage any of these plants and release radiationinto the surrounding area, as in Japan. Since the 9/11 terrorist events and the Hurricane Katrina disaster, this nation's disaster response capabilities have improved. However, some restrictions and command issues still impede Defense Support to Civil Authorities (DSCA). It is not a matter of when the next disaster will strike; it is only a matter of how prepared are we are to respond to it.

The circumstances of how, when, and where a disaster strikes and the quality of the response do not allow for lengthy discussions and legal reviews during the incident. Disasters strike anytime, anywhere. They take "many forms – a hurricane, an earthquake, a tornado, a flood, a fire or a hazardous spill, an act of nature or an act of terrorism. [They build] over days or weeks, or [hit] suddenly, without warning."[6] If history is a good predictor of the future, then the United States will be struck by many man-made or natural disasters that will require federal assistance. "The American people fully expect that all military

forces that are available and can help respond to a disaster will do so without unnecessary delays."[7] Even with the addition of recent changes in policy and law, further changes are needed to ensure that our nation receives the best possible support during the next disaster.

## Background

On 29 August 2005 Hurricane Katrina made landfall for the second time as a Category 3 storm along the coast of Louisiana. The aftermath and the response to this natural disaster made it the costliest natural disaster to strike the United States. Its 1,349[8] deaths make it the deadliest hurricane in the United States since 1928.[9] Much has been written about the response by the state and federal government to this catastrophic event. Much of the literature lauds the heroism at the tactical level of many of the first responders from the National Guard and the federal forces responding to the disaster. In his testimony to Congress, Assistant Secretary of Defense for Homeland Defense, Paul McHale praised, "the ability of military forces – active duty, Reserves, and the National Guard." He cited their capabilities to "respond quickly and effectively to an event of this magnitude [as] a testament to their readiness, agility and professionalism."[10] Despite these heroics, many critics have lamented about the inept response at the strategic level by both the state of Louisiana, where 90% of the fatalities from the storm occurred, and the federal government.[11] According to the Katrina Lessons Learned report and in spite of the tactical and operational heroics, "the response to Hurricane Katrina fell far short of the seamless, coordinated effort that had been envisioned by President Bush when he ordered the creation of the National Response Plan."[12] This strategic failure was evident in the needless squabbling between the leadership of the state of Louisiana and the executive branch over who would be in charge of the relief effort. Further, because of antiquated legislation, federal forces could not effectively respond until law and order had been restored. Former New Orleans's emergency operations chief, Terry Ebbert, sums it up this way: "We can send massive amounts of aid to tsunami victims, but we can't bail out the city of New Orleans."[13] A late and haphazard response to a domestic disaster from a country that provides timely financial aid, manpower, and equipment to disaster response around the world is incomprehensible.

The thoroughly documented state and federal response to Hurricane Katrina before, during, and after its landfall was appalling. A plethora of information in libraries, journals, books and newspaper archives analyze this failure. This paper does not purport to be another analysis of the Department of Defense (DoD) response to Hurricane Katrina. Rather, it argues for what needs to be accomplished to be better prepared for the next disaster.

As Major General (Ret.) Punaro concluded in his response to members of the House and Senate Armed Services Committee:

> *When it comes to disaster response, the American people don't care whether it is an active duty, Guard, or reserve helicopter who rescues them from a rooftop. They believe that protecting American lives and property here at home is as important—or more important—than putting a bayonet in the heart of a terrorist in the Khyber Pass, as important as that is.*[14]

A thorough discussion of DSCA must begin with an understanding of how military forces are formed within the DoD and the way they currently respond to domestic disasters. The following discussion cites relevant Constitutional and legal issues to clarify problems in the uses of the military to respond to domestic disasters. The way military forces responded to Hurricane Katrina in 2005, absent further changes, is the way they will respond to future disasters inside of the United States. This way is based on the Constitution and federal law.

As they crafted the Constitution, the founding fathers took extreme care not to place all governmental power at the federal level. Instead they developed a federalist system whereby "states share powers with a central national government."[15]

Additionally, they had an aversion to the large standing British Army that occupied the original colonies and answered only to the King of England. They saw this hegemonic relationship as a threat to civil liberties, and so were wary of a militarized executive authority as they developed the Constitution.[16] Accordingly, they granted the states the authority to form militias – the precursor to the National Guard – to defend the states, and to provide, when needed a federal military force. Although the founding fathers despised a standing army, they

also realized that a professional full-time Army would be required to protect the nation and advance national interests because the militias would be ill prepared for this. Therefore the Constitution authorized the Congress to form this Army. But in order to avoid maintaining a long-term standing army, they stipulated that, "no appropriations of money to that use shall be for longer term than two years."[17] In this way, they attempted to avoid forming a permanent federal military force. The Constitution states:

> *The Congress shall have power… To raise and support Armies,.. To provide and maintain a navy… To provide for calling forth the Militia to execute the Laws of the Union, suppress insurrections and repel Invasion; To provide for organizing, arming, and disciplining, the Militia, and for governing such part of them as my be employed in the Service of the United States.*[18]

In the matter of command and control, the Constitution declares:

> *The President shall be Commander in chief of the Army and navy of the United States, and of the militia of the several states, when called into the actual service of the United States.*[19]

The Constitution clearly indicates who can form and command these different military forces. The states have the right to form and maintain militias under the command of the governor; the Congress has the authority to form land and naval forces that are commanded by the President.

**Military Forces**

There are two primary types of military forces that can be called on to support civil relief operations inside the United States – state National Guard forces, and federal military forces.

The National Response Framework and DoD policy recognize that the primary responsibility for protecting life and property and maintaining law and order in civilian communities is vested in state and local governments.[20] DoD policy also recognizes the responsibility of the federal government, including DoD, to assist the states in maintaining order during a crisis. In certain instances, DoD assets may be available

**Federal military forces:** Regular Army, Navy, Marine and Air Force personnel and units; mobilized Army, Navy, Air Force and Marine Reserve forces and personnel, and any National Guard forces and personnel mobilized for federal service in accordance with Title 10 USC. The President of the United States is their Commander in Chief.

**State National Guard forces:** Air and Army National Guard personnel and units that are serving under state control, in accordance with Title 32 USC. The governor of their each respective state has overall command responsibility for the National Guard in that state and is their Commander in Chief. State National Guard forces do not include state defense forces organized outside of the National Guard.

**Figure 1: Military Force Structure**[21]

to support civil authorities for routine and catastrophic incidents. Under our current system, the first military asset that is usually called on to provide this support is the National Guard. National Guard forces provide their governors with a crucial first military response to disasters. National Guard units located in every state across the country may conduct support in one of three ways:

- State command or state active duty (SAD) status under control of the governor as the commander-in-chief: Forces mobilized in this status receive mission orders and direction from the governor. They are paid by the state.
- Title 32 status under the control of the governor: Much like in SAD status, troops mobilized under Title 32 receive mission orders and direction from the governor. But the federal government pays them. States prefer using the Guard under Title 32 because the federal government pays the bill and the governor retains control. National Guard forces responding to the disaster during Hurricane Katrina ultimately were placed under this status by the Louisiana governor with agreement from the President.
- Title 10 federal status under control of the President: National Guard forces mobilized under Title 10, or moved to Title 10 status become federalized and are now under the command and control

of the President of the United States. The federal government pays Title 10 forces.

Controlled by their governors in either SAD or Title 32 status, National Guard units may perform a wide variety of missions, to include law enforcement. State forces mobilized under the governor "normally operate as part of a state National Guard joint task force"under command and control of the governor; states adjutant generals (TAG) usually assume operational command of a task force.[22] The National Guard forces responding to Hurricane Katrina in New Orleans were primarily from the state's Air and Army units. But because of federal deployments to Iraq, many of the state's units were not available when Hurricane Katrina struck. However, under the Emergency Management Assistance Compact (EMAC), "a legal framework established in the wake of Hurricane Andrew in 1992, to flow National Guard soldiers and other first responders into the region from states across the country," Governor Blanco was able to obtain National Guard forces from across the United States to supplement her own units.[23] National Guard forces responding from another state remain under "command and control of their regular leaders, but the organizational units will come under the operational control of the state receiving assistance."[24]

Federal Forces – excluding reserve forces, which will be addressed separately – are commonly referred to as the Title 10 Regular Army and are "organized into operational forces intended for deployment and ground combat operations, and the generating force."[25] The Regular Army provides numerous advantages to civilian leaders during disaster relief operations. Already on active duty, they can immediately contribute to these operations without getting their employers' leaves of absence or without getting them on an appropriate payroll. In many cases National Guardsmen are civilian policeman, fireman and emergency management technicians (EMTs) – both the civilian first responders and the military first responders. The civilian employers of these personnel can ill afford to release them when a disaster strikes. Their dual roles, coupled with deployments of Louisiana National Guard and Reserve forces on operational missions, hampered responses to Hurricane Katrina. Similar circumstances may arise in the future. Federal forces trained and legally able to conduct law enforcement

in the future can relieve this situation. Additionally, "the ability of the Regular Army to generate large forces rapidly and sustain them for long periods in an emergency is one of the component's primary attributes for civil support."[26] However, most Regular Army forces are not located in local communities across the country. Rather they are centrally located on federal bases within the United States. If the base happens to be located in the vicinity of the disaster and all the protocols are followed for the uses of federal forces then the communities that surround the base are in luck. Mobilizing and deploying full-time federal forces to more distant locations can take precious time, even if the force is a global response force on a recall timeline. However, a different type of force, albeit a federal and therefore a Title 10 force, that is more readily available to the DoD and civilian leaders is the Reserve force.

If the National Guard is the nation's first military responder, then the Army Reserve is normally the "first Title 10 responder"[27] to support disaster relief. Army Reserve forces are similar in nature to National Guard forces in that they are located in almost every state or territory and are able to provide time-sensitive assistance in a crisis environment. However, due to their status as federal forces, activated Reserve forces fall under the command of the President, not a governor. Reserve forces, which are usually activated only temporarily, often contain key support assets that are in demand in response to disasters. By design, Reserve forces consist of a large proportion of the combat support and combat service support assets in the United States Army – such as Aviation, Medical, Engineers, and Military Police personnel.

They serve as Title 10 forces when activated, so they are subject to the same regulations and rule of law that Regular Army forces fall under. Nevertheless, the recent presidentially signed 2012 National Defense Authorization Act (NDAA) includes recommendations from the presidentially formed Council of Governors that would allow the "Secretary of Defense the authority to mobilize Title 10 Reserve forces at a governor's request to assist in the federal response to a domestic emergency for not more than 120 days."[28] Although this recent positive change will allow for a quicker response from Reserve forces that are located across the country, until all federal forces are

allowed to be placed under the command of a governor the response will continue to be inefficient. Regardless of the type of force that is available for support, several federal laws stipulate the DoD's roles and responsibilities in DSCA within the United States.

**Authority/Legislation**

The *Posse Comitatus Act* (PCA) of 1878 along with its two primary statutory exceptions, the *Robert T. Stafford Disaster Relief and Emergency Assistance Act*, and the *Insurrection Act*, constitute the three primary legal authorities that regulate the use of DoD assets to support disaster relief inside the United States. Restrictions in the PCA and its two statutory exceptions have caused problems during federal efforts to respond to Hurricane Katrina.

Federal forces and their accompanying equipment are always available to provide support to the governors of the states. However, there are legal restrictions on what these forces are allowed to do when responding. Federal forces conducting DSCA are governed primarily by the Posse Comitatus Act. Specifically, federal forces are restricted in their conduct of law enforcement operations within the United States and its territories. Although the Congress has amended the PCA on numerous occasions to permit the President under certain situations to use federal forces in this manner, the limitations imposed – either actual or perceived – on federal military forces hindered support during Hurricane Katrina. According to a Rand study commissioned by the DoD to provide findings and recommendations on the military response to Hurricane Katrina, "Civilian and military officials were also hesitant to deploy federal land forces in the deteriorating law-enforcement environment…there were concerns about deploying active-duty federal forces to the area given the constraints of Posse Comitatus."[29] As the situation in New Orleans continued to deteriorate federal leaders hesitated to deploy federal forces in a support role because of the possibility that these forces would be forced into a law enforcement role – in a possible violation to the PCA.[30]

The PCA is set forth in only a brief, short sentence. But this succinct law, which is often liberally interpreted, has had a huge impact on the domestic uses of U.S military assets. These liberal interpretations

and amendments by Congress have turned this succinct Act into an impediment to support inside the United States. The Act, as amended in 1956 declares,

> *Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a Posse Comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both.*[31]

Although not included in the original law, the DoD felt obligated to subject the Navy and the Marine Corps to PCA in subsequent directives. The PCA was initially passed into law on 18 June 1878 in response to complaints about the Army's involvement in supporting the Reconstruction governments in the southern states after the Civil War.[32] But over time it has turned into a quagmire that prevents well-intentioned individuals at all levels of government to use our military forces in the homeland. Nowhere was this more evident than the days and weeks following the landfall of Katrina along the coast of Louisiana and New Orleans. As the first responders were either overwhelmed or unable to secure the environment, lawlessness overtook New Orleans. Looting took a nefarious turn as roaming gangs pilfered cars, electronics, and clothing. [33] Snipers terrified the staff and patients of the New Orleans Charity Hospital as they attempted to evacuate New Orleans began to resemble the streets of Baghdad after the fall of Saddam Hussein. [34] "The inability of the local and state officials to stop rampant looting in and around New Orleans created a security vacuum"that went unfilled.[35] Only limited National Guard troops were initially available. Local police officers were exhausted from conducting search and recovery operations and were largely unable to maintain law and order for a variety of reasons. Federal forces could have filled this law enforcement gap, but they were not employed in this manner. The restrictions of the PCA prevented a readily available asset from being deployed to save lives within the United States. This situation has yet to be corrected.

In a country where the military has an approval rating of 76%, 65% higher than last-place Congress,[36] the citizens of our country should not be concerned about a fulltime military takeover of the law enforcement

mission or the ceding of rights that are guaranteed by the Constitution. Federal forces will be needed to support domestic law enforcement in the future. The use of federal forces in this role should be addressed now, rather than during another multi-state disaster such as a New Madrid earthquake rupture.

The *Robert T. Stafford Disaster Relief and Emergency Assistance Act* was originally enacted in 1988 and more recently amended in 2000.[37] Considered to be the "centerpiece of federal disaster policy,"[38] this Act authorizes the President to make a wide range of federal aid available to states that are hit by disasters. The Act authorizes the President to declare an incident either a major disaster or an emergency. This declaration has different implications for relief operations. This Act also establishes cost-sharing guidelines between state and federal governments.

**Emergency vs. Major Disaster:** Under the Stafford Act, the President can designate an incident either as an "emergency" or a "major disaster." Both authorize the Federal government to provide essential assistance to meet immediate threats to life and property, as well as additional disaster relief assistance. The President may, in certain circumstances, declare an "emergency" unilaterally, but may only declare a "major disaster" at the request of a Governor that certifies the State and affected local governments are overwhelmed. Under an "emergency," assistance is limited in scope and may not exceed $5 million without Presidential approval and notification to Congress. In contrast, for a major disaster, the full complement of Stafford Act programs can be authorized, including long term public infrastructure recovery assistance and consequence management.

**Figure 2: The Robert T. Stafford Act**[39]

The Stafford Act also provides statutory authority for employing military forces in disaster relief.[40] It allows the President, through the DoD, to provide military assistance to states requesting assistance. Specifically the Act allows DoD to make available "personnel, equipment, supplies, facilities, and managerial, technical and advisory services" for use after the President makes a declaration of emergency of disaster.[41] The Act does not, however, authorize the use of federal military forces that are

responding under the auspices of the act to maintain law and order and military forces are prohibited from performing law enforcement functions while federalized.[42] Legislative attorney, Jennifer Elsea emphasizes that federal military resources can be utilized under the Act under three conditions,[43] all of which occur after a disaster strikes and only following a governor's request for assistance:

- Essential Assistance (10-day authority): Upon request of the governor, the President may task the DoD to provide emergency work the President deems essential for the preservation of life and property in the aftermath of an incident. Assistance is available for up to 10 days prior to a presidential declaration of an emergency or a major disaster.
- Emergency Declaration: Unless the President determines that a disaster threatens preeminently federal interests, such as a seaport or federal military base, the governor must show that the state is unable to respond without the federal assistance. Additionally, the governor must first use all of the state's available assets, to include the National Guard, before requesting assistance.
- Major Disaster Declaration: The prerequisites for a major disaster declaration are similar to those for the emergency declaration. In his or her request for assistance, the governor must follow the same steps to show the state cannot handle the incident. Until the governor requests assistance, the president will not declare a major disaster.

The Stafford Act and the Constitution both vest power to maintain the well being of the state exactly where it should be – on the state. However, as was witnessed following Hurricane Katrina there are times when a state cannot handle the overwhelming impacts of the disaster. Then additional help is required.

The last piece of the puzzle guiding the way that DoD provides support within the United States is the *National Response Framework* (NRF) and the concept of tiered response. "The NRF is a guide to how the nation conducts all-hazards response."[44]

This capstone document provides, "operational direction for incident management to ensure timely and effective Federal support to State, tribal and local related activities."[45]

Additionally, from a federal to state level, "the framework defines the key principles, roles, and structures that organize the way we respond as a nation."[46] As part of the broader *National Strategy for Homeland Security Strategy*, the NRF focuses on the ability of the nation to "respond to and recover from incidents"[47] in a timely and effective manner. Much like the Constitution, the NRF, "places significant trust and responsibility in the capabilities of state and local governments to help protect the American people."[48] This framework assumes that in certain circumstances states will seek federal assistance in responding to disasters. Central to this doctrine is the premise of tiered response.

Tiered response is based on support that "originates at the local level and is progressively supported by additional response capability when needed."[49] Tiered response acknowledges that "state, local and tribal governments, which best understand their communities and the unique requirements of their citizens,"are better able to provide effective first-response capabilities.[50] As the situation escalates and civil first responders such as, "law enforcement, fire, public health, and emergency medical services,"[51] become overwhelmed, a graduated response from higher agencies and authorities occurs from within the state, including use of the state's National Guard. Upon exhaustion of local, state and inter-state assets, the governor may seek federal support. The most frequent type of support under this request – other than financial – is for additional personnel, either emergency or law enforcement personnel, and equipment from FEMA or DoD. Although not discussed in the NRF, but embedded in federal law as a statutory exception to the PCA, is the Insurrection Act of 1807. Not part of any published response, the Insurrection Act authorizes a legal response that can be provided by the President to address a deteriorating situation, a situation much like in post-Katrina New Orleans.

This Act grants the President the authority to use federal armed forces in a law enforcement role when state governments fail, refuse, or neglect to protect the rights of its people.[52] This federal support is usually delivered at the request of a governor. For example, consider the

support provided to Los Angeles in 1992 when President George H. W. Bush deployed federal forces to California to help quell the riots that broke out following the Rodney King trial verdict. However, a common misconception, which prevailed during the Hurricane Katrina crisis, is that the President must have a governor's request in order to take action under the Insurrection Act. That is not the case. Section 322 of this Act empowers the President to use federal troops autonomously to address a variety of civil disturbances.[53] However, the last time a President utilized the powers vested in this Act without the request of a governor was in the 1950s and 1960s when southern states were not implementing the civil right laws enacted by Congress.[54] President Bush and Governor Blanco both considered using the Insurrection Act to authorize using federal troops to restore law and order in New Orleans. Perhaps they declined to do so for political reasons. One occasion, on 2 September 2005, illustrates their situation.

Several times after the hurricane made landfall, while New Orleans was becoming a war zone, the President, instead of using the Act to employ federal troops in a law enforcement capacity, continued to "press Governor Blanco to request a federal takeover of the relief effort so that federal troops could be deployed to restore law and order."[55] President Bush and his cabinet were concerned that such a unilateral action would have been viewed as federal bullying of a southern Democratic governor.[56] So they refused to use the Insurrection Act without Governor Blanco's request. Moreover, the administration was worried about the political message that would have been sent by "a president ousting a southern Governor of another party from command of her National Guard."[57] In the meantime the citizens of New Orleans continued to suffer needlessly.

Governor Blanco was unwilling to request assistance under the Insurrection Act for fear of having her National Guard federalized.[58] She did not want to lose control of the support effort, even as mayhem was taking over New Orleans. Needless political wrangling and numerous attempts to skirt the PCA persisted after Hurricane Katrina made landfall. Sadly, this politicized indecision undermined what first and second responders were able to do at all levels. Even so, many of the systems and procedures in place today have evolved from the dismal

performance at the state and federal level during the Katrina response. However, these political challenges have yet to be appropriately addressed. They will inevitably resurface in future responses.

There are primarily two opposing views that are argued with regard to the PCA and the use of the military in civil support. First, repeal the law – and stand back from the political repercussions. Or keep the law as is – even though it has proven to be troublesome and in recent times an actual impediment to proper civil support. In reality, this law has outlived its usefulness, despite recent amendments. As Michael Spak, a former Army Judge Advocate General (JAG) Colonel, concludes: "The exceptions made in the name of national security in recent decades have left Posse Comitatus a hollow shell of its original self."[59] Absent a full repeal of the Act – which would not be agreeable to everyone, there is a third option. The Act should be further amended to authorize all military forces to conduct law enforcement without relying on the authority of another Act – The Insurrection Act. The amendment should allow the president to deploy federal forces to places where local first responders have been unable or overwhelmed until such time as the first responders are able to restore law and order. At that point the federal forces would be removed from the law enforcement situation and the sanctity of federalism would be returned. In this amendment, Congress could require the President to provide presidential updates to the legislative branch on the status of forces providing support. Congress could also place a time restriction, such as a 120-day maximum, on federal forces providing law enforcement. If the time limit is reached, the President must either remove the federal military forces from that location or request an extension from Congress.

The tiered response framework resides on the premise that local or state officials must ask for assistance from either another state or the federal government once the state has exceeded their ability to respond to a crisis. The challenge, as witnessed during Hurricane Katrina and what would most likely be seen in the New Madrid scenario, is what happens when first – and even second – level responders are overcome or unavailable and basic services such as emergency care and security are not being provided. During the flooding that followed from Hurricane Katrina, "many state and local public safety agencies suffered extensive

damage" and were immediately unable to perform.[60] For example, the fire departments in Grand Isle and Slidell had to close due to building and vehicle damage.[61] Some 147 New Orleans police officers abandoned their positions and the Emergency Operations Center in Orleans Parish was forced to close due to flooding.[62] Furthermore, the Infantry Brigade from Louisiana, a brigade that contained many first responders for the state, was returning from a deployment to Iraq as Katrina made landfall in New Orleans. It was largely unavailable to provide support.

Hurricane Katrina exposed a serious flaw in national disaster response plans. These plans fail to recognize that local police, fire and medical personnel might be incapacitated and unable to provide support.[63] These challenges are rarely discussed or stressed in drills and command post exercises between state and federal agencies. Yet they remain as relevant today as they were in 2005. Hurricane Katrina provides only a prelude to what happens when first and second responders are overwhelmed and unable to provide a safe and secure environment for rescue workers. Without an amendment to the PCA, when federal forces once again are deployed to support a response, they will continue to be hindered in what they can provide. The same questions and issues that arose in September 2005 have yet to be addressed.

Most disasters that strike the United States will be handled at the local and state level. They will not require the use of federal forces, either reserve or active duty. However, when the governor of a state requests additional military forces through the President, National Guard and federal forces could operate together. The 2012 National Defense Authorization Act (NDAA) raises the possibility that reserve forces will be among the first federal forces to provide assistance after a disaster. It is also inevitable that federal forces and National Guard forces will operate together in the United States to provide DSCA. So command and control of military forces within the United States should not be a contentious issue, either culturally or politically. These two types of forces have been operating successfully together in combat zones around the world for the past ten years. Nevertheless, no issue is more controversial or polarizing at the state and federal level than who should command military forces that are conducting civil support operations.

Currently, under the federal laws described earlier, there is a "constitutional basis for distinct and separate chains of command for state and federal military forces."[64] These separate chains of command have worked well in a single-state crisis such as the April 2011 National Guard response to the devastating tornadoes that struck in Alabama, or to preplanned events such as the 2009 Presidential inauguration.[65]

However, they have not worked well when federal and state forces are working together in unplanned disasters such as the response to Hurricane Katrina. The response by both state National Guard forces and federal forces during Hurricane Katrina was disjointed at the strategic level, which then "significantly degraded the integration and synchronization" of responding National Guard and federal forces.[66]

**Command and Control of Military Forces in Disaster Response**

Two command options are available when federal and state forces are deployed together in the same operating area inside of the United States – Parallel Command and Dual Status Command (DSC). Parallel command has been used frequently in the past "in many large-scale civil support operations."[67] Under this arrangement, state and federal forces operate in the same area of operations under separate chains of command. The response to Hurricane Katrina was eventually conducted under the parallel command structure. The military federal task force – Joint Task Force Katrina – fell under the command of NORTHCOM, led by Lieutenant General Russell Honore. The state task force fell under the command of the governor of Louisiana, led by the Adjutant General, Major General Bennett Landreneau. Although this type of command structure has worked effectively during past pre-planned events, including the 2009 Presidential inauguration, the fact is that this command structure was only effective because of extensive pre-planning, because close working relationships were developed, and because the established coordination occurred before the event took place.

Certainly good working relationships can be developed among Interagency leaders. But at the operational and tactical levels such relationships are not feasible because of the wide array of forces that are involved and the broad range of situations in which they may become involved. Interestingly, Army Field Manual 3-28, *Civil Support*

*Operations*, recommends using this parallel command only when close coordination is possible; further, "its effectiveness depends on a close working relationship between commanders."[68] Such relationships cannot be developed in the 10 days before a hurricane strikes, to say nothing of their prospects in responses to unplanned events. Among other factors, the parallel command structure used in response to Hurricane Katrina contributed significantly to the debacle of that response.

As noted in the Federal Response to Hurricane Katrina lessons learned, "a lack of an integrated command structure for both active duty and National Guard forces exacerbated…coordination issues during the initial response."[69] Colonel Ludwig Schumacher concluded: "The separate chains of command employed during Hurricane Katrina significantly degraded the integration and synchronization…from different commands."[70] Lieutenant Colonel (Ret.) Jeffrey Burkett concurs: "Parallel command military operations can be problematic in the chaotic environment of a disaster recovery because of control of information, timely decision-making…and situational awareness… when command and control are divided."[71]

In *The Utility of Force*, Rupert Smith although commenting on North Atlantic Treaty Organization and United Nations command structures reinforces the limitations of a parallel command structure: "If a student at any military staff college…produced a plan that had forces operating in the same space answering to two different chains of command…he would have his cards marked fail"[72] – and quite possibly be run out of town.

It is easy to see the many disadvantages of relying on a parallel command structure to respond to a sudden disaster. Extensive coordination would be required at every level. Disjointed relief efforts would be unavoidable. Many tasks would be wastefully duplicated. Whether it was due to President Bush's legal restrictions on placing federal forces under command of the governor, or his refusal to invoke the Insurrection Act for fear of the political repercussions, or Governor Blanco's refusal to cede control of state National Guard forces to a federalized response for her own political reasons, the parallel structure was chosen as a last resort to reverse a grossly deteriorating situation in New Orleans.

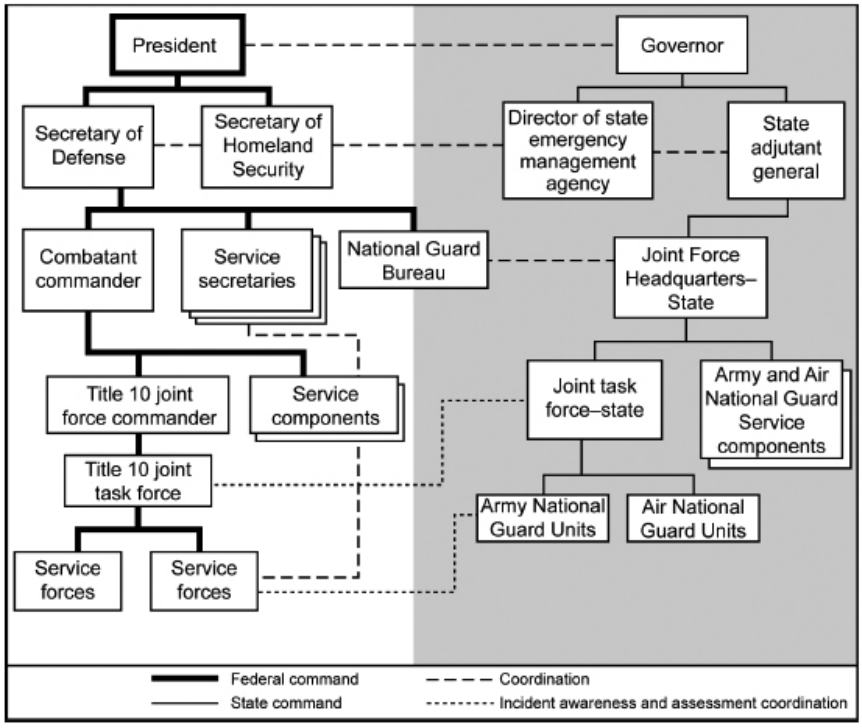


**Figure 3: Example Parallel Command Structure.**[73]

In February 2010, the presidentially formed Council of Governors met for the first time under President Obama's guidance to "strengthen the partnership between federal and state governments in protecting the nation against all manner of threats, including…natural disasters."[74] One of the Council's five working groups – Unity of Effort – was charged with addressing the proper integration of military forces during domestic operations.[75] During the first meeting Secretary Gates, in an attempt to thaw a frozen relationship that had developed since Hurricane Katrina between DoD and the states, acknowledged the responsibilities of governors to provide for the welfare of their states. By August 2011, the Council of Governors and DoD had agreed that the DSC structure would be the usual and customary command and control arrangement when state and federal forces are employed simultaneously.[76]

The DSC structure is not a new command structure within DoD. However, until 2011 this type of command structure has been used

only in pre-planned, single-state operations. The National Guard's support in 2004 for Operation Winter Freeze was a multi-state, and pre-planned effort. This structure was used to provide logistical support for the 2004 and 2008 Republican and Democratic conventions, for the 2004 G8 summit conference, and most recently during Operation Winter Freeze, when the Guard supported the Border Patrol along the Canadian border.[77] But the DSC concept has yet to be challenged in an unplanned disaster. The first opportunity to test this command structure on something besides a preplanned event would have occurred during the response in August 2011 to Hurricane Irene. This storm was bearing down on the East Coast as predictions of widespread flooding, power outages and infrastructure damage were dramatically broadcast to an anxious public. Capitalizing on lessons learned discussions and agreements between the leadership of the states and the federal government, DoD and the state governors decided upon the DSC structure for the projected federal and state response to this incident.

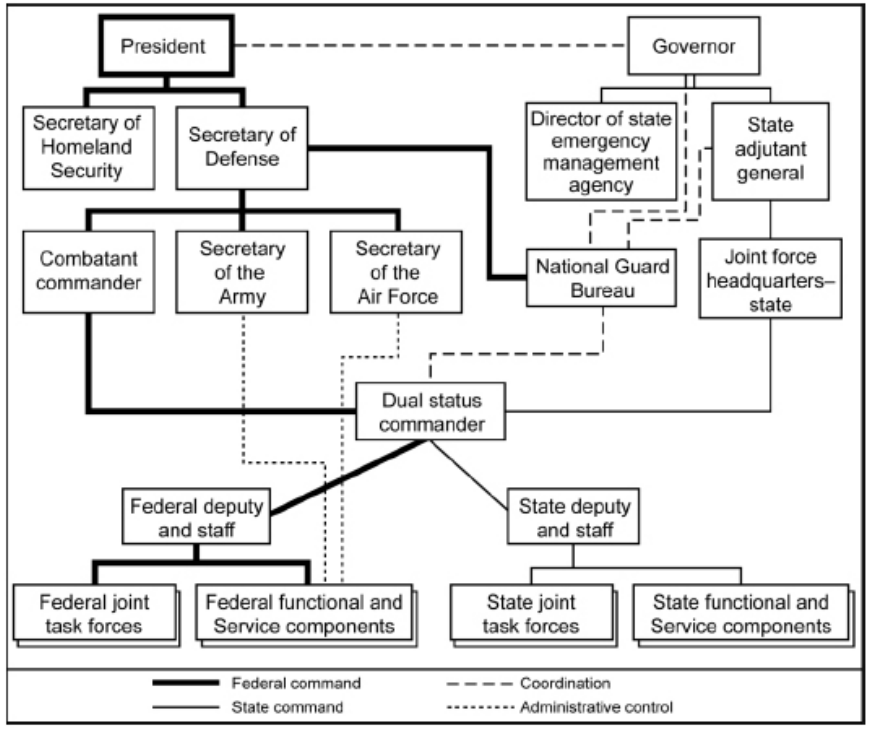


**Figure 4: Example Dual Status Command Structure**

"The Hurricane Irene recovery activities marked the first time that dual-status commanders were used to provide command and control over both active-duty and reserve-component (National Guard and Army Reserve) forces."[78] However, this response went no further than Army North deploying Defense Coordinating Elements (DCE) to FEMA regions in the areas projected to be affected and the assignment of the dual status commanders by the governors and DoD in the four states projected to behit. But Hurricane Irene mainly steered clear of the coast and required no federal response.[79]

The dual status commander will normally be a National Guard officer at the Brigadier General level or higher. This commander will be nominated by the governor and agreed upon by the President through a memorandum of agreement (MOA). This MOA must be signed before the selected officer can perform his or her duties to avoid future complicating liability determinations and confusion over the PCA issues. The previously discussed work around of PCA is embedded in the dual status command structure as well. National Guard officers have precisely the correct legal status to serve as dual status commanders. Further, they are familiar with the area of operations; they are aware of their states' capabilities; they have established relationships that will facilitate disaster responses; and they have working relationships with local, state, and federal officials in their states.

Unlike the parallel command structure the DSC structure does not require extensive pre-planning and coordination prior to its implementation. Most of the pre-planning at the command-level comes during the dual status commander's experiences with NORTHCOM and ARNORTH prior to his or her assignment to that position. The DSC construct acknowledges that the president commands federal forces and that the governor commands state forces. So the designated DSC is able to command federal forces and state forces. But some issues remain.

The separate chains of command of the parallel command structure remain, but there is only one dual status commander. However, this commander must command two different forces with different rules for employment for as long as federal forces are subject to the PCA. Additionally, contrary to common perception, the commander must

execute orders from multiple bosses, namely the governor and the president. If these bosses have conflicting political views, this conflict could jeopardize the response equation.

Federal forces responding inside the United States are hampered by a culturally and politically supported command system. Governors do not want federal forces operating inside of their state without some sort of control over them. Presumably, dual status commanders will provide that control. But neither the President nor DoD want to cede control of federal forces operating in states without retaining the command line that runs through NORTHCOM. Federal officials cite the Constitution to support their rights to control the federal responding force. In November 2009, this author was deployed as an active duty Aviation Battalion Commander task organized under a National Guard Brigade Headquarters for a year. He received no special training or orientation for this assignment. He simply responded to a routine order that enabled U.S. forces to conduct multinational combat operations outside the United States. Our active, reserve and guard forces should be able to work as closely and smoothly in performing domestic operations, especially in response to disasters in our own country.

Joint Publication 3-0 defines tactical control (TACON) as "command authority over assigned or attached forces or commands…made available for tasking, that is limited to the detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned."[80] This command relationship would solve many, if not all, of the challenges that the parallel command structure presented during Hurricane Katrina. It designates a limited command relationship that maintains the command authority and integrity of the unit. The obvious change would be the authorization for a federal force to operate under control of the governor. Recognizing this in 2008 and 2009 Senators Patrick Leahy (D-Vt.) and Kit Bond (R-Mo.), then co-chairs of the U.S. Senate National Guard Caucus, introduced legislation that would give state governors the ability to exercise TACON of federal forces responding to disasters in their states. The DoD opposed this proposal, citing the Constitution in its response to the Senate. In a letter from DoD to the Senate and House Armed Services Committee, DoD resorted to Article II, Section 2 of

the Constitution, which designates the President as the Commander in Chief of the Army of the United States.[81] The President would have to relinquish his command of federal forces to a state governor under this legislation. But DoD's selective use of the Constitutional argument is all too obvious. Why is it possible for active duty units to work side-by-side with National Guard forces in a foreign country yet inside the United States the DoD objects? Seven years after Hurricane Katrina made landfall DoD has shown little if any desire to cede control of federal forces to a governor within the United States. Likewise, governors have shown little interest in allowing federal forces to operate in their states without oversight of a National Guard commander. The TACON relationship that allows federal forces to carry out a specific task under a governor's control addresses the command and control issues that ran amok during the response to Hurricane Katrina. Senators Leahy and Bond have forged the way ahead for military forces operating inside the United States to conduct effective disaster support operations. But the DoD apparently wants none of this.

## Conclusion

Steve Abbot, Chairman of the Advisory Panel on DoD Capabilities for Support of Civil Authorities, chartered to provide DoD and Congress with information on the readiness of the country for disaster response, delivered the panel's findings to Congress on 15 September 2010. This report cited factors that "complicate effective response to major incidents."[82] Among these factors was our federalist system of government presented by the Constitution and the "guarding of prerogatives"[83] by agencies at all levels of state and federal government. These issues persist seven years after Hurricane Katrina made landfall. Nonetheless, there have been numerous changes to facilitate the support that DoD provides to the states during disasters. But the recency of this report to Congress shows that some issues must still be addressed as we prepare for the next incident. The time for political and military diddling has long passed. The citizens of this nation demand their leaders to secure and support the country. They expect unhindered responses to inevitable disasters – natural and man-made. As the panel concludes, "[i]t is an obligation of all those in positions of responsibility to immediately search for, discover and implement

solutions to overcome the barriers to response," regardless of political party or military service culture.[84]

Congress should amend the Posse Comitatus Act to allow federal forces to conduct law enforcement during situations where first and second responders are unable to do so. Additionally, Congress should amend federal statutes to allow federal forces to serve in a TACON relationship under the governor of a state while supporting civil support operations inside of the United States. Both of these suggestions would enable the nation's leaders to employ our entire military force to support beleaguered civil leaders. If our leaders fail to provide these legislative changes, the debacle of our response to the Hurricane Katrina disaster is likely to repeat itself, perhaps on a much larger scale.

# The National Guard on the Southwest Border: Defining the Role

**Colonel Tim Lawson**
United States Army National Guard

> *All across the country, in every region, every city and town, Americans want the federal government doing everything it can to secure our borders.*[1]
>
> —Janet Napolitano, Secretary,
> Department of Homeland Security

Ten years after the attacks on the World Trade Center, the United States finds itself in one war, closing out a second, and in addition spending billions of dollars each year to secure the country. Presidents Bush and Obama considered the security of the U.S. Southwest border at risk, as both deployed National Guard troops to augment the Border Patrol. National Guard troops currently remain on the border providing intelligence, surveillance and reconnaissance and infrastructure support. Multiple threats, and shortfalls in the United States Customs and Border Protection (CPB) capabilities and capacities to combat those threats, continue to hamper border security. These shortfalls, threats and a porous Southwest border combine to create an opportunity for possibly using the National Guard to augment the Border Patrol permanently. The National Guard can contribute additional capabilities and capacities in equipment and manpower to augment the Border Patrol and help fill gaps in border security. The National Guard currently provides Southwest border support to the Border Patrol; however, the intention of the augmentation is to allow the CBP time to increase capabilities and capacities. There is no long term plan to permanently leave the National Guard on the Southwest border. This paper addresses the threats, civilian capabilities and functions, shortfalls in capabilities and capacities, precedence, legality, risks, and appropriateness of military support on the Southwest border. This paper argues that the National Guard is a viable option to augment

the Border Patrol on a permanent basis and continue to support with intelligence, surveillance, reconnaissance and infrastructure support.[2] Now is the time to define the National Guard's mission and role on the Southwest border.

Security controls and policies at America's borders enable the flow of millions of people and facilitate the transactions of billions of dollars of legal commerce each year. Nevertheless, illegal activity exists and sophisticated illegal enterprises are competing to exploit porous borders.[3] The four common types of threats that compete along this gateway are traditional customs and border policing crimes, gangs, transnational criminal organizations (TCO) and transnational terrorist organizations (TTO).[4]

Traditional customs and border policing crimes include illegal immigration, alien smuggling, and narcotics trafficking. All impact the overall quality of life of border residents, economic expansion and environmental protection.[5] Most traditional law enforcement centers on the arrests of illegal immigrants. Federal law enforcement estimates that law enforcement apprehends 10 to 30 percent of illegal aliens who cross the border. A 2005 estimate indicated that as many as 4 to 10 million illegal aliens crossed into the United States during that year.[6] In 2010, CBP turned away over 227,000 aliens who attempted to enter illegally and apprehended more than 8,400 people for various crimes, including murder, rape, and child molestation. CPB also seized over 870,000 pounds of illegal drugs, $147 million in currency, more than 29,000 fraudulent documents, and over 1.7 million pieces of prohibited plant materials, meat, and animal byproducts.[7] CBP and local law enforcement efforts resulted in a decrease in apprehensions of 36 percent nationwide from 2008 to 2010 with the majority of the decrease coming from the Southwest border. CBP views this as an indication that efforts are effective and that fewer people are attempting to cross the borders illegally. However, drug seizures continue to increase by over 50 percent and CBP estimates that they only seize 10 to 20 percent of drugs crossing the border.[8]

The threat posed by gang involvement in drug trafficking is increasing, particularly in the Southwest Region and their influence continues to be a threat to both law-abiding citizens and law enforcement officers.[9]

Gangs form the network for retail drug distribution in the United States and are the dominant retail drug suppliers in large and midsized cities.[10] Additionally, the Southwest border remains the primary gateway for moving illicit drugs into the United States.[11] In 2009, the U.S. Department of Justice (DOJ) estimated that approximately 28,100 gangs with over 731,000 members operated in the United States.[12] These gangs vary in size from a few members to tens of thousands, and their affiliations range from loose ties to coalitions of highly structured multinational enterprises.[13] Gangs use drug distribution revenues to buy weapons and fund other criminal activity, such as kidnapping, racketeering, and property crime. This activity impacts large cities throughout the United States and is not strictly limited to border cities. Many gangs have a direct or indirect involvement with the border for trafficking purposes and their connection to cartels continues to grow.[14] In 2010, at least 15 U.S. gangs reportedly collaborated with Mexican TCOs in attempts to traffic drugs.[15]

DOJ estimates that the costs associated with suppressing gang activity is over $1 billion a year.[16] Securing the border would impact far more than just border areas and help make the United States safer.

A fast growing threat to the Southwest border is the transnational criminal organizations.[17] The Southwest border hosts robust legal commercial activity, however, the border is also the site for violent criminal activity. These enterprises are carried out by organized criminal organizations and include the smuggling of drugs, humans, weapons and cash.[18] Furthermore, this generation of sophisticated and violent cartels is presenting significant challenges to U.S. law enforcement.[19] In 2009, Mexican officials estimated that cartels murdered between 6,500 and 8,000 individuals in Mexico. By 2010, the number increased to more than 11,600 drug related homicides and an estimated 34,500 total deaths since 2006, making the Mexican border one of the most dangerous areas in the world.[20] The struggle for control of lucrative smuggling corridors leading into the United States is creating unprecedented levels of violence.[21] Increased pressure put on the cartels by both Mexican and U.S. security officials is forcing cartels to escalate their tactics, and U.S. law enforcement increasingly experience violent encounters with cartel members.[22] Cartels control much of

the production, transportation, and wholesale distribution of illicit drugs bound for and in the United States.[23] Increasing coordination among Mexican drug cartels, human smuggling networks and U.S. based gangs continue to add to security problems.[24] Additionally, these organizations operate with military style weapons and technology that rival or exceed CBP and local law enforcement capabilities.[25] Law enforcement agrees that little crosses the respective cartel territories along the border without cartel knowledge and that certain cartels are now authorizing the use of force inside the United States to protect their illegal drugs.[26] Law Enforcement agencies continue to report cartel violence spillover creeping closer to a permeable Southwest border, reinforcing the need for continued vigilance.

The threat of transnational terrorist infiltration through U.S. borders remains a critical concern. Each year, U.S. law enforcement agencies apprehend hundreds of Special Interest Aliens (SIA) from Special Interest Countries (SIC) with known ties to terrorist organizations.[27] CBP reported apprehending 59,017 other than Mexicans (OTMs) in 2010, most of whom were apprehended along the Southwest border. OTMs apprehended included 663 from SICs with known terrorisms ties. These countries include Iran, Syria, Cuba, Saudi Arabia, Afghanistan, Somalia, Sudan, Pakistan and Yemen.[28] Admittedly, not all SIAs are terrorists and it is difficult to quantify the true threat that terrorists pose to U.S. borders. Nevertheless, indicators of the threat are clear. For instance, members of Hezbollah, the Lebanon-based terrorist organization, have already entered the United States by way of the Southwest border. In 2002, authorities arrested Salim Mucharrafille, a café owner in Tijuana, Mexico, for smuggling more than 200 Lebanese people into the United States, including several believed to have ties to Hezbollah.[29] Also, in March 2005, Mahmoud Kourani, an illegal alien who had been smuggled across the U.S.-Mexico border after bribing a Mexican consular official in Beirut for a visa, pleaded guilty to providing material support to Hezbollah. Officials discovered that Kourani was the brother of the Hezbollah Chief of Military Operations in Southern Lebanon, and would eventually be found to have solicited funds for Hezbollah terrorist activities from his home in Dearborn, Michigan.[30]

The most recent indication of potential TTO activity along the Southwest border is the alleged attempt by Iran to assassinate the Saudi ambassador to the United States. The United States charged two men, including a member of Iran's special foreign actions unit, known as the Quds Force, in New York Federal Court with conspiring to kill the Saudi diplomat, Adel Al-Jubeir. Justice Department officials say the men tried to hire a purported member of a Mexican drug cartel to carry out the assassination with a bomb attack while Al-Jubeir dined at his favorite restaurant. The purported member happened to be a paid informant for the Drug Enforcement Administration, who exposed the plot.[31]

A significant portion of illicit alien traffic is part of organized criminal and potential terrorist activity, and poses a sizable threat to U.S. national security.[32] The large number of aliens attempting to enter the country illegally could unintentionally provide cover for terrorists and allow them to leverage illicit networks to smuggle a person or weapon of mass destruction into the United States.[33] Although cartels are the fastest growing threat, the case could be made that it is only a matter of time before terrorists take advantage of current conditions and attack the United States. It stands to reason that sophisticated terrorist organizations will find other avenues to attack the United States as increased security closes traditional avenues. CBP acknowledges that the potential exists for a single person or small group to cross the border carrying chemical or biological weapons, weapons of mass effect, or other implements of terrorism, and they could cross undetected.[34]

These concerns prompted the last two U.S. Presidents to react by placing National Guard troops on the Southwest border. President Bush, before his decision to deploy National Guard troops, stated that "the need to enforce our border is urgent, and that's why, in coordination with our governors, we're going to send 6,000 National Guard troops to be deployed on the southern border."[35] Prudence would suggest that National Guard troops remain on the border due to continuing threats of violence spillover from Mexico's drug war, and from the ever increasing concerns over the potential for TTOs to cross unsecure borders while being masked by the large flow of immigrants.

As threats continue to change, so have the organizations that are responsible for the protection of the border. After 9/11, the U.S. government believed that it needed to improve vigilance, increase preparedness, reduce vulnerabilities, and guard against any future attack.[36] A safe and secure homeland means more than preventing terrorist attacks, however. The liberties of all Americans and their privacy must be protected, as well as their safety. Protection must also preserve the means by which we interchange with the world through travel, lawful immigration, trade, commerce, and exchange.[37] The early 2000s brought about the most sweeping reform in government in nearly half a century, with the creation of the Department of Homeland Security (DHS) and the important recognition of the Homeland Security Enterprise. The Quadrennial Homeland Security Review of 2010 identifies the need for collective efforts and shared responsibilities of Federal, State, local, tribal, territorial, nongovernmental, and private-sector partners as well as individuals, families, and communities to maintain critical homeland security capabilities.[38] These organizations have a variety of functions and capabilities within the Homeland Security Enterprise.

The Homeland Security Act of 2002 established a cabinet level Department of Homeland Security and merged most interior and border enforcement functions, placing them under one agency. The four federal agencies that fall under DHS and are responsible for securing the U.S. borders are U.S. Customs and Border Protection (CBP), U.S. Immigrations and Customs Enforcement (ICE), the U.S. Coast Guard, and the Transportation Security Administration (TSA).[39] Since the inception of the DHS, the number of agents has increased from about 10,500 officers to patrol borders and about 17,600 officers inspecting travelers at air, land and sea ports (Ports of Entry, POE) to over 20,000 officers for border protection and over 20,600 for security at POEs. The dollar amount associated with investment amounted to around $11.9 billion for fiscal year 2010.[40]

The CBP is the primary organization within DHS that provides the front line responders to immigrations and customs violations, and is the agency responsible for the entirety of the nation's borders.[41] CBP combines all the previous border law enforcement agencies under

one administrative umbrella. Immigration and Naturalization Service (INS), the Border Patrol, the Customs Service, and the Animal Plant Health Inspection Service make up the CBP today.[42] The CBP mission is to prevent terrorists and terrorist weapons from entering the country, secure the U.S. borders and ports, control flow of illegal drugs, apprehend illegal immigrants, and protect American agricultural and economic interests.[43]

The Southwestern border accounts for over 97% of all illegal alien apprehensions and commands the most attention from DHS and CBP.[44] Forty three POE connect major U.S. interstate highways for lawful trade and commerce.[45] The CBP is responsible for enforcing U.S. immigration and federal laws along the border between official ports of entry. The *National Border Patrol Strategy of 2005*, defines the mission and focuses on five objectives: establishing the substantial probability of apprehending terrorists and their weapons as they attempt to enter illegally between ports of entry; deterring illegal entries through improved enforcement; detecting, apprehending, and deterring smugglers of humans, drugs, and other contraband; and leveraging "Smart Border" technology to multiply the deterrent and enforcement effect of agents; reducing crime in border communities, thereby improving the quality of life and economic vitality of those areas.[46] The national strategy lays the foundation for gaining operational control of the border, focusing on the ability to detect, respond to and interdict border penetrations in high priority threat potential areas. The strategy builds on "Prevention through Deterrence" and relies on agents to rapidly deploy in response to threats.[47]

The Border Patrol divides the Southwest region geographically into nine Border Patrol sectors and conducts a three-tiered border enforcement strategy. Line watch, roving patrol and checkpoints make up the three tiers. As of 2010, over 88 percent of border patrol agents nationwide are dedicated to the Southwest border, totaling over 20,000 personnel and an expense of over 3 billion dollars a year. Most of the Border Patrol's agents perform line watch operations and maintain a high profile to deter, arrest or turn back anyone attempting to illegally enter the United States. The second tier, roving patrols, has the responsibility

to detect and arrest those who make it through the first line of defense and is located behind the line watch elements.[48]

Checkpoints make up the third tier of defense for the Border Patrol. Permanent and tactical checkpoints are located 25 to 100 miles inland and located on major U.S. highways and secondary roads. Permanent checkpoints are fixed facilities that include buildings, technology and computers linked with national law enforcement databases, and operate on major U.S. highways. In eight of the nine Southwest border sectors, there are 32 permanent checkpoints and one under construction in the Tucson Section. Tactical checkpoints are temporary in nature and do not have permanent structures.

Tactical checkpoints augment permanent checkpoints by monitoring and inspecting traffic on secondary roads and focus on areas used by illegal aliens and smugglers attempting to evade permanent checkpoints.[49] As of 2008, there were 39 tactical checkpoints in operation. The non-permanent status of tactical checkpoints affords the Border Patrol the ability to change locations on a daily basis. About four percent of Border Patrol agents man checkpoints; however, checkpoints represent about 35 percent of drug seizures and about two percent of apprehensions on the Southwest border.[50]

In 2006, DHS initiated the Secure Border Initiative (SBI) program, which added technology and fencing capabilities to the Southwest border. As of May 2011, DHS erected 649 miles of fencing, 299 miles of vehicle barriers, and 350 miles of pedestrian fencing in selected locations. The initiative included the purchase of unmanned aircraft systems (UAS). DHS currently has seven UASs operating throughout North America and plans to expand their fleet to 24 total UASs by 2016, including 11 on the Southwest border.[51] SBI added non-intrusive inspection systems, Remote Video Surveillance Systems (RVSS), thermal imaging systems, radiation portal monitors, and mobile license plate readers. The SBI initiative has cost over $4.4 billion to date and has improved border security, but has failed to achieve the levels of security desired.[52]

Despite these massive efforts significant shortfalls in securing the Southwest border remain. These shortfalls in capabilities and capacities

are in the areas of manpower, checkpoint operations, fencing, and patrolling.

Manpower shortages continue to hamper the progress of the Border Patrol to secure the border. As of March of 2011, the Border Patrol reported achieving varying levels of operational control on the Southwest border.[53] The Border Patrol classifies operational control into two levels of control: controlled and managed. Controlled is defined as the ability to deter or detect and apprehend illegal entries at the immediate border and managed is a multi-tiered deployment of Border Patrol resources to deter, detect, and apprehend illegal entries into the United States. Managed level of control spans out to 100 miles or more away. The Government Accountability Office (GAO) recently declared that of the 873 miles of border under operational control, 15 percent is controlled and the remaining 85 percent is managed.[54] The GAO also reported that nearly two-thirds of the 1,120 Southwest border miles that had not yet achieved operational control were at the "monitored" level. Monitored means that across these miles, the probability of detecting illegal cross-border activity is high; however, the ability to respond is defined by accessibility to the area or availability of resources. The remaining miles remain at "low-level monitored," meaning that resources or infrastructure inhibited detection or interdiction of cross-border illegal activity. The Border Patrol report that these two levels of control are not acceptable for border security.[55] DHS also acknowledges achieving an acceptable level of border control across less than half of the Southwest border.[56]

The Border Patrol continues to have problems with checkpoint operations, as well. GAO reported in August 2009 that the Border Patrol lacked the measures to adequately operate these checkpoints effectively and efficiently, and weaknesses in checkpoint design and operation increased the risk that illegal activity may travel to the U.S. interior undetected. Border Patrol officials said that several factors impeded higher levels of performance, including insufficient staff, canine teams, and inspection technology.[57]

The inability of the Border Patrol to adequately patrol fenced areas continues to be a problem. According to CBP, during fiscal year 2010, there were 4,037 documented and repaired breaches of the fencing;

CBP spent $7.2 million to repair the breaches, or an average of about $1,800 per breach.[58]

Due to continuing threats and shortfalls in capabilities and capacity, DHS requested National Guard assistance in July of 2010.[59] At present, National Guard troops are positioned on the border in an effort to combat the transnational criminal organizations that smuggle weapons, cash and people across our Southwest border.[60]

The inability of DHS to obtain operational control of the border indicates that there is a need for additional support and has border governors, congressmen and senators requesting National Guard support.[61] U.S. Senators John McCain (R-AZ) and Jon Kyl (R-AZ) introduced the Border Security Enforcement Act of 2011, which is a 10-point comprehensive border security legislation to combat illegal immigration, drug and alien smuggling, and violent activity along the border between Mexico and the United States. This legislation includes the request to immediately deploy no fewer than 6,000 National Guard troops to the Southwest border and deploy 5,000 additional Border Patrol agents to the Southwest border by 2016.[62] The concern expressed in the McCain-Kyl initiative is not isolated. In a letter forwarded by the National Treasury Employees Union to Senator Joe Lieberman, the CBP was reported to be understaffed and requiring more manpower to provide even minimal security to the borders.[63] Similarly, a recent article in *The Journal of Strategic Security* cites a recommendation to double the CBP workforce in the next five years.[64]

While the Border Patrol's strategy still includes the ambitious goal of gaining operational control of our nation's borders[65] current concerns over the climbing U.S. debt may have significant impacts on the DHS budget and future manning and equipment initiatives. The Fiscal Year 2011 budget included a requested reduction of 181 border agents for the Southwest border area.[66] This reduction coupled with a ten percent attrition rate for the CBP may have an impact on the ability to obtain desired control of the border.[67] Although the Border Patrol continues to increase operational control on an average of 126 miles each year, there is plenty of room for improvement.[68]

The Border Patrol credits the slow progress primarily to having to prioritize its resources to sectors deemed to have greater risk from illegal activity and diverting assets from other areas.[69] Placing the National Guard on the border permanently to augment the Border Patrol could be one step taken to help to facilitate achieving operational control of the border in the face of shortfalls that currently exist and those that appear to be forthcoming.

The formation of the U.S. Border Patrol in 1924 marked the transfer of responsibility for securing the border, away from the military to a new Federal agency.[70]

From that point, the role of the military on the border was largely non-existent until the 1980s. The passing of the *Defense Authorization Act of 1982* reestablished a role for the military in support of law enforcement in the nation's so called "War on Drugs." This Act allowed the military to operate and maintain military equipment on loan to federal law enforcement agencies, train law enforcement officers, and report and share information on criminal activity.[71] The passing of the *Defense Authorization Act of 1989* expanded upon the 1982 authorizations by allowing the U.S. military to loan equipment to state, and local law enforcement agencies in counter drug and drug interdiction operations.[72] Although these Acts greatly enhanced the military's capability to support civil authorities, it did not allow the military to directly participate in police activities.[73]

*Operation Jump Start*, initiated in 2006, authorized the deployment of up to 6,000 soldiers along the borders of Texas, Arizona, New Mexico, and California. National Guard Soldiers and Airmen served along the border to support the U.S. Border Patrol's efforts to stem the flow of illegal immigrants into the United States.[74] President Bush made it clear that National Guard soldiers would only support the Border Patrol by operating surveillance systems, analyzing intelligence, installing fences and barriers, building and improving patrol roads and providing training. Guard members did not serve in a direct law enforcement role, but provided much needed reinforcement to the Border Patrol.[75]

By the time Operation Jump Start ended in July of 2008 over 30,000 National Guardsmen had participated in the unprecedented operation

from across the nation. During this time, there was a reduction in both criminal activity and the apprehension of illegal aliens on the border.[76] Operation Jump Start officially ended on July 15, 2008.[77]

President Obama authorized the call up of 1,200 National Guard troops in May of 2010. This authorization was in response to requests from the four border state governors to provide support in the fight against illegal immigration and criminal activity along the border.[78] National Guard troops currently remain on the border helping with intelligence work, drug and human trafficking interdiction, and relieving border guards on security tasks in order for them to conduct more law enforcement activities.[79] The National Guard is providing support, but are not arresting or engaging in enforcement activities directly attributed to any illegal crossing of aliens or narcotics.[80] Deployment of National Guard troops provide enhancement to border protection and law enforcement personnel from DHS and DOJ to target illicit networks trafficking in people, drugs, illegal weapons, money, and the violence associated with these illegal activities.[81]

Shortages in manpower and equipment, the continual increase of threats, and the demand from Border States, all point to the need for filling the gaps in order to secure the Southwest border. However, using the military on the border invokes valid questions particularly in respect to the legality, risks and appropriateness associated with such an option.

Specific constitutional authority and legislative acts permit and limit the use of military forces on the borders. The constitutional authority that permits Congress and the President to deploy armed forces are contained in Articles I, II and IV of the United States Constitution. Article I, Section 8 authorizes Congress "to provide for calling forth the Militia to execute the Laws of the Union, suppress Insurrections and repel Invasions."[82] Article II, section 2 establishes the President's authority to faithfully execute the laws of the United States and to serve as the Commander in Chief of the Army and Navy, as well as the Militia of the States.[83] Article IV requires the federal government to protect each State against invasion and against domestic violence.[84]

The Posse Comitatus Act (PCA) of 1878 is the primary act that limits military participation in civilian law enforcement within the United States. The PCA states "Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army as a posse comitatus[85] or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both."[86] The PCA is the legal framework that restricts the operation of active duty military within the borders of the United States. This act forbids the direct participation of active duty military personnel in search, seizure, arrest, or other similar activity during support activities to civilian law enforcement agencies.[87] The PCA does not prevent the military services from supporting the police, nor does it preclude them from enforcing the law when so ordered by the president. It does prevent them from being the police under normal circumstances.[88]

The PCA applies to federal forces and does not apply to the National Guard unless they are "federalized."[89] The National Guard may be called to active duty in an exclusively federal status (Title 10 of the United States Code), in an exclusively state status, or under state control with federal pay and benefits (Title 32 of the United States Code).[90] Title 10, for instance, is the authority that National Guard units are serving overseas in support of Operation Enduring Freedom in Afghanistan. Under a Title 10 duty status, National Guard personnel operate under the control of the President, receive federal pay and benefits, and are subject to the PCA.[91] Under Title 32 duty status, National Guard personnel generally serve a federal purpose and receive federal pay and benefits, but command and control remain with the governor.[92] As an example, in Operation Jump Start, National Guard troops remained in a Title 32 status and under control of the governors of the four states. This status would allow the National Guard forces to provide the maximum extent of administrative and command flexibility for support.[93]

The exception to the PCA is when the National Guard remains under control of a state, in a Title 32 or a state active duty status,[94] and does not enter into a federal status.[95] However, once federalized, National Guard troops fall under a Title 10 duty status and PCA applies.[96] The

use of the National Guard tends to be the best fit for use of military forces for a border mission. This is due to the ability of border governors to maintain National Guardsmen in a Title 32 duty status and exempt them from the restrictions of the PCA. This exemption allows more flexibility for use, if required.

The passing of three Acts expanded the role of the military support to law enforcement agencies. In 1981, Congress passed the Military Cooperation with Law Enforcement Agencies (MCLEA) Act, which prescribed how the DOD could assist in the war on drugs. The Act permits the military to execute the following supportable activities: sharing of information; loaning equipment and sharing facilities; providing expert advice and training; and maintaining and operating equipment in conjunction with counterterrorism operations or the enforcement of counterdrug laws, immigration laws, and customs requirements.[97] The National Defense Acts of 1991 and 2006 expanded DOD support to federal, state, and local law enforcement agencies in support of counterdrug and counterterrorism operations. The 1991 Act provided for the construction of roads, fences, and lighting along the U.S. border; providing linguists and intelligence analysis services; conducting aerial and ground reconnaissance; and establishing command and control networks to integrate with law enforcement and military activities.[98] The 2006 National Defense Act authorizes the military to deploy assets to the border to assist DHS in order to deny terrorists, drug traffickers, and unauthorized aliens. However, military forces are to only provide an augmenting capability and operate in a supporting role to federal, state and local law enforcement.[99]

The military was not to perform any direct law enforcement activities, which enabled them to support and remain within the limits of the PCA.

The use of the military to aid in securing the Southwest border has inherent risks and the United States will need to address the mitigation of those risks. Primary risks include concerns surrounding lethality and the perception of militarization on the one hand; and the high operational tempo of the National Guard on the other. Although not all inclusive, these are risks that will require attention.

The modern National Guard has become a combat seasoned force whose lethal potential may raise concerns when placed in a border security mission. However, among today's threats are heavily armed organizations that easily rival or exceed the protection afforded the Border Patrol.[100] Increased pressure placed on cartels by Mexican and U.S. security officials has caused the cartels to escalate their tactics. U.S. law enforcement officials increasingly experience violent encounters with cartel members.[101] Rick Flores, a Texas Sheriff, spoke before a congressional hearing in 2006 and said that "cartels utilize rocket propelled grenades, automatic weapons, and use body armor and Kevlar helmets."[102] In January 2006, law enforcement agencies seized a large cache of weapons in Laredo, Texas. Among the items seized were two completed improvised explosive devices and materials for making thirty-three more. They also found large quantities of AK-47 rifles, ammunition, and bullet proof vests.[103]

Attacks on CBP agents continue to increase on the Southwest border. Between 2009 and 2010, CBP agents experienced a 45 percent increase in assaults against them.[104]

Introduction of military forces, serving alongside CBP agents, could potentially serve as a deterrent to these kinds of assaults. An armored high mobility multi-purpose wheeled vehicle (HMMWV) is not too much lethality to counter the types of adversaries we are discovering along the border.

However, perceptions of militarization of the border could send an unwanted message to the world that the United States may no longer be "open for business." This goes against the U.S. open door/land of opportunity reputation. The clash between national sovereignty and the human rights of immigrants has inspired several activist groups to file suit against U.S. border enforcement policies with the Inter-American Court of Human Rights and charges of militarization are prominent in their protests.[105]

Activists argue that soldiers have skills for military combat and are poorly suited to resolve such issues as immigration and border protection. They claim that the United States has embarked on a

dangerous and far-reaching precedent at a time when anti- immigrant hysteria is rampant.[106]

However, it is important to note that these arguments only apply to immigration issues and do not address either criminal or terrorist threats on the border. An Opinion Research Corporation poll conducted in May 2006 showed that 64 percent of Americans were in favor of sending National Guard troops to the border.[107]

In order to mitigate the perceptions of too much lethality and a militarized border, the United States will need to establish a strategic communication plan to reassure the American people. The foundation of that plan should be a simple depiction of the mission. The National Guard is currently augmenting the Border Patrol, supplementing surveillance, increasing intelligence analysis and providing engineer support. It is not arresting, apprehending, detaining or incarcerating aliens. The military understands that it is not their job to be a police force, nor are they trained for those types of missions. The intent is not to be another law enforcement agency, but merely an augmentation to the CBP.

The strategic communication plan will also need to communicate that we are not enforcing laws against American citizens, but against illicit trafficking and illegal aliens, while reinforcing between the ports of entry and under control of DHS and the Border Patrol. Americans must understand that this is a measure to prevent illegal entry by organizations and people with intent to do harm to the United States and its citizens. The National Guard, if needed, could provide a response with the capabilities required to counter any external threats that may potentially escalate beyond the capability of the CBP.

The United States runs the risk of potentially overextending its reserve components through a permanent military solution for securing the border. Governors may balk at relinquishing their units to go and support border missions. This possessive nature is understandable, as they feel they need these assets in their state in case of an emergency. The current operational tempo of the National Guard has been high due to the wars in Iraq and Afghanistan and left many states with lower troop levels to respond to emergencies. During Operation Jump Start

(OJS), governors retained the authority to decline OJS missions that might degrade their own ability to respond to crises.[108] The National Guard's ability to deploy over 30,000 citizen soldiers and airmen from across the nation while having close to 50,000 soldiers deployed to support overseas contingency operations demonstrates that non-border governors recognized the shared need to respond. This is a gateway issue that requires a national response, and the National Guard has been willing to pay their part.

This risk is decreasing as U.S. troops are coming out of Iraq. Permanent missions and an established number of forces required to augment Border Patrol will bring some predictability to this mission. The use of the Army Force Generation model (ARFORGEN) can identify a long term, unit rotation plan that takes into consideration the requirements of each state. The National Guard Bureau can implement a sourcing plan for units to rotate through this mission and balance the War on Terrorism.[109]

The National Guard's number one priority is the security and defense of our homeland, at home and abroad and is the appropriate force of choice for supporting border security. The inherent mission of the National Guard, as the first military line of defense for the homeland, helps to make the National Guard's use on the border a natural fit, aligning that mission with their long standing role. The former Acting Director of the Army National Guard, MG Raymond Carpenter, recently addressed Army War College students, and reminded the audience that the National Guard must continue to stay meaningful and engaged to continue to be relevant.[110] A permanent border solution could give the National Guard that meaningful engagement. MG Carpenter further stated, "The National Guard is the right force, as well as the force of choice for a border mission. The National Guard is capable of providing the full spectrum of options regarding support to the CBP, from observer missions to security missions of great intensity. Although not routine to the Guard prior to 9/11, it fits with our dual mission responsibly, federal and state, to protect the citizens of our country."[111]

The Army National Guard currently has over 350,000 personnel and 28 Brigade Combat Teams (BCT) in its ranks that could fulfill a

permanent brigade size mission on the border and not impact current troop strength required for Afghanistan.[112] A standardized unit to fill a border mission would facilitate numerous planning and equipping issues associated with this requirement. The use of a BCT could help National Guard Bureau standardize this mission with personnel and equipment. The National Guard currently has one BCT in Afghanistan and has no requirement to backfill it. Upon return of the 45th IBCT, there will be no BCTs deployed from the National Guard and none scheduled in the foreseeable future, making the use of BCTs a feasible option for the National Guard.[113] BCTs have anywhere from 3,460 to 3,720 personnel, depending on the type of BCT (Light, Heavy or Stryker). The use of a BCT gives a consistent number for augmentation on the border and works well with planning and resourcing, while providing a headquarters for command and control.

The use of National Guard BCTs provides equipment that would be of great use to border security. Currently the Border Patrol uses Unmanned Aerial Systems (UAS) and night vision equipment for border security. UAS systems reside in the CBP's Office of Air and Marine division.[114] A BCT has four UASs and are a part of the Tactical Unmanned Aerial System (TUAS) Platoon in the Brigade Special Troops Battalion. The specialized equipment that a BCT has to offer makes the use of a BCT the most beneficial unit for a border mission. The permanent use of the National Guard to augment the Border Patrol could eliminate the need to purchase additional equipment that would be redundant, ultimately save money and afford valuable training opportunities for the National Guard.

The great strides gained over the past ten years by National Guard forces fighting in combat zones have been momentous. The permanent assignment of the National Guard on the border can capitalize on this experience and help the National Guard remain relevant to the homeland security fight. The DoD, in cooperation and consultation with DHS, should consider implementation of the following recommendations:

- ***Establish permanent border regions for the National Guard.*** Permanently establish regions for augmentation of the Border Patrol by the National Guard and build a permanent brigade-size facility and corresponding battalion facilities to support

rotational National Guard units. This will create a joint operating environment and facilitate the augmentation of the Border Patrol. The building of these facilities will address the issue of lodging and sustainment for National Guard units and ultimately be cost effective in the long run. The need to identify ideal locations for facilities will require additional studies and Border Patrol input.

- ***Permanently position a brigade set of equipment on border.*** Position a brigade set of equipment on the border for units to fall in on. The equipment drawdown in Iraq could provide many HMMWVs and equipment for repositioning and available for use on the border. Units can deploy and fall in on the equipment much like they did in Iraq and as they are currently doing in Afghanistan. The positioning of equipment reduces costs and eases the logistics of rotating units to the border.
- ***Increase manning to provide for duration staff.*** Department of the Army should allocate additional Active Guard and Reserve (AGR) assets to support a full time duration staff to help manage the facilities and the rotation of units. These AGR personnel should fall under NORTHCOM and be the primary liaison for the Guard's border mission. Permanent assignment of these troops will provide continuity with NORTHCOM, rotating units and the Border Patrol.
- ***Establish detailed rotation plans.*** Synchronize rotation plans with the ARFORGEN cycle to establish predictability and allow governors to plan for their states. Synchronized border mission rotations with potential operational deployments overseas will require careful monitoring to minimize operational fatigue of National Guard units; however, coordination between the National Guard and Forces Command can address this issue.

The implementation of these key recommendations will help establish a permanent solution for the National Guard to augment the Border Patrol on the Southwest border. The recommendations contribute to keeping the Guard operational while providing a vital, relevant mission. Although much is required to execute a plan that allows the National Guard to permanently augment the Border Patrol, this paper outlines the start point to facilitate that process.

The current mission of the National Guard does not necessarily need redefining, as their dual mission is to provide to the states trained and equipped units to protect life and liberty, while providing the nation trained and equipped units to globally defend the United States and its interests.[115] Permanently placing the National Guard on the border fits within these mission sets and provides an excellent capability for supporting security on the Southwest border. The mission should only include supporting the CBP with surveillance, intelligence analysis and engineering support. National Guardsmen should provide support in an augmentation role and refrain from any direct law enforcement duties. There is no expectation that the National Guard will replace law enforcement, but only augment them to allow for increased security. The dual mission unique to the National Guard and troop draw downs facilitate the expansion of the role of the National Guard with additional Homeland Security missions. Likewise, the threats, alongside shortfalls in capabilities and capacities of the CBP support the need for additional assistance.

The use of the National Guard to augment the Border Patrol is a viable, economic and appropriate solution that can help address Americans growing concerns over organized crime and international terrorism and the government's ability to secure the Southwest border in the face of those threats. Securing U.S. borders will continue to be a prominent and growing focus of U.S. strategic planning, unilateral law enforcement, military actions and cross-border cooperation.[116] The many complex issues associated with controlling the security of the Southwest border will require all elements of national power. Additionally, security will need to be a coordinated effort of both interagency and intergovernmental agencies in order to ensure the level of protection required to keep the United States safe from these threats. It is time for the United States to examine the National Guard's role and mission in relation to defending the homeland and make them an integral part of protecting America's borders.

# Section Two

## Change Continues: Emerging Issues in Homeland Security and Defense


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

# Introduction

**Dr. Brian Nussbaum, Ph.D.**

Homeland Defense and Security Issues Group
Center for Strategic Leadership and Development
U.S. Army War College

Homeland security and homeland defense mean many things to many people. For example, both the government agencies who engage in homeland security,[1] and the scholars and researchers who study it,[2] have faced problems defining it with any great precision and consistency. That is largely because of the changing nature of the threat and risk environment that homeland security is a response to. As the risk environment has changed, so too has the set of activities that are considered to be homeland security (the same is true of homeland defense); emerging threats and hazards have led to innovation and policy change. As new issues emerge, homeland security and homeland defense must adapt to keep pace. In fact, the story of defending and securing the homeland is indeed one of a mission that has changed in response to new threat environments, resource availability, and national priorities. The increasing salience of natural disasters after Hurricane Katrina, or the emerging focus on cyber security today, do not represent a break with the past as much as they do a continuing calibration of the efforts to protect American citizens, their property and their way of life.

## The Case of the Changing Concept of "Homeland Security"

Immediately after the attacks of September 2001, the idea of homeland security was encapsulated in the October 2001 formation of the President's Office of Homeland Security, led by former Pennsylvania Governor Tom Ridge. About a year later, in November 2002, the Office of Homeland Security became the Department of Homeland Security (DHS), incorporating more than twenty agencies in the largest reorganization of the federal government in a generation. This early version of homeland security was very much a reaction to the

attacks in 2001, and focused almost entirely on countering the threat of terrorism.

However very quickly, there were discussions about an evolving understanding of what homeland security was. In 2004, the Center for Strategic and International Studies (CSIS) and the Heritage Foundation suggested a reorganization of DHS in a document entitled *DHS 2.0: Rethinking the Department of Homeland Security*.[3] While this document did not call for a wholesale reevaluation of what homeland security was, it did suggest organizational changes and reorientation that would adjust the early counter-terrorism focus. It suggested numerous adjustments and alterations that were ultimately adopted by DHS, including increased focus on Risk as a framing and driving concept, establishing DHS authorities (and limitations) for missions like infrastructure protection and cyber-security, and improving and streamlining agency management. In 2005, DHS announced the findings of a "Second Stage Review" that included many of the changes to the organization that were advocated for in the Homeland Security 2.0 report.[4] If "homeland security 1.0" was solely about the countering the terrorist threat, "homeland security 2.0" was defined by a broadening focus on other risks to populations and infrastructure.

The next major change to homeland security would follow the crushing and well-publicized impact of Hurricane Katrina on the Gulf Coast in 2005. The death of over 1500 Americans and the tens of billions of dollars of damage to the coastal areas shocked the nation and forced a reexamination of the kinds of threats, hazards and risks that needed to be addressed in homeland security. New or reinvigorated discussions about many issues – the role of the Federal Emergency Management Agency (FEMA) in DHS, the threat of natural disasters, infrastructure resilience, and the role of federalism in disasters and catastrophes – all followed.[5]

The same two organizations that issued the Homeland Security 2.0 report – CSIS and the Heritage Foundation – put out a follow-on report in 2008, entitled *Homeland Security 3.0: Building a National Enterprise to Keep America Free, Safe and Prosperous*.[6] This 2008 report made explicit some discussions that had been percolating in the homeland security community since at least the Hurricane Katrina

debacle. "Resilience" became a key term – protecting people and infrastructure was not enough, rather communities and infrastructure needed to engage in preparedness and mitigation activities to leave them able to spring back after damaging shocks. The federal government – and governments generally – were not in a position to handle the entire burden of preparedness and emergency response; rather a "whole of community" response involving the private sector, charities and individuals and a culture of preparedness were needed. In the same way that some of the recommendations from the first report made their way into policy and doctrine, so too did many of the suggestions in the 2008 Homeland Security 3.0 report. FEMA adopted the "whole of community" approach to preparedness and disaster planning,[7] and Presidential Policy Directive 8 enshrined the role of resilience in policy.[8]

**Emerging Issues in Homeland Security and Homeland Defense**

Much as the concept homeland security has evolved overtime, so too have the problem sets that homeland security and homeland defense practitioners have been forced to deal with. Today there is a new set of issues with which security practitioners must contend. These include internal constraints (fiscal and resource limitations), new vulnerabilities (cyber security concerns), and areas of the homeland that are becoming increasingly salient in security discussions (the Arctic).

One of the most widely discussed issues in the homeland security and homeland defense realms today – and in many policy areas – is the specter of budget cuts and fiscal austerity. Doing "more with less," and the prioritization of missions is a key aspect of organizational response. Beth Wald provides a controversial argument about one way in which resources could be reallocated, when she suggests eliminating or minimizing the role of the Department of Defense (DoD) in combating narcotics trafficking.

> *The DoD should not be treated as a contractor with services available for hire to other departments. It should perform missions that it is uniquely capable of performing, not additional missions it is able to perform or support. DoD's resources are greatly constrained. The Department needs to be prepared for the next 9/11 and other crises. It does not need to be performing ancillary*

> *missions, especially those for which there has been so little return on more than two decades of investment.*

This kind of out-of-the-box thinking is likely to be important to dealing with decreases in resource availability.

Cyber security is one of the major areas of growing concern in homeland security and homeland defense. The increasingly interconnected information systems that underpin much of our economy and critical infrastructure, combined with emerging cyber threats that can cause physical damage in the real world (as evidenced by the STUXNET infection that reportedly damaged Iranian nuclear facilities) have made cyber security a hot button issue in homeland security and defense. Lieutenant Colonel Charles Douglass describes some of the legal authorities and requirements that both enable and restrict the ability of practitioners to protect networks, secure infrastructure and respond to such cyber threats.

Finally, the expansion of resource extraction (petroleum exploration, mining, etc.) and tourism in the Arctic region will have major impacts on the need for security and disaster response capabilities to operate in the region. Lieutenant Colonel Wayne Bunker provides an important overview of the key stakeholders and strategic security issues in the Arctic region, as well as the impacts of Climate Change and international cooperation on U.S. policy there. The DoD and the Coast Guard are likely to be particularly affected as they are among the few government agencies with the air and maritime capabilities to reach the area.

# Ending the Military's Counternarcotics Mission

**Beth S. Wald**
Defense Intelligence Agency

> *Let this be recorded as the time when America rose up and said no to drugs. The scourge of drugs must be stopped. And I am asking tonight for an increase of almost a billion dollars in budget outlays to escalate the war against drugs. The war must be waged on all fronts. Our new drug czar, Bill Bennett, and I will be shoulder to shoulder in the executive branch leading the charge….And much of [the money] will be used to protect our borders, with help from the Coast Guard and the Customs Service, the Departments of State and Justice, and, yes, the U.S. military.*[1]
>
> —President George H. W. Bush, February 9, 1989

Thus, the U.S. "War on Drugs" was introduced to the U.S. public. The U.S. military had worked with other countries combating illicit narcotics production and trafficking before that time. President Bush's February 1989 primetime speech, however, marked a shift that would lead to billions of taxpayer dollars being spent by the Department of Defense (DoD) in its counternarcotics mission, named a national priority by then-President Bush and every U.S. President since then. This paper will question the results of the U.S. military's counternarcotics effort and propose that in today's constrained fiscal environment, perhaps the military should begin to withdraw from that mission and instead refocus its efforts on its key mission areas, i.e., more tangible threats to our nation's security.

## Background

Prior to FY1989, DoD's counternarcotics efforts had been largely limited to supporting law enforcement agencies with training, assistance, and aircraft.[2] Giving the DoD an expanded counternarcotics mission had

been a subject of some debate in 1988, when then-Secretary of Defense Frank Carlucci and former Secretary of Defense Caspar Weinberger publicly opposed formally expanding the U.S. Armed Forces' role in narcotics interdiction. They argued "that the mission of the armed forces is to protect the nation from foreign armies, not drug smugglers, and that civilian law enforcement agencies, especially the Coast Guard, should be given the resources necessary to do the job."[3] Under new leadership, the DoD was forced to comply when President George H. W. Bush introduced the *National Drug Control Strategy* which brought the U.S. military into the forefront of what was then called the "War on Drugs" in 1989.

> *As the perceived threat of communism faded and eventually collapsed in the 1980s, the drug war replaced the Cold War as the military's central mission in the Western Hemisphere. Few in the military establishment, however, embraced the counternarcotics mission enthusiastically.*[4]

National Security Directive (NSD) 18 identified "reducing the flow of illegal narcotic substances to the United States," as a principal foreign policy objective of the Bush Administration. The directive stated that narcotics abuse is devastating to our society, has had a "destabilizing effect on friendly governments," and should be "dealt with aggressively."[5] The corresponding National Defense Authorization Act designated DoD as the lead agency for the "detection and monitoring of aerial and maritime transit of illegal drugs into the United States."[6] It directed Secretary of Defense Dick Cheney to revise DoD policy guidance to expand military support of U.S. counternarcotics efforts and provide counternarcotics training to the governments of the Andean region, under what became the Andean Initiative.[7] The military's focus was and remains on illicit-narcotics eradication and interdiction.[8] Initial DoD guidance approved by Cheney included, "(1) Assistance for nation-building, (2) Operational support to host-country forces, and (3) Cooperation with host-country forces to prevent drug exports."[9] On September 18, 1989, Cheney called on the leaders of the armed forces to develop plans to counter the flow of illegal drugs from entering the United States. He also called for plans to deploy military forces in

support of U.S. and allied law enforcement agencies, especially along the U.S.' southwestern border.[10]

Since then, DoD has spent billions of dollars combating the illicit drug trade, with little to show for it. According to one British correspondent: "Four decades on, in a world (and an America) accursed by poverty and drugs, there is almost universal agreement that the war on drugs has failed as thoroughly as that on poverty."[11] There are several possible reasons for the low return on investment of the U.S. military's counternarcotics efforts. One reason for this apparent failure is that the armed forces are not appropriately trained to combat criminals and criminal organizations. Another reason is that focusing on the supply side of the problem by combating the narcotics production and trafficking has proven ineffective over the decades DoD has been engaged in the effort. A third reason for the apparent failure of the military's counternarcotics program is a lack of viable metrics. Finally, a far more controversial reason relates to the nature of the illicit drug problem. If illegal drugs and the narcotics production and trafficking organizations are actually social welfare and law enforcement challenges, rather than threats to national security, the military is arguably the wrong tool to counter them.

The DoD should begin to wind down its role in combating drug trafficking. The military has been visibly and formally engaged in the counternarcotics effort since 1989, when so directed by Congress and the President. In that time, its impact has been minimal, with little to no effect on either the supply or price of illicit narcotics entering the United States. The mission was initially opposed by DoD leadership which subsequently was compelled to implement it. Especially in this era of fiscal austerity, the application of military force to a mission which arguably falls outside the military's key mission areas seems doubly inappropriate.

**Mission Mismatch**

The armed forces are primarily trained to fight other military or paramilitary forces, or as the saying goes, "to kill people and break things." Military personnel are not trained for law enforcement, and especially not for law enforcement activities on the U.S. side of our

borders where they are routinely called upon to provide direct support to law enforcement agencies (LEAs) against narcotics traffickers. One example is that military personnel are collocated with Drug Enforcement Agency (DEA) personnel at the El Paso Intelligence Center where they share intelligence information and support LEA operations.

One guiding principle of DoD's counternarcotics efforts is that in accordance with the Posse Comitatus Act (PCA) of 1878, the military is not permitted to take an active role in law enforcement activities. Still, since 1980, Congress and the President have significantly weakened the prohibitions of the PCA seemingly in order to permit military personnel to more aggressively pursue a counternarcotics border mission.[12] One example is the *Military Cooperation with Civilian Law Enforcement Agencies Act*, passed by the U.S. Congress in 1981.[13] The act, codified in Title 10 of the U.S. Code, Chapter 18, allows the DoD to provide equipment, facilities, training, advice, and, "any information collected during the normal course of military training or operations that may be relevant to a violation of any Federal or State law within the jurisdiction of such officials."[14] In the late 1980s, when increasing DoD's role in narcotics trafficking was under debate, Congress favored giving law enforcement duties to the military in patrolling the nation's borders. In 1988, the U.S. House of Representatives voted to have the military "seal the borders" to narcotics trafficking within 45 days, "while the Senate voted overwhelmingly to expand the role of the military in the anti-drug campaign."[15]

The 1989 National Defense Authorization Act, cited earlier, identified DoD as the single lead agency for the tracking and monitoring of illicit drug transfers into the United States, by sea or by air, also effectively weakening the provisions of the PCA.[16] Although given the narcotics trafficking detection and monitoring mission in the air and at sea, DoD was not given responsibility for that mission on land.

Occasionally, the military has been called upon to provide surveillance and monitoring support to law enforcement authorities along our southwestern land border, at a significant expense. Two recent National Guard deployments to the border cost about $1.35 billion through last September. The first was significantly larger with about 6,000 personnel, from June 2006 to July 2008. A deployment of some

1,200 personnel from July 2010 through September 2011 cost close to $145 million. The deployments were authorized under Title 32 of the U.S. Code, and therefore, federally funded; but the troops served under their respective governors.[17] In 2006, President George W. Bush announced the deployment of up to 6,000 National Guard troops to the southern border under Title 32 of the U.S. Code. The Guard units also served under their respective governors, while fully funded by the federal government, i.e., DoD.[18]

DoD rotary and fixed wing aircraft began replacing the National Guard contingent in January of 2012. "Aircraft outfitted with high-tech radar and other gear can cover more ground than troops in spotting and catching illegal border crossers and drug smugglers," the *Army Times* reported.[19] In addition to surveillance activity, the aircraft are also available to transport Customs and Border Patrol (CBP) agents to a site where illegal activity is spotted.[20] The National Guard planned to reduce its presence on the border from the 1,200 authorized in 2010 to 300 in 2011, and to none by the end of 2012. The premise is that CBP would, in that time, increase its number of agents on the border as well as the requisite technology.[21]

Some, such as pundit Bill O'Reilly of Fox News and Texas Governor Rick Perry, suggest raising the U.S. military's role in the counternarcotics realm by again having its active duty component patrol our southern border with Mexico, or by increasing DoD's unmanned aerial vehicle monitoring of the border.[22] Perry even suggested during a campaign stop last October that he if were elected President, he might deploy U.S. military forces to the Mexican side of the border. "It may require our military in Mexico working in concert with them [the Mexicans] to kill these drug cartels and keep them off our border."[23] U.S. Senators John McCain and Jon Kyl in 2010 called for 3,000 National Guardsmen to be sent to the Arizona-Mexico border as part of a comprehensive national border security plan to, "combat illegal immigration, drug and alien smuggling, and violent activity along the southwest border."[24] The presence of armed military personnel along our nation's borders would not present the image of a welcoming democratic country and could cause consternation in Mexico. More significantly, the Mexican government is trying to downplay the U.S. role, especially its military

role, in assisting its law enforcement and military counternarcotics efforts. Also, Soldiers and Marines are not border guards, and are not trained for law enforcement responsibilities.

The dangers of having them on the border can be seen in the 1997 shooting of 18-year-old Texas high school student Esequiel Hernandes, who was herding his family's goats near the Mexican border. Unfortunately for him, the teenager fired his .22 caliber rifle in the direction of a camouflaged Marine patrol, possibly to scare away wild dogs. Rather than announcing themselves and demanding that the teen drop his weapon, as law enforcement officers would have been compelled to do, one Marine returned fire, with deadly consequences.[25]

**Supply and Demand**

Attacking the "supply" side of the U.S. drug problem has proven largely ineffective in that as long as "demand" persists, the suppliers have demonstrated they will rise to the challenge of providing what the market will bear. The premise of the U.S. Goverment's counternarcotics efforts is that by interfering with the supply of illegal drugs entering the United States, and cutting into that supply, the laws of economics would dictate that prices would increase to a point where fewer people could and would purchase illegal substances. Toward that end, the U.S. military trains and equips the armed forces and law enforcement agencies of other countries to combat narcotics producers and traffickers, detects and monitors drug trafficking, participates in drug eradication programs and shares information with U.S. law enforcement entities and partner nations.[26] As of November 2011, DoD had active counternarcotics programs in the following 22 countries: Peru, Colombia, Afghanistan, Bolivia, Ecuador, Pakistan, Tajikistan, Turkmenistan, Uzbekistan, Azerbaijan, Kazakhstan, Kyrgyzstan, Armenia, Guatemala, Belize, Panama, Mexico, Dominican Republic, Guinea-Bissau, Senegal, El Salvador, and Honduras.[27]

More recently, the training of the Mexican Marines is one of several ways in which the U.S. military has quietly escalated its role in Mexico's drug war in the past three years since implementation of the Merida Initiative, part of a U.S. "whole of government" effort to support the Mexican government's fight against the cartels. Under the initiative,

the United States gave $900 million in assistance to Mexico from 2009 through 2011. It also shifted from a focus on equipping and funding the Mexicans, to training, thus enhancing partnership capabilities. The program has had numerous operational and tactical successes, with more than 30 senior cartel leaders having been arrested or killed, compared with one in the six years prior to Merida.[28] The long-term effects of arresting or killing cartel leaders appear negligible, however, as others rise up to replace them (see the "hydra effect" below) or a cartel splits and two leaders replace the one, as was the case with the Beltran Leyva organization.[29] The *New York Times* similarly explains that, "the violence has been fueled in part by the splintering of drug organizations under siege, which led to escalating rounds of bloody infighting over territory and criminal rackets."[30] Meanwhile, the drug related violence in Mexico goes on unabated.

According to Mexico's *Excelsior* newspaper, drug violence reportedly claimed 47,515 lives from December 2006, when President Felipe Calderon deployed thousands of troops against the cartels, through September 2011.[31] When that number of lost lives is divided by the number of corresponding months and days, an average of one person died every hour of every day during that period. When the data for the first nine months of 2011 is viewed separately, the rate of violence skyrocketed, with one person succumbing to drug violence every half-hour, or 48 killings per day.[32]

The rise of drug trafficking organizations in Mexico coincided with the U.S.' success in training Colombia to combat its drug cartels. The U.S.' Plan Colombia arguably contributed to Mexico's surge in violence by shifting Colombia's narcotics trafficking organizations and routes elsewhere. The plan unintentionally pushed transshipment routes into West Africa for cocaine destined for Europe and Africa, and up through Mexico for cocaine intended for North America, greatly strengthening and even giving rise to some of Mexico's more powerful cartels.[33] An *Associated Press* report in 2009 observed, "The United States has spent hundreds of millions of dollars to help Colombia dismantle its major cartels but may have actually helped the Mexicans gain traction in South America in the process."[34] In fact, NSD 18 which outlined the International Counternarcotics Strategy in 1989, warned

that successful counternarcotics efforts in Colombia could lead to a "shifting of trafficking organizations and infrastructure to locations in Bolivia and Peru…without expanded efforts in those two countries."[35] The directive therefore proposed counterdrug assistance to all three countries, but did not envision the subsequent shifting of trafficking patterns beyond the Andean countries.

The U.S. Goverment effort has been predicated on the belief that a successful counternarcotics strategy should attack the supply side of the problem. A drop in supply would lead to higher narcotics prices which would drive many users out of the market. However, according to *Drug War Politics: The Price of Denial*, "the attempt to suppress the drug trade through a war on supply generates two self-defeating effects – the profit paradox and the hydra effect – which together doom the effort."[36] The profit paradox is created by cartels' raising prices to compensate for depleted supply. The higher prices mean higher profits, encouraging more suppliers to enter the market. More suppliers maintain or even raise the supply of drugs available, countering any pressure to raise prices. Therefore, law enforcement and military efforts to attack the supply side of the illicit narcotics problem has no noticeable effect on the price of product. The hydra effect simply asserts that if one source of an illegal drug is shut down another will take its place.[37] The same concept in counterterrorism is often referred to as "whack a mole."[38] The result of the military's supply-side involvement is summarized by *The Oberver's* Ed Vulliamy:

> *The war in the so-called "producing" countries has ravaged Colombia, is currently tearing Mexico apart, and again threatens Afghanistan, Central America, Bolivia, Peru and Venezuela. In places such as West Africa, the war is creating "narco states" that have become effective puppets of the mafia cartels the war has spawned.*[39]

**Metrics**

One factor significantly complicating assessing DoD's progress, and impeding progress in the counternarcotics effort is the lack of a coherent system within the department to measure its effectiveness in combating illicit drug production and trafficking. A 2010 report by

the Government Accountability Office (GAO) states that measuring performance is essential in providing managers with a "basis for making fact-based decisions, but that DoD's system is inadequate and the results not utilized to improve management and oversight of the system."[40]

As cited above, the U.S. Goverment position has been that been that success could be somehow measured by a reduction in the amount of illegal drugs entering the United States, and a subsequent rise in the price of those drugs as a result of the reduced supply, in accordance with the basic tenets of supply and demand. The 2011 *Department of Defense Counternarcotics and Global Threats Strategy* dedicates a page to the discussion of a need for "metrics" regarding the development of performance indicators to, "observe progress and measure actual versus expected results."[41] Such wording is too vague to be of significant practical value in assessing accomplishments to date. The strategy identifies the importance of using performance metrics and states that the Deputy Assistant Secretary of Defense for Counternarcotics and Global Threats (DASD CN&GT), "with inputs from stakeholders, *will issue* guidance and instructions for formulating and reporting on performance metrics that reflect theater-level operational plan CN&GT objectives and activities."[42] In short, metrics guidance is forthcoming, some twenty-three years into the directed effort. When asked what metrics the DASD uses to judge the effectiveness of its counternarcotics programs, a senior DoD official observed that if using the decreased quantity and increased prices of illicit narcotics in the United States as measures of effectiveness, the military's counternarcotics efforts could not be deemed successful.[43] The official did, however, cite some specific cases of DoD support resulting in major seizures. Nonetheless, despite more than two decades of concerted DoD effort, U.S. law enforcement agencies have witnessed no significant drop in the supply nor rise in price of illegal narcotics entering the United States.[44] According to the UN's *2011 World Drug Report,* the retail (street) price of heroin in the United States in (adjusted for inflation) 2009 dollars dropped from $231 per gram in 1990 to $157 per gram in 2009, and when further adjusted for purity as well as inflation, dropped significantly further from $1,051 per gram in 1990 to less than half, at $491 in 2009.[45] Some of that price drop could be attributable to the relatively

stable demand for heroin in the United States; however, if rising prices for illicit drugs is considered a measure of the effectiveness of U.S. counternarcotics efforts, we appear to be falling short.

The UN estimates that the United States comprises the single largest cocaine market in the world, accounting for the consumption of some 157 metric tons of the 440 metric tons available for consumption worldwide in 2009. That data point belies the fact that as compared with estimates for 1989, U.S. cocaine consumption has dropped some 70%.[46]

Whether the drop in domestic consumption is the result of changing preferences or successes in prevention is unclear; but there has been no corresponding increase in interdiction successes. In fact, interdictions along the southwest border area dropped from 27,361 kilograms of cocaine in FY2006 to 17,830 kilograms in FY2010, and from 69,561 across the entire United States in FY2006 down to 44.063 kilograms in FY2010, as demonstrated by the below chart.[47] During the same period, seizures of methamphetamines and marijuana increased significantly.

Statistics can raise more questions than they answer. There appears to be little data identifying or quantifying the role played by DoD in LEA tactical successes in intercepting illegal narcotics along the border. One may point to kilograms of narcotic X seized in a given year (as shown above); but DoD's role in those interdictions is unclear since DoD is not authorized to conduct U.S. interdictions, only to support them.[48] DoD assists LEAs on our borders primarily with reconnaissance assets, "boots on the ground" (usually National Guard personnel under Title 32 authority) surveillance support, transportation assistance and information sharing. The *Army Times* reports that in fiscal year 2011, "apprehensions on the Southwestern border fell to 340,252, one-fifth the level reported in fiscal [year] 2000….In Arizona, Border Patrol apprehensions fell to 129,118, the lowest number in 17 years."[49] A significant number these apprehensions were almost certainly drug-related; however, data breaking out the types of apprehensions conducted is not readily available. Without useful metrics, one is hard-pressed to demonstrate a consistent track record of DoD results in the counterdrug mission. Only the dollar cost of those efforts is readily quantifiable.

## TOTAL U.S. SEIZURES BY DRUG IN KILOGRAMS*

| REGION | FY2006 | FY2007 | FY2008 | FY2009 | FY2010 |
|---|---|---|---|---|---|
| **Cocaine** | | | | | |
| Southwest Border Area* | 27,361 | 24,780 | 17,459 | 18,737 | 17,830 |
| Northern Border | 2 | <1 | <1 | 18 | 23 |
| Rest of U.S. | 42,198 | 33,177 | 28,547 | 29,629 | 26,210 |
| Total U.S. | 69,561 | 57,957 | 46,006 | 48,384 | 44,063 |
| **Methamphetamine** | | | | | |
| Southwest Border Area | 2,706 | 2,128 | 2,221 | 3,278 | 4,486 |
| Northern Border | <1 | 1 | 135 | 0 | 11 |
| Rest of U.S. | 2,872 | 3,100 | 3,696 | 3,323 | 4,202 |
| Total U.S. | 5,578 | 5,229 | 6,052 | 6,601 | 8,699 |
| **Heroin** | | | | | |
| Southwest Border Area | 449 | 358 | 496 | 737 | 905 |
| Northern Border | 5 | <1 | 0 | 28 | 20 |
| Rest of U.S. | 1,719 | 1,631 | 1,404 | 1,485 | 1,637 |
| Total U.S. | 2,173 | 1,989 | 1,900 | 2,250 | 2,562 |
| **Marijuana** | | | | | |
| Southwest Border Area | 1,046,419 | 1,459,162 | 1,242,758 | 1,730,344 | 1,545,138 |
| Northern Border | 5,455 | 3,084 | 2,369 | 3,784 | 2,194 |
| Rest of U.S. | 237,330 | 263,904 | 227,948 | 241,000 | 262,164 |
| Total U.S. | 1,289,204 | 1,726,150 | 1,473,075 | 1,975,128 | 1,809,496 |

**Source: National Drug Threat Assessment 2011**[50]

***Includes seizures made by federal, state and local law enforcement officers along and within 150 miles of the border.**

**Figure 1.**

| FY2005 | FY2006 | FY2007 | FY2008 |
|---|---|---|---|
| $1,147.8 | $936.1 | $1,137 | $1,314.8 |
| **FY2009** | **FY2010** | **FY2011** | |
| $1,397.2 | $1,558.3 | $1,689.2[51] | |

**Figure 2. DoD Counternarcotics Funding (in millions of U.S. dollars)**

## Nature of the Threat

The flow of illegal drugs into the United States is both a legal-criminal and a social welfare concern; but does it rise to the level of a national security threat that merits military involvement under the umbrella of homeland defense? Even the highest policy-making levels of the U.S. Government seem to disagree. The *2010 National Security Strategy* warns, "Transnational criminal threats and illicit trafficking networks continue to expand dramatically in size, scope, and influence – posing significant national security challenges for the United States and our partner countries."[52] One could argue over the semantics of what constitutes a "national security challenge" versus a "national security threat;" but suffice it say, a "challenge" usually does not rise to the level of a "threat." Meanwhile, among the five overarching policy objectives identified in the U.S. *Strategy to Combat Transnational Organized Crime* (TOC) is:

> *Defeat transnational criminal networks that pose the greatest threat to national security.…Further, we will seek to prevent collaboration between criminal and terrorist networks and deprive them of their critical resources and infrastructure, such as funding, logistical support for transportation, staging, procurement, safe havens for illicit activities, and the facilitation of services and materiel, which could include WMD material.*[53]

Thus, the Strategy to Combat TOC states that transnational criminal networks may post a threat to national security. Meanwhile, the new *National Defense Strategy* (NDS), released in January 2012, does not even mention DoD's counternarcotics mission.[54] Further, it defines the U.S. military's role in homeland defense more narrowly than the U.S. Goverment and DoD have in the past, explaining, "U.S. forces

will continue to defend U.S. territory from direct attack by state and non-state actors."[55] The activities of drug trafficking organizations would hardly constitute a "direct attack" on U.S. territory, probably not what was envisioned by the drafters of the NDS. The NDS also redefines Homeland Defense and Defense Support to Civil Authorities in way that precludes addressing counternarcotics.[56] The President's 2012 State of the Union address similarly defined homeland defense as responding to attacks directed against the United States.[57]

In his prepared statement for the Senate Select Committee on Intelligence on January 31, 2012, the Director of National Intelligence, James Clapper, did not identify drug cartels or cartel violence in Mexico as a serious national security concern. Rather, he asserted that although, "Mexican cartels have a presence in the United States…we are not likely to see the level of violence that is plaguing Mexico spill across the U.S. border."[58] He also stated that, "the factor that drives most of the bloodshed in Mexico – competition for control of trafficking routes and networks of corrupt officials – is not widely applicable to the small retail drug trafficking activities on the U.S. side of the border."[59]

A Mexican commentator recently observed that the Mexican government's efforts to combat the cartels with military force, with support of the United States, only leads to more violence. He observed with some irony that the United States then worries about the possible cross-border seepage of the resulting violence it does not realize it has caused.[60] The violence associated with Mexican narcotics trafficking organizations remains almost exclusively within Mexico's borders, despite some overflow into the U.S.' southern border states. Drug-related violence within the United States falls largely in the domain of drug dealers, drug users and gang members, i.e., criminals, and as such, does not easily fall into the category of a national security threat.

The term "narcoterrorism" was coined ostensibly to demonstrate the nexus between narcotics trafficking organizations and terrorist organizations. By effectively identifying cartels as terrorist organizations "by another name," one can more easily justify claims that that they threaten U.S. national security interests. The term was likely coined to sound the national security alarm and obtain counterterrorism funding

in the continuing effort to combat the drug cartels, according to one senior Defense official.[61]

Further, referring to the business of cartels as constituting narcoterrorism, and formally identifying them as terrorist organizations would allow the U.S. Goverment a range of strategy and policy options and military tools that would otherwise not be available in combating them.[62] While both drug cartels and terrorist organizations use violence as a tactic to further their goals, they are different. Cartels are criminal enterprises whose leaders are motivated by profit. "Mexican and Colombian drug trafficking organizations earn between $18 billion and $39 billion a year."[63] Terrorist organizations have a political, or perhaps, even a social or religious goal. Former Mexican Attorney General Arturo Chavez repeatedly maintained that the narcotics cartels were not terrorist organizations. He observed that their violence was not intended to weaken the state, and that their motivation was economic, not ideological.[64] Also referring to the Mexican cartels, Dr. Paul Kan observes that:

> *Even violent acts by the cartels and gangs directed at government targets are meant as a signal for the government to retreat from its confrontational stance; they are designed to intimidate the government rather than to serve as a political statement… Terror and insurgent groups try to sway constituents with violence; cartels try to satisfy clients by circumventing or undermining the state."*[65]

Some members of the U.S. Congress, most notably those from the southwestern border states, have even suggested that Mexican cartels be identified as terrorist organizations and placed on the State Department's Foreign Terrorist Organizations List.[66] In support of a Republican bill to do just that, the Enhanced Border Security Act (HR 3401), Representative Michael Paul of Texas stated: "I believe that the drug cartels are acting within the federal definition of terrorism, which basically says to intimidate a civilian population or government by extortion, kidnapping or assassination. That is precisely, precisely what the drug cartels do. They extort."[67] Representative Eliot Engel disagreed with the characterization, plainly stating that Mexico is experiencing "narco-crime" and not terrorism, observing:

> *If I were living in a place where gun battles were leaving scores of people dead and previously safe streets were now hideouts for thugs and criminals, I would feel a sense of terror, too….[however] There is a difference between acts which can cause terror and terrorist acts….The narco-criminals in Mexico have no political aims, they are brutal outlaws who want money, but they don't want to throw out the government and take over."*[68]

Representative Michael McCaul of Texas points to last year's failed plot by Iranian government agents who believed they were working with a Mexican Los Zetas cartel associate to assassinate the Saudi Ambassador to the United States, to demonstrate alleged ties between drug cartels and terrorism.[69] The so-called cartel member was actually a paid informant of the DEA.[70] The cartel did not support the Iranian effort. According to Robert Valencia, a Research Fellow with the Council on Hemispheric Affairs:

> *[H]aving the U.S. State Department label the Zetas a terrorist organization solves nothing. The addition of the Zetas to that list won't stop cartels from running the drug market nor from establishing international ties. Furthermore, unlike terrorist organizations such as al-Qaida, these cartels' goals do not include attacking the U.S. The Zeta cartel's motive is money, not ideology.*[71]

The experience of Colombia is very different from that of Mexico. In Colombia, insurgent organizations such as the Revolutionary Armed Forces of Colombia (FARC), National Liberation Army (ELN), and the now disbanded Democratic Alliance (M-19), routinely funded their operations through activities including narcotics trafficking. In the 1980s the lines dividing the activities of the insurgent organizations and the cartels were sometimes blurred, as in the 1985 M-19 and drug cartel-coordinated attack on the Palace of Justice in Bogota, in which 115 people were killed, including 11 Supreme Court justices.[72] A 2012 State Department report on Colombia explains that since the early 1980s, "left-wing guerrillas" have conducted "terrorist and drug-trafficking activities," while the drug cartels have continued their violence.[73] Thus, even though Colombia's insurgents have used trafficking to line their coffers and fund their operations, they are not to be confused with narcotics cartels. Also, cartel related violence has

diminished since Colombian security forces killed notorious Medellin cartel leader Pablo Escobar in 1993.[74]

There undeniably is an occasional confluence of interests between drug cartels and terrorist organizations;[75] however, such a confluence does not make cartels terrorist organizations, nor does an occasional linkage confirm the existence of so-called narcoterrorism. Research on this connection is episodic and data is not readily available. Some disincentives for cartels and terrorist organizations partnering are:

> *…increased attention from government authorities; fear of compromising internal security; ideological resistance to illegal endeavors, such as drug trafficking, kidnapping and fraud; and sufficient sources of non-criminal funding from charities, large private donors, licit businesses and state sponsors.*[76]

**Recommendations and Conclusion**

The U.S. Government should focus on attacking the "demand" side of the illicit narcotics problem in the United States. A fundamental principle of economics is that demand drives supply; therefore, demand for illicit drugs drives narcotics production and trafficking. Mexican President Felipe Calderón has repeatedly asked the United States to do more to address the demand side of the drug trade, as well as the flow of weapons from the United States to the cartels.[77] Much of the cartels' market is in the United States. Even the *National Drug Control Strategy* acknowledges that demand within our borders contributes significantly to the illicit drug trade:

> *We must begin our efforts to disrupt TOC [transnational organized crime] by looking inward and acknowledging the causes that emanate from within our own borders to fuel and empower TOC. The demand for illegal drugs within the United States fuels a significant share of the global drug trade, which is a primary funding source for TOC networks and a key source of revenue for some terrorist and insurgent networks.*[78]

Illicit drugs endanger the public health and safety of our citizens. Resources should be directed toward public health programs to counter addiction and educational programs to prevent it. The *National Drug*

*Control Strategy* outlines a viable plan for addressing the U.S. demand for illegal drugs. The specific recommendations follow:

- Strengthen efforts to prevent drug use in our communities
- Seek early intervention opportunities in health care
- Integrate treatment for substance use disorders into mainstream health care and expand support for recovery
- Break the cycle of drug use, crime, delinquency, and incarceration
- Disrupt domestic drug trafficking and production
- Strengthen international partnerships
- Improve information systems for analysis, assessment and local management[79]

The *National Drug Control Strategy* further states that "we must also stop the illicit flow from the United States of weapons and criminal proceeds that empower TOC networks."[80] It emphasizes additional resources and capabilities for the integrated Border Enforcement Security Task Forces on our southern border "to investigate the organizations involved in cross-border crimes."[81] What is perhaps the most telling aspect of the *Drug Control Strategy* is that the DoD is mentioned only once in the entire document.

"Only the Defense Department is able to do that," is an oft-used excuse for other U.S. Government departments relying on DoD resources, rather than those departments obtaining and maintaining their own capabilities. The DEA and the FBI should pursue adequate funding from Congress to fully support their missions, to alleviate and end their dependence on DoD for transportation, reconnaissance, and other support functions. Congress should also adequately fund the Department of Homeland Security and LEAs to control our borders. They must have the technical capabilities to conduct successful intelligence, surveillance and reconnaissance missions and have sufficient funding to hire more personnel to apprehend persons entering the United States illegally, especially since they could be trafficking in illegal substance or be the victims of human trafficking. LEA intelligence units should be adequately resourced to monitor and

stop the flow of weapons from the United States to Latin American cartels, and to track cartel finances where possible.

Rather than compelling DoD to continue or become further immersed in a fight it has not been able to win, perhaps the time has come to reallocate those resources to law enforcement agencies and allow the department to reprioritize its core missions, especially given today's budget cuts and associated downsizing. Being good stewards of taxpayers' money demands that DoD dedicate its precious resources to where it can best accomplish mission. At a time when the military is in the midst of an effort to rearm, train and refit itself to perform its key missions, and with dramatically reduced resources, those programs showing the least success and the least relevance to core missions should at least be closely scrutinized.

On January 26, 2012, DoD issued its plan to cut more than $259 billion during FY13-17.[82] Since the Congressional Super Committee failed to reach the hoped for compromise on U.S. Government spending cuts, DoD is obligated to prepare for even deeper cuts than previously projected, and perhaps, sequestration. At a time when the Department is refocusing on its key mission areas and considering dropping non-critical missions, this author submits that the time to reconsider the continued viability of DoD's counternarcotics mission has come. The less than two billion dollar DoD counternarcotics budget is a small percentage of the Department's overall budget, reflecting its low level of significance vis-à-vis the overall DoD mission. In time of declining budgets the Defense Department should not be performing ancillary missions, and should instead focus on key threats to best protect our national security.

The new *National Defense Strategy* identifies the key military missions for which DoD must prepare. Specifically, those missions are: counterterrorism and irregular warfare, to deter and defeat aggression, power projection, counter weapons of mass destruction, operate effectively in space and cyberspace, maintain the nuclear deterrent, defend the homeland the provide support to civil authorities, provide a stabilizing presence (abroad), conduct stability and counterinsurgency operations, conduct humanitarian disaster relief and other operations.[83] Let the U.S. military conduct the missions it is best trained and equipped

to perform – those identified above. The DoD should not be treated as a contractor with services available for hire to other departments. It should perform missions that it is uniquely capable of performing, not additional missions it is *able* to perform or support. DoD's resources are greatly constrained. The Department needs to be prepared for the next 9/11 and other crises. It does not need to be performing ancillary missions, especially those for which there has been so little return on more than two decades of investment.

Should analysts one day identify a clear sustained link between drug cartels and terrorist organizations, the U.S. Government would need to determine how to best address that threat, and if it constituted a national security threat to the United States. Obviously if such a nexus appeared to threaten a government deemed hostile to U.S. interests, Washington would probably choose to monitor the situation from afar. Also, if the nexus proved to be a one-time localized linkage the U.S.' concern would be less than if such a nexus seemed to be a model that other criminal and terrorist organizations had reason to follow. If cartels and terrorist organizations came together in a way deemed a serious credible threat to U.S. national security interests, the services of the U.S. Armed Forces could and should be called upon to meet it. Even then, the military should only be called upon if given a clear strategy for success, achievable end states, and an exit strategy.


U.S. ARMY WAR COLLEGE
Prudens
Futuri
Carlisle Barracks, PA

# 21ST Century Cyber Security: Legal Authorities and Requirements

**Lieutenant Colonel Charles W. Douglass**
United States Air Force

America is at a strategic crossroads. The emergence of cyberspace as warfighting domain has brought with it new dimensions of national power. Unless fully understood by national security professionals, this new domain may constitute the ultimate "Achilles Heel" in U.S. security. The United States could be subdued by a cyber attack for which we are not currently prepared. The nexus between established Department of Defense (DoD) authorities, warfighting doctrine, and evolving cyber policy requires a greater focus on how to fight and win in cyberspace and less focus on how to apply cyber fundamentals to a two-dimensional war of geography. This paper challenges the assumptions that underpin current DoD organization and readiness to meet the emerging – and very real – cyber threat. Failure to address cyberspace as a wholly new domain, unencumbered by traditional concepts of geographic boundaries and the legal precedents which govern the application of conventional military force, will ultimately compromise the security of our nation.

In order to grasp the complexity of the artificial restraints placed on federal agencies' ability to meet cyber threats, one need look no further than United States Code (U.S.C).[1] U.S.C. is "the codification by subject matter of the general and permanent laws of the United States based on what is printed in the Statutes at Large."[2]

Of the 50 subject matter titles, only 23 have been entered into statutory law. However, U.S. legal authorities for operating in cyberspace (covering everything from appropriations to intelligence systems to warfare to law enforcement) are mentioned either implicitly or explicitly in 10 of the 23 Codes (not counting Statutes at Large or Supplemental issuances).[3] Further complicating this issue is the dysfunctional series of so-called lead agency responsibilities. For example, the Department of Homeland Security (DHS) is the lead federal agency for cyber

policy and management, yet it has no direct authority over DoD's cyber operations.[4] Specifically, no single federal department or agency has been granted directive authority to establish a uniform standard of system accreditation, hardware or software interoperability mandates, or individual user access protocols. The current autonomy of each federal department to handle these critical issues presents a clear threat to the U.S. government's operation in and through cyberspace.

## The Cyber Environment

Cyberspace is a man-made domain. In this respect, it is unique among the other four warfighting domains.[5] However, in matters of governmental regulations and national security, cyberspace is very similar to the maritime and air domains in four key ways:

- The preponderance of activity occurring in cyberspace is commercial (or private)
- Private industry owns and creates the ways and means to access the domain
- Codification of international conventions originates from the customs and operating procedures of the private and commercial sectors operating in the domain
- Activity occurring through the domain may involve "transit" through architecture and systems residing in sovereign nations who may not have the knowledge or capability to identify, restrict or interdict illicit or nefarious actions

In light of these commonalities, one would expect formation of a federal regulatory body to govern the Cyber Domain comparable to those that exist for governing the maritime and air domains (e.g., the Federal Aviation Administration or the Federal Maritime Administration). Because cyberspace is a man-made domain, a variety of regulatory agencies lay claim to governing functions within it: the Federal Communications Commission, the National Security Agency, DHS, and the Department of Commerce, to name a few. Additionally, when the threat of a cyber attack exists, an equally confusing array of defense, exploitative, and forensic authorities must be engaged to defend against such an attack. Was the attack directed against

intellectual property or military secrets? Was the attack conducted by a state or a non-state actor? Can we ascertain who is responsible for the attack quickly enough to retaliate? What constitutes an act of war in cyberspace? And, in the event of an act of war, who has the authority to direct retaliatory (perhaps anticipatory) actions in response to a cyber threat? These are just a few of the questions that arise concerning the U.S. ability to anticipate and counter a dynamic cyber threat.

Complicating the cyber environment is the much-discussed low "cost of admission" to operate in cyberspace. Unlike the significant economic and technical/industrial capabilities and capacities required to become a space-faring nation, the national investment to have credible and respected cyber power is a bargain. For example, consider the reputed case of Russia's use of "botnets"[6] during the 2008 conflict in Georgia – as well as the assessed technical competence of Russian cyber intrusions. The damage inflicted by cyber warfare can be measured in multiple dimensions; lost intellectual property, state secrets, or "kinetic-like" effects on infrastructure. In comparison to an air strike or naval blockade or spy ring, the attractiveness of an aggressive, offensive cyber campaign is abundantly clear. But an army of competent cyber warriors cannot be quickly assembled by recruiting a ghost army of angry nerds huddled in poorly lit basements or drafty garages across Eastern Europe. State-level cyber warfare capabilities are expensive in real terms. However, investments in cyber capabilities are frequently measured in millions of dollars vice the billions of dollars it takes to build and sustain modern, conventional military capabilities.

## The Case of Estonia

In April and May of 2007 Estonia experienced a wide-ranging, three-week cyber attack on virtually every one of its major governmental information systems by a sophisticated – and experienced – enemy.[7] While Russia has consistently denied responsibility for this distributed denial-of-service barrage attack, it did appear to be the concluding event of a political dispute between Russia and Estonia. This multi-dimensional dispute escalated over the relocation of the Bronze Soldier monument in Tallinn that commemorates Soviet casualties in the Great Patriotic War (World War II).[8]

The speed, effectiveness, and depth of the attacks were staggering, paralyzing the Estonian executive branch of government, all of the ministries, all of the state's political parties, major banks, parliament, half of the news agencies, and a variety of telecommunication companies. As Europe's most 'netted' country with the highest wireless connectivity rate per capita (viewed as a basic human right by the Estonian government), all Estonians immediately felt impact of this devastating attack.[9]

Equally intriguing was the institutional hand-wringing at the European Union (EU) and NATO regarding not *what to do*, but simply *what to say* about the attacks. Political considerations aside (Poland, for example, stymied EU efforts to issue a unanimous statement decrying the attack as an act of cyber warfare), this incident and the subsequent controversy within NATO revealed significant implications for Article V of the North Atlantic Treaty. This article specifies that an attack on one member is an attack on all, yet it reserves individual national responses to the discretion of the individual member governments. This is the fundamental question: "If Estonia actually came under cyber attack, did the cooperative self-defense provision in Article V come into play?" Article V specifically states that "an armed attack against any ally" requires a response by the NATO members.[10] But, was Estonia subjected to an *armed* attack? Article IV certainly seemed to apply to the situation: "The Parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened."[11] The central problem was not just the cyber attack, but whether under the North Atlantic Treaty a cyber attack could be considered an attack in the traditional sense of the word.

Ultimately, NATO did nothing to assist Estonia – possibly because the attack caught NATO members off-guard. Although NATO military headquarters has erected a reasonable network defense architecture, many NATO members do not have any such system in place for their national governments. The attack highlighted a critical vulnerability in the 21st century NATO model: operations in cyberspace necessitate a review of defensive capabilities across all member nations. This review should include the cyber networks of civil governance, private

and commercial critical infrastructure, and military cyber systems. Following the Estonian ordeal, a flurry of legal discussions, high level conferences and new policies signaled a watershed in cyber warfare doctrine and theory on both sides of the Atlantic. In NATO, a "digital agenda" was established to set common priorities for the EU digital marketplace and European information and communication technology education.[12] Specific definitions of cyber war and cyber-terrorism were integrated into the NATO lexicon (largely framed by Ahmad Kamal's work, *The Law of CyberSpace*). And NATO's tenth center of excellence was established for Cooperative Cyber Defense (CCDCOE) at, of all places, Tallinn.[13] Perhaps the most important (if underplayed) outcome was CCDCOE's recognition of the need for collaboration among government, military, private and commercial institutions for defense-in-depth of dual-use information technologies.

Across the Atlantic, the U.S. government has been besieged by internal cyber issues as well. Immediately prior to the Estonian attack, the U.S. Air Force publicly acknowledged a deep intrusion by a foreign entity into contractor-held computer systems supporting the Joint Strike Fighter program. In the months following the Estonian attack, the DoD was subjected to a malicious code propagation (labeled as "agent.btz") through U.S. Central Command. In response, DoD engaged all of the Department's cyber resources (code named Operation BUCKSHOT YANKEE) to address the problem.[14] Most experts concur that the agent.btz malicious code was part of a Russian attack.[15] However, attacks known to have originated from within China have exfiltrated terabytes of information. In fact, the Munk Centre for International Studies, a Toronto-based think tank, estimates China has conducted successful cyber espionage intrusions in 103 countries employing *GhostNet* architecture in a complex strategy to "win the information war."[16]

As the DoD grappled with these major cyber espionage events, DHS was designated the lead federal agency for protection of critical infrastructure, including cyberspace. DHS was assigned this critical task despite growing evidence that Russia and China had clearly and deliberately organized cyber forces to conduct state-on-state information warfare campaigns. Designating DHS as the lead, while reserving specific authorities for the military has generated

unsettling uncertainty regarding the Administration's policy on cyber attacks resulting in the following question: "Are these attacks purely law enforcement issue or a national security issue that requires an integrated response posture unidentified in current policy?" The situation has not been clarified appreciably since the Estonian attack. In a report to Congress in November 2011, the Office of National Counterintelligence stated bluntly:

> *Billions of dollars of trade secrets, technology and intellectual property are being siphoned each year from the computer systems of U.S. government agencies, corporations and research institutions to benefit the economies of China and other countries…*[17]

The lessons NATO seems to have learned following Estonia's experience of a major cyber attack appear to have been noticed – but ignored – by the U.S. government. The implications of a major cyber attack on the economic and information systems of the U.S. commercial sector during a simultaneous attack across the federal government are arguably catastrophic.

## Organizing for Cyber Warfare

The 2010 Joint Operating Environment (JOE), the 2011 International Strategy for Cyberspace, and the 2011 Department of Defense Strategy for Operating in Cyberspace all acknowledge that the DoD must consider all operations in cyberspace to have implications for the security of all elements of national power – through the full depth, breadth, and scope of governmental, military, private, and corporate infrastructure.[18,19] The current military mission in cyberspace is not fully responsive to the President's guidance to maintain "an **inherent right to self-defense** that may be triggered by **certain aggressive acts** in cyberspace" (emphasis in original).[20] Across the federal agencies, the Departments of State, Justice, and Commerce have responsibility for the preponderance of U.S. involvement in global cyber security and governance agreements, entities, and efforts. However, the preponderance of U.S. cyber warfare investments focus on military issues and intelligence collection.[21]

Despite the exploitation of cyberspace as a viable commercial and informational domain for more than 30 years, the DoD has struggled to integrate its role in this domain with the roles of the broader interagency. Although the DoD requirement to classify systems and capabilities tied to intelligence collection and cyber defense/attack methodologies is both understandable and reasonable as justification for keeping the other departments and agencies at arm's length, it creates a two-fold problem. First, it fosters a pervasive attitude that a man-made domain is simply a collection of operating systems and their interfaces (e.g., hardware, software, data transmission, and human operators). Hence, a set-piece process of firewalls, accreditation, and technical improvement provides sufficient defense in the Cyber Domain. This view essentially degrades a complex warfighting domain to the level of rudimentary warfare akin to siege craft and castles. This mindset ignores the exceptionally complex nature of the cyber domain and its fluid environment in which military operations constitute only a small fraction of its activities.

Second, the military's current organizing construct for conducting cyber operations is misguided. This construct has evolved from each of the DoD's communications and intelligence "tribes." Each tribe has developed legacy capabilities and counter-capabilities largely independent of other tribes' efforts. While the United States was following this dysfunctional, suboptimal approach, its competitor nations with less restrained doctrinal views of the cyber domain wreaked havoc with the intellectual property of defense contractors and planted untold volumes of malicious code and spyware in U.S. defense information systems. These actors effectively shaped the cyber environment before the U.S. military realized it was, in effect, engaged in a "cyber war."

Vice Admiral Arthur Cebrowski, former head of the DoD's Office for Transformation, published several papers and articles through 2004 advancing an important conceptual point. Simply stated, his thesis was that "beyond the more rigid definitions of systems and enablers, cyberspace is a new strategic common." He described cyberspace as:

> *…the domain of information and cognition that includes the channels of mass media and finance. Like its conceptual predecessors,*

> *it is an international domain of trade and intercontinental communication. Increasingly, it can increase, sustain or diminish a nation's position of power in economic, diplomatic, or military terms.*[22]

Similar to the maritime and air domains, cyberspace is dominated by private investment, business innovation, and commercial use. But cyberspace is exponentially more pervasive than the maritime and air domains. Nonetheless, conceiving the implications of the cyber domain in terms of Sea Power Theory may prove useful. For example, a massive naval fleet patrolling the world's oceans – as Alfred T. Mahan advocated – may be far less effective than positioning several smaller naval elements to patrol potential hot-spots and to protect our trade routes as Julian Corbett articulated.[23] A cyber corollary would posit that providing defense-in-depth of only those nodes vital to the defense industrial base, while simultaneously providing for an exploitative and attack capability to be used only when necessary, may be the best course of action rather than a Mahanian "defend all, attack everything" mode of systems defense and "brute cyber force." This cyber strategy is arguably moot because the "cyber gates" have already been breached making it necessary for the federal government contend with enemies within as well as external threats. The fact that the enemy is "within the gates" also makes it necessary to integrate domestic law enforcement into the national cyber defense architecture.

Domestic law enforcement in cyberspace is complex. The Defense Cyber Crimes Center (DCCC) and its law enforcement agency liaisons are bound by law to orient and operate against only clearly defined, domestically based criminal attacks or acts. But state-sponsored espionage and attacks on the defense architecture remain Title 10 and Title 50 operations managed by Cyber Command's Service components and the National Security Agency (NSA). This construct requires an unrealistic level of coordination *in real time* to monitor and exploit an attack, and then develop Title 10 response options (when applicable and only if approved). This compartmentalization of authorities among commands and agencies is insufficient for post-attack forensics or for characterizing a transient attack when an attack lasts mere seconds. Similarly, law enforcement agencies must cede

monitoring responsibility of a cyber attack when Title 10 (Armed Service Secretary or Combatant Commander) or Title 50 (technical intelligence gathering) authorities are required. Overall, the current interagency construct is a confusing myriad of competing authorities. This uncoordinated diffusion of authority and responsibility hinders the federal capacity to operate offensively in cyberspace and cedes freedom of maneuver to an enemy.

The Corbett-like approach to cyber defense would also enable the government, military, private and commercial sectors to better coordinate and synchronize their activities, thereby enhancing DoD's intelligence and cyber superiority missions. This may require the commercial sector to subordinate some of its priorities to the economic, statutory – and even diplomatic – controls necessary to sustain national security within cyberspace, much as commercial aviation shares the skies with military flights. Unifying cyber defense under a single agency for coordination and control provides significant advantages for strengthening national cyber security, particularly given limited federal resources to meet the emerging threat and competing commercial and private interests.

**Assessing the Next Threat and Calculating Risk**

Nothing in this world is free. Certainly in a time of fiscal austerity for all federal departments and agencies, the need to evaluate priorities for allocating resources is even more essential. So, against what threat should the nation focus its scarce national resources? The problem is difficult to frame in clear terms. What does appear to be clear however is that the intellectual property of the United States is a key target that is currently under attack by organized cyber espionage. Additionally, the potential for a deliberate, state-on-state cyber attack is not just possible, but likely.

Regarding intellectual property, we must expand the working definitions of what is meant by the term. In an all encompassing sense, intellectual property should include the product of individual expression (such as music, art, poetry, architectural design, etc.) as well as the culmination of years of business expertise, research, and technological advances. What used to be viewed as a corporate secret – not necessarily the target of state-sponsored espionage – is now the principal target of

economic espionage through cyberspace. Steven Chabinsky, Deputy Assistant Director of the FBI's Cyber Division, provided candid – and eye-opening – commentary on this issue:

> *This is definitely the golden age of cyber espionage. Foreign states are stealing data left and right from private-sector companies, nonprofit organizations and government agencies.*[24]

A key problem is the seeming failure of U.S. national leadership to recognize cyber espionage as a form of information and economic warfare. The commercial sector produces new technologies and capabilities employed by the federal government – the government itself does not produce or design information technology.[25] If a competitor nation – like China or Russia – with a nationalized business model can acquire the trade secrets of these companies, they can compete in the market-place without having to develop the product through costly and time intensive research and innovation, making their product cheaper and comparable U.S. products more expensive. Worse, as the U.S. company fails to compete successfully, it may also fail as a viable business model. So, the U.S. technological advantage dissipates. In effect, the advantage has been stolen and then used against the United States. However, viewing this reality as a threat requires a cognitive strategic awareness which U.S. leaders seem to lack.

According to NSA Director, General Keith Alexander, in only two days a major American company recently lost one billion dollars worth of intellectual property developed over 20-plus years.[26] In many cases the victims can't place a precise value on the stolen information. In other cases, the cost is staggering: "$100 million worth of insecticide research from Dow Chemical; $400 million worth of chemical formulas from DuPont; and $600 million of proprietary data from Motorola."[27]

Beyond this economic threat is the very real potential of a state-sponsored attack on the United States – beyond the scope of that which occurred in Estonia. What would happen if a competitor nation decided that acquiring a credible cyber warfare capability was in its vital interest, and that the principal target for this capability was the United States? Unfortunately, this is not fiction but a developing reality.

In mid-December 2011, Iran announced investment of $1 billion in its defensive and offensive cyber warfare capabilities. At the same time, Univision aired a documentary of Venezuelan and Iranian diplomats receiving a briefing on future cyber attacks on the United States.[28] It is hard to evaluate the viability of Iranian offensive cyber capabilities. But it is not so difficult to estimate the formidable skills of Russian and Chinese experts with whom Iran has collaborated in recent years to develop cyber capabilities. Iran's interest in an offensive cyber weapon is as much a factor of prestige as revenge. However, revenge may be the key, given the case of the "Stuxnet" malicious code which propagated through the Iranian nuclear enrichment facilities at Natanz in 2010.[29] Interestingly, Iran did not immediately acknowledge the attack, although the malicious code destroyed a number of uranium enrichment centrifuges and industrial system controllers. Although this cyber attack is generally assumed to be an Israeli or Israeli-U.S. cyber attack, the source of the malicious code (as indicated by Russian-owned Kaspersky Labs) was untraceable.

> *Kaspersky Lab has not seen enough evidence to identify the attackers or the intended target but we can confirm that this is a one-of-a-kind, sophisticated malware attack backed by a well-funded, highly skilled attack team with intimate knowledge of SCADA technology. We believe this type of attack could only be conducted with nation-state support and backing.*[30]

Israel has established a precedent for taking military action against the nuclear capabilities of its adversarial neighbors. It is plausible that Stuxnet was the cyber equivalent of an air strike. Such a cyber attack may be an Israeli strategic choice: "Israel certainly has the ability to create Stuxnet…and there is little downside to such an attack, because it would be virtually impossible to prove who did it."[31] Interestingly, a cyber attack may have neutralized ground radar and anti-aircraft systems in Syria prior to the September 2007 Israeli Air Force strike on an alleged reactor site in Deir-ez-Zor during Operation ORCHARD.[32] Whether or not ORCHARD was a precursor to the Natanz/Stuxnet cyber attack, the damage to the Natanz facility was significant.[33] Indeed, it spread to several hundred personal computers and the associated Siemens-controlled industrial systems, including sub-components of

the Bushehr Reactor Facility. No matter who launched Stuxnet, the global community has received a clear message: Cyber warfare is now a viable tool in the national arsenal and may be employed with or without conventional military forces. Iran and its technical assistants in North Korea now have all the incentive and the technical know-how they will ever need to develop an offensive cyber warfare capability and employ it against the United States.

**Whole of Government Approach?**

U.S. Cyber Command was organized to provide a command and control element capable of synergizing the nation's defensive cyber operations and architectures with intelligence gathering (i.e., computer network exploitation) and attack options resident within the NSA in support of Geographic Combatant Commands, the Services, and Defense agencies. In short, Cyber Command was conceived as the clearing house for all cyber warfare activities for the joint community and to serve as the DoD interface with the interagency.

Arguably, Cyber Command does not yet have a sufficient track record to be assessed as adequate to perform its mission. However, the risk incurred with conducting *business as usual* given the steadily growing threat of cyber espionage and the implications of a major cyber attack, like that executed on Estonia in 2007, leaves little doubt that a "whole of government" approach is needed to protect the economic and political underpinnings of our country. The defense of our government, private, and corporate information and banking systems is at least equal in importance – possibly of greater importance – than protecting the military's cyber infrastructure.

One defense agency is specifically charged with the integration and standardization of the defensive and technical components of the DoD's cyber portfolio: the Defense Information Systems Agency (DISA). With its information technology portfolio easily eclipsing that of any other federal agency (measured in billions of dollars and employing nearly 170,000 dedicated communications, information and cyber personnel), the DoD has a surprisingly discordant array of cyber and network architectures.[34] DISA, one part of this corporate structure headed by the Deputy Assistant Secretary of Defense (DASD)

for Cyber, Identity, and Information Assurance, was to be enhanced by the addition of a new sub-Secretariat for Networks, Integration and Information (NII). DISA was initially planned to become part of U.S. Cyber Command's integrated span of control. This initiative would have unified defensive and interoperability standards under a single DASD by integrating the NII/DISA roles and missions to provide a unified approach to standardization across the DoD information technology portfolio. This effort to create a DoD-wide enterprise information technology strategy, possibly as a precursor to an interagency Federal Information Technology Sharing Directive, would have provided the catalyst needed to ensure unity of effort, a defendable baseline of software and hardware, and a governmental accreditation standard. However, in July 2011, in one of his final official acts, Secretary of Defense Robert Gates disapproved the DISA and Cyber Command merger. The NII office was then officially disbanded. Touted as an efficiency-in-government measure, this action has yet to prove efficient across the cyber defense portfolio in terms of interoperability, unity of acquisition (strategy and accreditation), or oversight under a single DASD or unified/sub-unified Commander. The most recent National Defense Authorization Act seems to direct a DoD information technology strategy modeled on commercial "cloud" servers. Its specific language countermands DISA's directive to manage a central common DoD server.[35]

In view of the seeming inability of DoD to formulate a coherent strategy to fulfill Title 10 and Title 50 cyber requirements – as balanced against the information technology enterprise – no interagency proposal has yet been advanced to address the nation's cyber vulnerabilities. Currently, responsibilities for the nation's cyber defense reside in certain legal authorizations and diverse direction from various federal agencies that make up a loose interagency architecture to manage issues of cost-sharing, standardization, and protocols of cyber defense. The benefit of a truly consolidated and defendable federal cyber portfolio appears to remain a goal – but, not at the expense of each department's autonomy. If a severe external catalyst is required to achieve such integration, the cost of such an attack may be far too expensive for our national security to bear. The reality of such a threat demands a fresh review of legal authorities and organizational constructs.

**Recommendations**

The cyber policy review directed by the President suggests three possible options to address the perceived disconnect between U.S. Code cyber authorities and current federal agency authorities.[36] The most effective solution must balance three imperatives to:

- Measurably improve national cyber security by consolidating necessary authorities in order to enhance interagency capacity to operate in cyberspace
- Integrate allied and commercial cyber efforts
- Deny adversaries freedom to act in cyberspace

One option that satisfies these three imperatives is to continue with U.S. Cyber Command as a sub-unified functional command with operational authority over NSA and Service Title 10 cyber warfare capabilities. Under this option, the security classification and controls necessary to conduct Title 50 operations would be preserved, but Title 10 authorities would be separated from Title 18 to preclude the appearance of a "digital posse-comitatus" as interpreted through 18 U.S.C. subsection 1385. Specifically, the requirement to conduct intelligence operations in cyberspace would be sustained, but the warfighting and law enforcement elements – and their appropriate legal statutes – would remain separated. This approach would support current U.S. policy to not militarize cyberspace. However, the opportunity costs with such a minimalist approach may be unacceptably high given our current inability to uniformly respond to cyber threats which are currently addressed by more than one set of U.S.C. authorities. In effect, the current approach is cumbersome and diffuse. It fosters an environment in which the attacker is the only fluid player. If this option is implemented, interagency efforts in cyberspace would remain as they are for law enforcement and for commercial and international players. Further, Cyber Command as a military-only solution retains the risk of sustaining a functional seam between the attacker and the Title 10/18 exercising authorities. Cyber Command may continue to identify and disclose vulnerabilities throughout U.S. networks.

A second option would segregate authorities that employ cyber capabilities in a centralized control/decentralized execution scheme

akin to the current employment of airpower. This option entails two key requirements. First, consistent with Presidential guidance, the DoD must meet interoperability goals by establishing a single agency responsible for all hardware, software, and transmission accreditation as a federal standard. Second, this agency must be empowered with the preponderance of defensive capability and exercise institutional control over all federal system firewalls, authentication and access standards, and security classification/encryption baselines across the U.S. government. This option would advantageously impose a stable process to address the majority of vulnerabilities across the federal information system architecture. However, if this agency lacks the authority to compel other federal agencies and departments to comply with its regulations, it may not fulfill its mission. This risk can be mitigated only if funding for information technology and cyber systems is also centralized. Without a compulsory mechanism, it could not effectively accredit the security of the government's operating systems. To succeed, this option must address how different agencies with disparate U.S.C. authorities can operate collaboratively within cyberspace in a unified effort. Lacking such provisions, this option would not resolve the core problem. Even so, it would improve the nation's cyber defense.

Despite failing to address the issue of a single entity prosecuting cyber crimes and threats, this option remains attractive from the perspective of a standardized network defense and DoD's autonomy. It would likely be the most palatable option in political terms. Federal agencies and departments could maintain their autonomy to develop and field software, systems and operating environments to meet their mission requirement while enabling a single agency to standardize a basic level of security, certification, and incident response capabilities.

A third option would transform U.S. Cyber Command from a sub-unified command to the headquarters of a Joint Interagency Task Force (JIATF). As a JIATF, the DCCC and NSA cyber elements would form the core of a netted operational command that would consolidate cyber control elements from other federal agencies. Thus a single commander at the JIATF would inherit authorities delegated by all of the component federal partners (U.S.C. 6, 10, 18, etc.), but would not assume a "force provider" role. A JIATF could operate across federal

agency authorities (U.S. Code) as a single command responsible for coordinating and conducting law enforcement, network defense, cyber security, intelligence exploitation, and cyber warfare. For addressing system accreditation and interoperability, the original plan to place DISA as the central coordinating and control authority remains the most viable option. The decision to move away from an enterprise approach to dismantle the single common server solution under DISA may prove to be misguided – especially when whole-of-government cyber security requirements are weighed against the growing threat.

One example of a functioning, successful, mission-oriented JIATF model can be found in the federal counter-narcotics effort at Joint Interagency Task Force – South (JIATF-South). This Task Force operates under the command of a U.S. Coast Guard flag officer with elements of the command holding both Title 10 and Title 14 law enforcement authorities. Incorporating nearly a dozen federal agencies it has reached a high level of success after nearly 23 years of experimental and iterative growth both within the task force itself and in terms of the interagency pursuit of unity of effort. The JIATF option provides the requisite depth, breadth, and scope of response across U.S.C. authorities. It also enables constituent federal agencies and military services to procure, operate, and defend their information systems and networks. A JIATF model would provide the most clearly defined consolidation of authorities to plan, coordinate, integrate, and synchronize law enforcement and military missions in cyberspace. However, the JIATF option also risks a political reaction. Any perceived U.S. efforts to militarize cyberspace would not be well received by the commercial telecommunications industry and by certain competitor nations. Therefore, if this option is pursued, a strategic communication campaign explaining the interagency nature of the JIATF would be required well in advance of the announcement of its formation.

## Conclusion

In the JIATF construct, the role of organizing, training, and equipping the component pieces of the task force would remain within the purview of the military services and other federal departments and agencies, subject to DISA-directed standardization and accreditation.

In this approach, each element of the federal cyber infrastructure would be individually responsible for consolidation of security standards and operations, yet each constituent would retain its identity and ability to operate in cyberspace. A benefit to this approach would be the potential cost savings from the use of standardized software, a reduced number of network operations centers, and a diminished bandwidth requirement for duplicate transmission backbones. Federal agencies with smaller resource pools could realize economies of scale from larger, interdepartmental procurement efforts. Ultimately, the highest payoff of a single integrated command operating across all relevant legal authorities to address all aspects of national cyberspace security can be achieved in a JIATF construct. However, this option is not without risk. The perceived militarization of cyberspace may muddle political and diplomatic sensitivities regarding cyber operations for the Departments of State, Commerce, and Justice and may complicate the commercial and private sector's integration of their cyber systems with the federal government.

Given the nature of evolving cyber threats, DoD must re-orient its operating parameters relative to all federal agencies. This new approach would leverage an economy-of-force effort to provide collective cyber defense and multilateral operations (as articulated in the 8 June 2011 NATO Cyber Defence Policy). It would also consolidate authorities to address and respond to threats to the nation's cyber security.

Historically, nations go to war for reasons of national prestige, pursuit of vital interests, or fear of attack. Recently Russia allegedly employed cyber power against Estonia for reasons relating to national prestige. China has employed cyber power to acquire economic dominance. And perhaps some nations have engaged in cyber warfare to preempt a clear nuclear threat.

Clausewitz's preeminent advice to strategists was to know when you are at war and the nature of that war. The United States is under cyber attack in a war which our national leadership has not yet acknowledged. This new form of warfare has been directed against our national information infrastructure. The threat of future – and more damaging – attacks has been signaled by Iran and those who would challenge U.S. global leadership. Now is the time to organize and fight

this war that is being waged against our nation. Now is the time to unify and refocus United States cyber defenses to protect the nation's vital interests in cyberspace.

# U.S. Arctic Policy: Climate Change, UNCLOS and Strategic Opportunity

**Lieutenant Colonel Wayne M. Bunker**
United States Marine Corps

A scientifically measurable increase in average annual temperature in the Arctic region has resulted in local environmental warming at a rate twice that of the rest of the planet. This change in temperature has caused the polar icecap to recede by a significant amount. During the summer months, Arctic ice has been melting at approximately 8 percent per decade.[1] In 2012, the polar icecap is 25 percent smaller than it was in 1978. Not only is Arctic ice diminishing, the thickness of the ice is also decreasing at a notable rate. Ice thinning has a cumulative effect because the thinner ice melts more quickly the following summer, further reducing the icecap. Snow-covered ice reflects the sun's rays and thus preserves the ice. But as Arctic ice coverage decreases, an increasing amount of the sun's energy is absorbed by the darker ocean, thereby warming the water. This process also contributes to warmer atmospheric and water temperatures which only melts more ice. Scientists claim that this warming trend could yield an ice-diminished Arctic summer within 30 years.[2] For the rest of this century, the Arctic will remain ice-covered to some extent during the winter months, and the amount of ice reduction will vary from year to year. Some degree of residual ice will remain during the summer months. The term "ice-diminished" refers to sea ice concentrations of up to 15 percent in a given area.[3]

An ice-diminished Arctic opens shorter maritime transportation routes while providing greater access to prime fishing areas, to large deposits of natural resources, and to increased tourism opportunities. All of these will have significant economic implications in the foreseeable future and will significantly increase human activity in the region. This Arctic transformation has raised both latent and emerging sovereignty and security issues, such as disputed national boundaries, rights to exploit

or obligations to protect natural resources, and freedom of navigation through international shipping lanes.

This paper examines U.S. Arctic policy, identifies relevant capability gaps, and offers recommendations for achieving national strategic objectives in this evolving region.

## U.S. Arctic Policy

In April 2011, President Obama signed the most recent revision of the Unified Command Plan (UCP), which includes significant changes in Department of Defense (DoD) Arctic region responsibilities. The 2006 version of the UCP assigned responsibility for the Arctic jointly among U.S. Pacific Command (USPACOM), U.S. Northern Command (USNORTHCOM), and U.S. European Command (USEUCOM). The current version now assigns this responsibility to USPACOM and USNORTHCOM. The Combatant Command boundaries were previously drawn simply along meridians of longitude; the updated boundaries now reflect a more geopolitical approach that better supports U.S. strategic interests within the region. Figures 1 and 2 depict this change in Combatant Command boundaries. Additionally, the UCP specifically designates USNORTHCOM as the joint advocate for Arctic capabilities which further signals recognition of how the changing Arctic climate is likely to affect U.S. national security interests and objectives over time.


**Figure 1: 2006 UCP**[4]

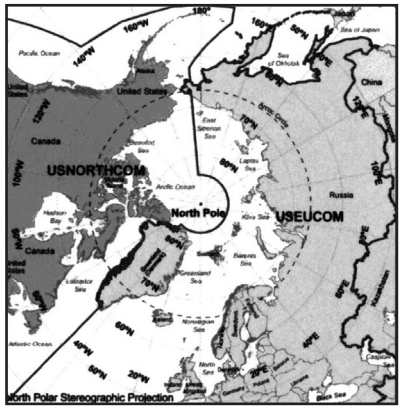


**Figure 2: 2011 UCP**[5]

U.S. strategic guidance for the Arctic region is found in the 2010 *National Security Strategy* (NSS), *National Security Presidential Directive 66* (NSPD-66), and *Homeland Security Presidential Directive 25* (HSPD-25), *Arctic Region Policy*. The NSS specifies Arctic interests as:

> *The United States is an Arctic nation with broad and fundamental interests in the Arctic region where we seek to meet our national security needs, protect the environment, responsibly manage resources, account for indigenous communities, support scientific research, and strengthen international cooperation on a wide range of issues.*[6]

NSPD-66/HSPD-25 list the following U.S. Arctic policy objectives:

- Meet national security and homeland security needs relevant to the Arctic region
- Protect the Arctic environment and conserve its biological resources
- Ensure that natural resource management and economic development in the region are environmentally sustainable
- Strengthen institutions for cooperation among the eight Arctic nations (the United States, Canada, Denmark, Finland, Iceland, Norway, the Russian Federation, and Sweden)
- Involve the Arctic's indigenous communities in decisions that affect them
- Enhance scientific monitoring and research into local, regional, and global environmental issues[7]

The 2010 Quadrennial Defense Review (QDR) cites several Arctic capability shortfalls such as communications, domain awareness, search and rescue, and environmental observation. Additionally, the QDR identifies shortfalls in capabilities needed to support both current and future planning and operations. One way to address these shortfalls is to leverage multinational and interagency cooperation.[8]

NSPD-66/HSPD-25 clearly identify "freedom of the seas," regarding surface navigation and overflight in the Arctic region, as a top national priority. The directive also points out that both the Northwest Passage and Northern Sea Route include international straits.[9] The

United States can assure future access to these straits as they become increasingly navigable by fulfilling relevant international obligations and responsibilities. An important first step in this direction is for the United States to ratify the United Nations Convention on the Law of the Sea (UNCLOS).[10]

## UNCLOS and Implications for Sovereignty

Recent trends strongly indicate that human activity in the Arctic region will continue to increase for the foreseeable future. This raises certain national and global security concerns. UNCLOS represents the international consensus on rules governing the use of the planet's oceans. This treaty was developed between 1973 and 1982; it was implemented on 16 November 1994. It combined several treaties governing laws of the sea that were previously separate. So, UNCLOS is a comprehensive treaty that codifies international law for the vast global commons of the world's oceans, which make up nearly three-quarters of the earth's surface. Notably, UNCLOS is an internationally accepted – and therefore legitimate – means of defining sovereignty over the world's oceans. It is particularly important in the Arctic, where several nations – including the United States – have conflicting claims. Articles within UNCLOS offer a framework for a peaceful resolution of sovereignty disputes. UNCLOS clearly specifies state and international rights as they pertain to the world's oceans.

The United States is the only Arctic nation that has not ratified UNCLOS. As of August 2011, 162 sovereign States and the European Union (EU) have ratified or acceded to the UNCLOS treaty.[11] The fundamental purpose of UNCLOS is to provide a set of international rules that govern the use of the world's oceans. These rules are designed to protect the economic, environmental, and national security interests of coastal states while safeguarding marine habitats and clarifying sovereign rights to natural resources. The treaty clearly defines several important geographical terms. Some of these physical domains defined in UNCLOS are internal waters, territorial waters, archipelagic waters, international waters, exclusive economic zones, and continental shelves.

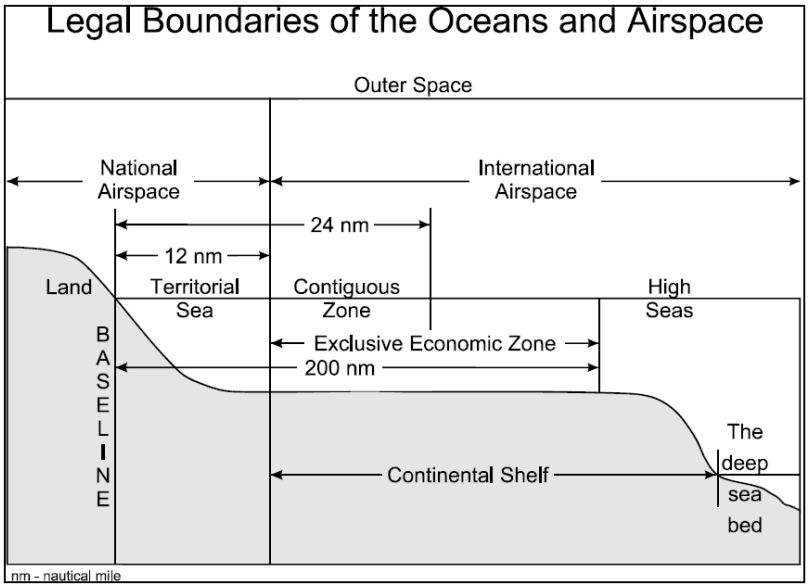


**Figure 3: UNCLOS Physical Geography Legend**[12]

Using these precise definitions, UNCLOS established an internationally recognized set of guidelines to prevent or resolve sovereign, economic, environmental and/or right of passage issues pertaining to the world's oceans. Regarding navigation, UNCLOS defines territorial waters as the area from a state's coastal baseline out to 12 nautical miles. This area constitutes the sovereign territory of the coastal state.

However, within this area, foreign vessels maintain the Right of Innocent Passage under certain precise circumstances.[13] The Right of Innocent Passage does not require prior notification. It is extended to surface transit of any ship or submarine through territorial waters so long as their transit is not prejudicial to the peace, good order, or security of the coastal state.[14] The next demarcated area is called the Contiguous Zone, which includes territorial waters and extends out 24 nautical miles from the baseline. Beyond territorial waters, the Contiguous Zone constitutes international waters for the purpose of navigation; however the coastal state maintains the right to enforce customs and immigration laws in the Contiguous Zone.[15] Beyond 12 nautical miles from the baseline line international waters where vessels are entitled to Freedom of the High Seas. In this capacity, foreign

vessels (surface vessels and submerged submarines) maintain the Right of Transit Passage in their normal modes.

The Right of Transit Passage also applies to unconstrained transit of such vessels, "in their normal modes through and over straits used for international navigation, and approaches to those straits."[16] UNCLOS also specifies how territorial boundaries of an archipelagic state are to be drawn and defines the Right of Archipelagic Sea Lanes Passage. Waters within an archipelago are considered sovereign internal waters. Nonetheless, ships, aircraft, and submerged submarines in their normal mode may transit through and over straits used for international navigation.[17] UNCLOS provides a legal basis for international vessels to legitimately transit international straits that lie within archipelagic sea lanes. In July 2011, during testimony before the Department of Homeland Security, the Commandant of the U.S. Coast Guard, Admiral Robert Papp, recommended:

> *As a matter of policy and stewardship, we encourage the Senate to ratify the Law of the Sea Treaty. Law of the Sea has become the framework for governance in the Arctic. Every Arctic Nation except the United States is a party. As our responsibilities continue to increase in direct proportion to the Arctic's emerging waters, it is more vital than ever that the U.S. ratifies the Law of the Sea.*[18]

The waters off Canada's northern coast between the Beaufort Sea and Baffin Bay are considered archipelagic waters by the United States and the EU. These waters include the Northwest Passage. Canada views these waters as strictly internal. Internal waters lie inland from the coastal baseline. The state maintains complete jurisdiction of internal waters. Foreign vessels transit internal waters only with the explicit consent of the sovereign nation that owns such waters.

## UNCLOS and Implications for Access to Natural Resources

The U.S. Geological Survey released a report in 2008 that indicated approximately 13 percent of the world's untapped oil reserves reside in the Arctic region. One-third of these reserves lie inside the U.S. Exclusive Economic Zone (EEZ) off the northern slope of Alaska. The report also estimated that approximately 30 percent of the world's

remaining natural gas reserves reside within the Arctic region.[19] In recent years, icecap melting, along with advances in technology, has rendered retrieval of natural resources in the Arctic both feasible and acceptable in terms of environmental risk.

In an effort conserve and responsibly exploit ocean and deep sea bed natural resources, UNCLOS defines an area called the Exclusive Economic Zone (EEZ). The EEZ extends out to 200 nautical miles from a state's coastal baseline. Within its EEZ, a coastal state possesses sovereign rights to all natural resources from fishing to deep seabed resources. Additionally, a provision within Article 76 of UNCLOS allows a nation to claim exclusive seabed mineral rights up to 350 nautical miles from its coastal baseline if it can be proved the continental shelf extends beyond the standard 200-nautical mile EEZ. Extended EEZ claims must be approved by the Commission on the Limits of the Continental Shelf (CLCS) within 10 years of a state ratifying UNCLOS.

The CLCS "consists of twenty-one technical experts who review a country's claims to ensure that the bathymetric and geological evidence submitted meets the convention's criteria."[20] This UNCLOS provision is particularly important for protecting U.S. claims in the Arctic. Among the five contiguous Arctic states (United States, Canada, Russia, Denmark, and Norway), the United States stands to gain tremendous mineral and oil extraction rights should the EEZ off the coast of Alaska be extended. The U.S. Government intends to continue to collect information required to support a claim that would extend the EEZ within the Arctic. However, as a non-member of UNCLOS, the United States is not eligible to submit a claim to the CLCS.[21] Representing the Council on Foreign Relations (CFR), Scott G. Borgerson argues the following:

> *By not joining [UNCLOS], the United States is actually giving up sovereign rights – missing an opportunity for international recognition or a massive expansion of U.S. resources jurisdiction over as much as one million square kilometers of ocean, an area half the size of the Louisiana Purchase. Remaining outside the convention prevents the United States from participating in the process of overseeing the claims of other countries to the extended continental shelf and from formally making its own.*[22]

As a non-member of UNCLOS, the United States "cannot fill its permanent seat on the ISA [International Seabed Authority] and is thus unable to exercise its special veto power over decisions on certain specified matters."[23] Ratifying UNCLOS allows the United States to apply for licenses through the ISA, which under the Convention, manages claims to resources in the deep seabed.

Shell Oil is currently the leading U.S. industry in offshore resource development within Alaska's EEZ, which extends into the Chukchi Sea. In May 2011, Shell Oil submitted its plan for oil exploration to the Bureau of Ocean Energy Management Regulation and Enforcement (BOEMRE). Shell had intended to begin exploratory drilling in the Chukchi Sea in 2012 using the Kulluk, a recently retrofitted mobile offshore drilling unit (MODU) specifically designed for offshore operations in the harsh Arctic environment.[24]

**U.S. Arctic Sovereignty Disputes**

UNCLOS is commonly referred to as the constitution of the sea. It offers an internationally recognized and legitimate framework to settle boundary and resource disputes between coastal nations. This is particularly important in the Arctic, where the United States has ongoing maritime boundary disagreements with both Russia and Canada. The United States and Canada have an unresolved boundary dispute in the Beaufort Sea, an area believed to be rich in oil, natural gas, and other resources. This dispute originates from the 1825 treaty between Britain and Russia that established the boundary between Alaska and the Yukon. The treaty adequately addressed land boundaries; however it did not determine maritime boundaries, so an area of 6,250 square nautical miles remains in dispute.[25] Additionally, the United States and Russia continue to abide by the terms of a maritime boundary agreement concluded in 1990. However, this bilateral agreement has yet to be ratified by the Russian Federation.[26] As a non-member of UNCLOS, the United States must attempt to resolve these disputes in another international forum.

## Freedom of Navigation in the Arctic

With the receding ice, both the Northwest Passage and the Northern Sea route (north of Russia) offer the potential for significantly shorter maritime trade routes. The efficiencies offered by dramatic reductions in distance, will most likely encourage a shift in maritime traffic to the Arctic routes.

The Northern Sea route instead of the Malacca Strait-Suez Canal route reduces the current trade route distance from Murmansk, Russia, to Yokahama, Japan by 7,700 miles, or 55 percent.[27] Similarly, the voyage from Rotterdam to Yokahama is reduced by 3,900 miles, or 35 percent.[28] The transit from Vancouver, Canada, to Rotterdam is shortened by 22 percent.[29]

Shortening the voyage by 3,900 miles and proceeding at a 15-knot speed of advance equates to a savings in transit time of approximately

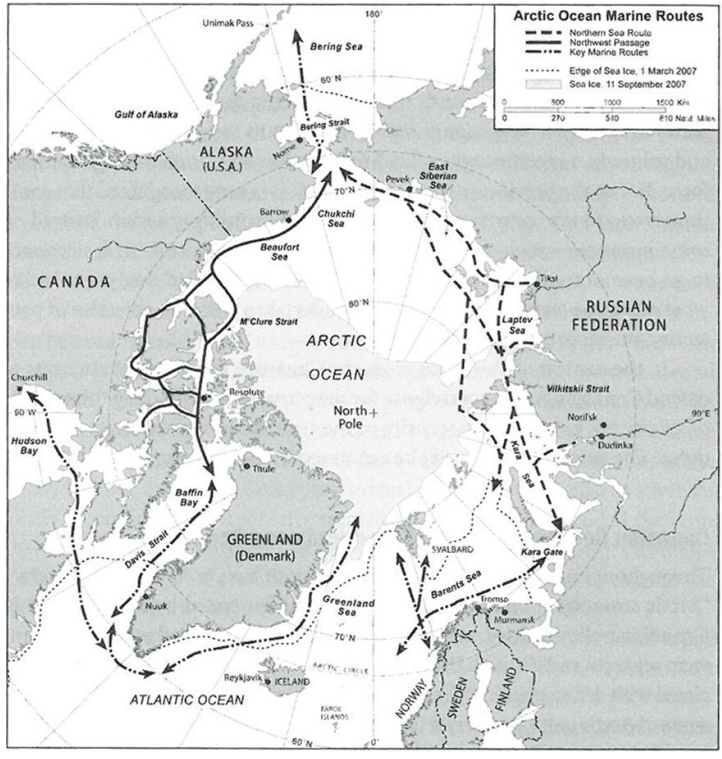


**Figure 4: Arctic Ocean Marine Routes**[30]

11 days. Escalating fuel costs increases the economic benefits of these shorter routes. The average Panamax containership costs $50,000 per day to operate; most of the expenses are for fuel and port charges.[31] Reducing the voyage by 11 days yields savings for that single voyage of $550,000.

| Port | Port | Via NSR (miles) | Via Canal (miles) | Percentage Difference |
|---|---|---|---|---|
| Murmansk | Yokohama | 5,770 | 12,840 | 55% |
| Rotterdam | Yokohama | 7,350 | 11,250 | 35% |
| Murmansk | Vancouver | 5,400 | 7,350 | 27% |
| Rotterdam | Vancouver | 6,920 | 8,920 | 22% |

**Table 1: Northern Sea Route Distances[32]**

In 2011 alone, 18 ships completed the voyage from northern Europe to northern Asia via the Northern Sea Route. The *Tschudi*, a Norwegian commercial ship, set the record in the summer of 2011 on her voyage from Norway to China. This route took only 21 days, 16 days less than required when taking the traditional route through the Suez Canal. The shipping company claims this shortcut saved an estimated $300,000 – with the added benefit of avoiding the pirate-infested waters off the coast of Somalia.[33]

Like the United States, the EU has a significant interests in ensuring that its member states' naval, and commercial vessels maintain freedom of navigation throughout the world, particularly in the Arctic. The EU views the Arctic as a potential major shipping route. The European Commission reported in 2008:

> *EU Member States have the world's largest merchant fleet and many of those ships use transoceanic routes. The melting of sea ice….could considerably shorten trips from Europe to the Pacific, save energy, reduce emissions, promote trade and diminish pressure on the main trans-continental navigation channels.*
>
> *….Member States and the Community should defend the principle of freedom of navigation and the right of innocent passage in the newly opened routes and areas.*[34]

## U.S. Arctic Capabilities

As other nations prepare to define and defend their sovereign jurisdictions in the Arctic, the capabilities required to protect and promote national interests there become more important. Russia is expanding its 20-vessel icebreaker fleet with the construction of additional nuclear-powered icebreakers. China, although not an Arctic nation, is building a state of the art icebreaker to conduct research and advance Chinese interests in the Arctic.[35] The EU and Canada have recently released new Arctic policy specifying their strategic objectives in the region. Additionally, the EU and Canada are fully utilizing their own icebreaking fleets (Canada with 6 vessels, EU nations with 19 vessels) to capitalize on new opportunities.[36]

Well before Alaska was admitted to the United States as the 49th state on 3 January 1959, the U.S. Coast Guard (USCG) was assisting Arctic scientific exploration, charting Arctic waters, providing humanitarian assistance to native tribes, conducting search and rescue, and exercising law enforcement activities in the region.[37] According to Admiral Robert Papp, Commandant of the U.S. Coast Guard: "We need to determine our nation's vessel shipping requirements for transiting ice-laden waters, consider establishing seasonal bases for air and boat operations, and develop a force structure that can operate in extreme cold and ice."[38]

Although the United States has a long history of Arctic operations, we are finding ourselves increasingly disadvantaged in terms of modern Arctic capabilities. One area in particular is U.S. icebreaking capability. In comparison to the other Arctic nations and key stakeholders to include China and the EU, the United States has fallen way behind. The entire inventory of U.S. icebreakers resides exclusively within the USCG, and consists of only three ships (two heavy icebreakers and one medium icebreaker). The *POLAR SEA* and *POLAR STAR* make up the heavy icebreaker fleet. Neither ship is currently in operational status. Each of these ships, operate with 134 crewmembers; they can break through ice up to 6 feet thick while moving at 3 knots.[39] On 14 October 2011, the USCG placed *POLAR SEA* in commissioned, inactive status, planning to fully retire the ship in fiscal year 2012.

The *POLAR STAR* is currently out of service undergoing a complex overhaul until 2013. Once this overhaul is complete, the *POLAR STAR's* service life will be extended to 2023.[40] In the meantime, the *HEALY*, a medium icebreaker with an estimated service life to 2029 is the only operational U.S. icebreaking capability. With its reduced icebreaking capability compared to that of *POLAR STAR* and *POLAR SEA*, *HEALY* was designed primarily to support Arctic scientific research.[41] The *HEALY* is capable of breaking through ice up to 4½ feet thick at a speed of 3 knots.[42] As the sole operational U.S. icebreaker, the *HEALY* is overworked. It is incapable of breaking the heavy ice that covers the Arctic surface most of any given year. Further complicating matters is the fact that the U.S. commercial fleet does not possess any heavy icebreaking capability. So DoD and commercial shipping companies must rely upon foreign-flagged commercial icebreakers or an ally such as Canada to provide this capability.[43]

Although the U.S. Navy does possess one ice-strengthened tanker for the purpose of resupplying the U.S. military installation in Thule, Greenland, it relies on foreign-flagged icebreakers and contracted shipping to accomplish the mission. The U.S. Navy's inventory of surface ships does not include any vessels outfitted with ice- strengthened hulls that allow for safe passage in first-year ice or marginal ice zones.[44]

So, the U.S. Navy has – at best – only marginal capability to conduct forward-presence and freedom of navigation operations in the Arctic. Although the Navy's submarine fleet has a rich history of Arctic operations, it is ill prepared to take advantage of the rapidly increasing surface navigability of Arctic waters.

## Capability Gaps

In a DoD report to Congress, several Arctic capability gaps were highlighted. These gaps ranged from communications to infrastructure shortfalls. Specifically, U.S. communications capabilities within the Arctic were reportedly both limited and degraded. For example, due to solar and magnetic phenomena associated with latitudes above 70°N, high-frequency (HF) radio signals are significantly hampered.[45] In addition, the lack of surface-based relay stations throughout the region further complicates communications. Although suitable for

surface navigation, Global Positioning System (GPS) in the region lacks the capability required for certain mission sets such as search and rescue (SAR) and precision weapons guidance. This limitation is due in part to "poor satellite geometry, ionospheric effects, and multipath interference."[46] Because GPS satellites do not pass over the North Pole, the ones that are visible to an Arctic GPS receiver appear low on the horizon. This reduces necessary satellite geometry and increases potential for a multipath environment.

Current U.S. infrastructure in the Arctic region (bases, airfields, ports, roads, railways, lodging and utilities) does not support the NSS or U.S. Arctic policy, NSPD-66/HSPD-25, or the QDR. This lack of infrastructure means the United States lacks maritime domain awareness and in some cases, cannot perform successful SAR missions. There are small U.S. military bases and ports in Alaska and the Aleutian Islands, however there are no facilities on the northern slope.[47] Figure 4 depicts current U.S. installations in the Arctic, including bases in Alaska and Thule Air Base, Greenland.

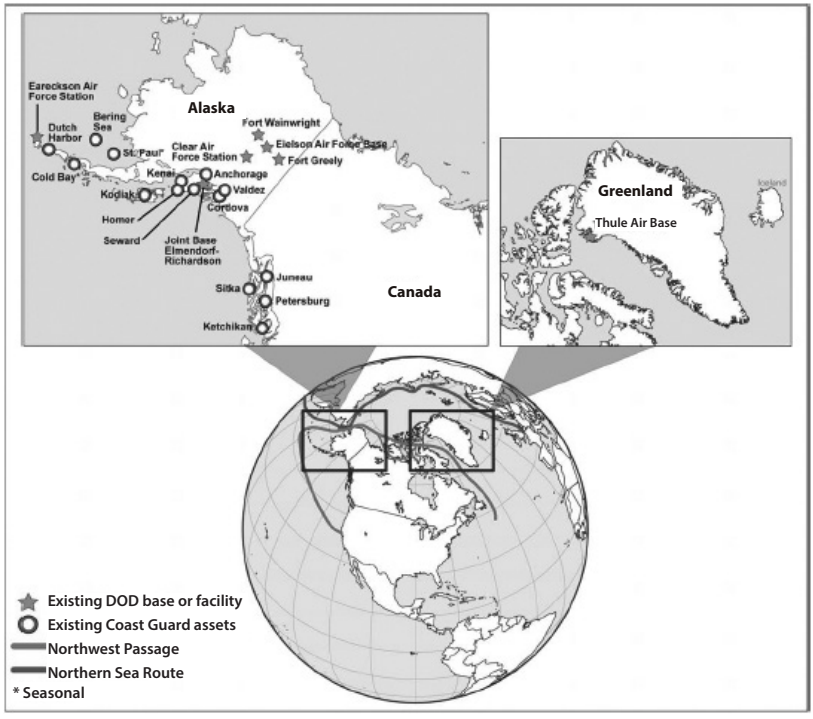


**Figure 4: Current U.S. Bases and Facilities in Alaska and the Arctic**[48]

Bases such as Elmendorf, Eielson, and Thule provide some SAR capabilities. However, the United States lacks the infrastructure and proximity of equipment to provide effective SAR support for most of the Arctic region, especially for the northern slope. As human activity in the Arctic region increases, so do the importance of Maritime Domain Awareness (MDA) and the supporting infrastructure.

Land-based as well as maritime capabilities used in support of Arctic MDA will require an appropriate infrastructure to support this evolving national requirement. In testimony before the Senate Commerce, Science and Transportation Subcommittee, Dr. Andrew Metzger, an expert on Arctic Marine Civil Infrastructure, reported:

> *…the norm for Arctic coastal communities is that existing housing, water, wastewater and power utilities only marginally meet community needs.…[and] escalating maritime activities, as well as development of any new marine infrastructure, will likely overwhelm these communities. [In addition], roadways are generally undeveloped and not connected to the contiguous highway system [and] there is no rail system. Transportation consists of annual barge service along with air service that is more frequent. Since barge traffic is sporadic during the one or two months of ice free seas, all materials must be carefully scheduled as much as a year in advance. Any missing materials must be either flown in or sent via barge the following year.*[49]

In January 2012, Metzger's assessment of limited Arctic infrastructure was validated when the USCG's only operational icebreaker, *HEALEY*, escorted the Russian-flagged oil tanker *Renda* through the frozen Bering Sea off the coast of Nome, Alaska. The fall barge shipments of fuel had failed to reach Nome, leaving the town of 3,600 people without winter fuel reserves. Since Nome was inaccessible by road, the option for delivery of 1.3 million gallons of oil by the *HEALY/Renda* team was chosen over the cost-prohibitive air-land option.[50] This was not the first time the people of Nome had faced disaster. During the winter of 1925, diphtheria ran rampant throughout the town, posing an immediate threat to the population of 1,400 as medicine to treat the disease ran perilously low. Then the air and sea method of resupply was not an option, so medicine was delivered by dog sled.[51] Today, the

population of Nome has more than doubled. Nome's U.S. citizens rely on oil and gas to heat homes and power modern machinery and vehicles. In this most recent scenario, the *HEALY/Renda* team was able to break through the ice and disaster was averted.

Building and maintaining infrastructure in the harsh Arctic environment is very expensive. Skilled labor and materials are scarce. The construction season is short. Structures must be specially designed for the Arctic environment. Without adequate infrastructure to support increasing human activity in the Arctic, the demand for accessible and effective SAR and MDA will only increase.

**International Cooperation**

A cooperative approach among international partners is key to ensuring U.S. interests are met within the Arctic region. A multinational effort is essential to ensure both human safety and appropriate environmental stewardship. A unilateral U.S. approach is simply not feasible. However, as the world's sole superpower and as a contiguous Arctic nation, it is imperative that the United States assumes an Arctic leadership role within the international community.

Perhaps the most important step for the United States is to ratify UNCLOS in order to establish the legitimacy of U.S. leadership among the other stakeholders who have interests in the Arctic. This would partner the United States with the seven other Arctic nations, along with six indigenous organizations that are permanent members of the Arctic Council.[52] This multinational assembly meets semiannually and "provides the greatest potential for a comprehensive resolution of environmental and governance issues in the Arctic."[53]

NSPD-66/HSPD-25 clearly acknowledges that the "Arctic Council has produced positive results for the United States by working within its limited mandate of environmental protection and sustainable development."[54] U.S. representation on the Arctic Council has slowly increased since its first meeting in 1996. In fact, in March 2010 Secretary of State Hillary Clinton met with her counterparts from Canada, Russia, Denmark, and Norway in Chelsea, Quebec, as part of the Arctic Ocean Foreign Ministers' Meeting. This meeting affirmed

the importance of the Arctic Council, its membership, and the need for "new thinking on economic development and environmental protection."[55]

However, the Arctic Council is hindered by its "lack of regulatory authority and the mandate to enact or enforce cooperative security-driven initiatives."[56] Although very useful for "scientific assessments" and "policy-relevant knowledge," the Council does not address military concerns.[57]

The International Maritime Organization (IMO) is yet another important international organization identified by NSPD-66/HSPD-25. It fosters both international cooperation and promotes U.S. interests in the Arctic. The IMO was formed in 1948 to "maintain a comprehensive framework for shipping" and regulation of "ocean carriers in terms of safety, pollution prevention, and security."[58] Within the UNCLOS framework, IMO provides a forum for settling the dispute between the United States and Canada concerning determination of international and internal waters along the Northwest Passage.

Security in the Arctic region is another critical issue that should be addressed through international cooperation. Given the U.S. infrastructure shortfalls and capability gaps discussed in this paper, international partnership is perhaps the most efficient, timely, and feasible means for achieving U.S. security objectives. SAR, icebreaker support, environmental disaster response, and logistical support are just a few examples of activities that all stakeholders should conduct cooperatively to sustain regional security and assure regional stability. Military exercises conducted jointly among other Arctic nations such as Operation Nanook (USN/Canada), Operation Cold Response (U.S. Marine Corps/Norway), and Operation Arctic Care (U.S. Army Reserve/U.S. Air National Guard) can enhance regional security and promote sharing of capabilities and multilateral infrastructure development.[59]

**Recommendations**

First and foremost, the United States should ratify the United Nations Convention on the Law of the Sea. To date, 162 sovereign states, all of

the Arctic nations, every major U.S. ally, and the EU have acceded to the UNCLOS treaty. The list of nations who have not ratified UNCLOS is short. It includes Iran, North Korea, and Syria.[60] As the world's sole superpower and as a contiguous Arctic Nation, the United States must join UNCLOS in order to have a legitimate voice in the region. UNCLOS is the internationally recognized instrument for peacefully resolving boundary and resource disputes, for extending EEZs where applicable, and for assuring freedom of navigation along the Northwest Passage and Northern Sea Route. The Obama Administration should aggressively pursue Senate ratification of UNCLOS. U.S. membership in UNCLOS is essential for advancing national security and for assuring economic and environmental interests in the Arctic and throughout the rest of the world.

As the United States assesses both its short-term and long-term capability gaps, it should carefully pursue planned and coordinated solutions that address the requirements of the Department of Defense, Department of Homeland Security, Department of State, Department of the Interior, Department of Transportation, Department of Commerce's National Oceanic and Atmospheric Administration, and other federal stakeholders – such as the National Science Foundation. A risk-based investment strategy for the Arctic should be developed that:

1. Identifies and prioritizes short-term and long-term Arctic capability shortfalls
2. Develops a timeline for addressing the identified shortfalls
3. Incorporates a process that ensures assessments are updated as appropriate.[61]

At a minimum, the U.S. government should sustain the current polar icebreaking fleet (*POLAR STAR* and *HEALY*) and initiate the programming, appropriation, design, and construction of two new USCG heavy icebreakers with appropriate support aircraft. They should be delivered no later than 2020 in order to replace *POLAR STAR* (forecast decommission: 2023) and *HEALY* (forecast decommission: 2029).

A joint, interagency airport and seaport facility – open to multi-national use – should be established on the north slope of Alaska. This installation should serve as Forward Operating Base (FOB)

for all appropriate stakeholders within the U.S. government. Basic capabilities of the FOB should include:

- Personnel support facilities (billeting, dining, etc.)
- Suitable aircraft and surface vessel servicing and maintenance capability
- Appropriate communications infrastructure to support to the full range of governmental operations within the Arctic

## Conclusion

The fundamental pillars of U.S. Arctic policy should be assured U.S. sovereignty, strong national and regional security, freedom of the seas, stewardship, and international cooperation. Global climate change is dramatically affecting the Arctic region. The receding Arctic icecap has brought with it the lure of vast deposits of exploitable natural resources, commercial fishing opportunities, shorter sea lanes, and increased tourism. Human activity is quickly increasing in the region. How the Arctic community's leaders react to these emerging issues may very well be one of the defining moments of the 21st century. As the icecaps continue to recede, U.S. interests in the Arctic region become more important. Compared to the other Arctic nations, the United States is slow in preparing for an ice-diminished or ice-free Arctic. U.S. inaction risks the nation's ability to influence the region as articulated in the NSS and more specific Arctic policy. This paper has identified some short-term and long-term Arctic capabilities gaps which are impediments for assuring U.S. strategic interests in the region. The uncertainty surrounding the rate and long-term forecasts of icecap recession requires deliberative preparation, especially in a period of fiscal austerity. The United States cannot afford to further delay its investments in the Arctic. U.S. leaders must invest in the Arctic infrastructure and in icebreakers, despite their considerable expense and long lead time. The Arctic is clearly a region that requires a joint, interagency and multilateral effort to support U.S. – and global – security interests.

# Endnotes

## Section One
## Recommitting Against Complacency

### Introduction

1. U.S. Department of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (January 2012).
2. Statutorily authorized under Title 32, United States Code §325(a)(2).
3. Statement of Secretary of Defense Leon E. Panetta, delivered in a presentation to the Environmental Defense Fund on 3 May 2012.

### Homeland Security and Homeland Defense: The Seam of Uncertainty Unstitched

1. Barack H. Obama, *National Security Strategy* (Washington, DC: The White House, May 2010), 18.
2. Scott Pelley, "Fighting Terrorism in New York City," September 25, 2011, *CBS News*, streaming video, 14:21, http://www.cbsnews.com/video/watch/?id=7382308n&tag=contentBody;storyMediaBox (accessed October 18, 2011).
3. Obama, *National Security Strategy,* 18.
4. Ibid.,19.
5. Ibid.,18-19.
6. Obama, *Presidential Policy Directive 8: National Preparedness* (Washington DC: The White House, March 30, 2011), 1.
7. Ibid., 2.
8. Ibid., 3.
9. Janet Napolitano, *Quadrennial Homeland Security Review Report* (Washington DC: U.S. Department of Homeland Security, February2010), viii.
10. Ibid., ix. Emphasis in original.
11. Ibid., 31.
12. Ibid.

13. Ibid., 34.
14. Ibid., 39.
15. George W. Bush, *Homeland Security Presidential Directive/HSPD-5* (Washington DC: The White House, February 2003), 1.
16. Ibid., 2.
17. Napolitano, *Quadrennial Homeland Security Review Report*, 72-73.
18. Robert M. Gates, *Quadrennial Defense Review* (Washington DC: U.S. Department of Defense, February 2010), 18.
19. Ibid.,19.
20. 2010 *Army Posture Statement,* Office of the Director of the Army Staff, Executive Strategy Group (Washington DC: U.S. Department of Defense), quoted in Christine Le Jeune, "Consequence Management: Steps in the Right Direction?," *Institute of Land Warfare*, September 8, 2010), 4.
21. U.S. Government Accountability Office, *Progress Made and Work Remaining in Implementing Homeland Security Missions 10 Years after 9/11* (Washington DC: U.S. Government Accountability Office, September 2011), 2.
22. Michael Chertoff, *National Incident Management System* (Washington DC: December 2008), 6.
23. Ibid.
24. U.S. Department of Homeland Security, *National Response Framework* (Washington DC: January 2008), 1. Emphasis in original.
25. Ibid., 57.
26. U.S. Joint Chiefs of Staff, *Homeland Defense* (Washington DC: U.S. Joint Chiefs of Staff, July 12, 2007), VII-5.
27. U.S. Joint Chiefs of Staff, JP 3-28 *Civil Support*, (Washington DC: U.S. Joint Chiefs of Staff, September 14, 2007), II-21-22.
28. U.S. Joint Chiefs of Staff, JP 3-41 Chemical, Biological, Radiological, Nuclear, and High-Yield Explosives Consequence Management, (Washington DC: U.S. Joint Chiefs of Staff, October 2, 2006), II-7.
29. Federal Emergency Management Agency Home Page, http://www.fema.gov/ (accessed 14 December 2011).
30. Ibid.
31. Gates, *Quadrennial Defense Review,* 19.

32. Steve Cichocki, "CBRN Response Enterprise Smartbook," briefing slides, United States Army Northern Command, December 2011.
33. National Guard Home Page, http://www.ng.mil/features/HomelandDefense/cst/factsheet.html (accessed December 14, 2011).
34. Cichocki, "CBRN Response Enterprise Smartbook"
35. Ibid.
36. General Charles H. Jacoby, Commander, USNORTHCOM, "USNORTHCOM CONPLAN, CBRN Response 3500-11" (Peterson Air Force Base, CO, United States Northern Command, August 17, 2011), 16.
37. *Emergency Management Assistance Compact*, Public Law 104-321, 104th Cong., 2nd sess. (October 19, 1996).
38. Jacoby, "USNORTHCOM CONPLAN, CBRN Response 3500-11," A-5.
39. Ibid., A-3.
40. Ibid., 22.
41. Ibid., 3.
42. Ibid., 18.
43. Steve Cichocki, "USNORTHCOM CBRN Response Enterprise Update To Senior Steering Group," briefing slides, Peterson Air Force Base, CO, USNORTHCOM, September 23, 2011.
44. Ibid.
45. U.S. Department of Homeland Security, *National Response Framework*, 10.
46. Ibid., 8.
47. Ibid., 40.
48. Ibid., 41.
49. Ibid., 42.
50. Chertoff, *National Incident Management System,* 23.
51. Napolitano, *Quadrennial Homeland Security Review Report*, 34.
52. James Burch, "The Domestic Intelligence Gap: Progress Since 9/11?,"*Homeland Security Affairs,* Supplement no. 2 (2008): 9.
53. Ibid., 10.
54. Mike McConnell, "Overhauling Intelligence," *Foreign Affairs* 86.4 (Jul/Aug 2007): 3.
55. Ibid., 3.

56. Ibid., 4.
57. Kevin D. Eack, "State and Local Fusion Centers: Emerging Trends and Issues," *Homeland Security Affairs*, Supplement no.2 (2008): 2.
58. Ibid., 1.
59. Ibid., 2.
60. Burch, "The Domestic Intelligence Gap: Progress Since 9/11?," 13.
61. Ibid.
62. Ibid.
63. Ibid., 14.
64. Christopher Voss, *Connecting Our Nation's Crisis Information Management Systems*, Thesis (Monterey, CA: Naval Post Graduate School, December 2008), 2.
65. Ibid., xvi.
66. Burch, "The Domestic Intelligence Gap: Progress Since 9/11?," 17.
67. Voss, *Connecting Our Nation's Crisis Information Management Systems*, 11.
68. Ibid., 18.
69. Ibid.
70. Ibid., 3.
71. U.S. Department of Homeland Security, *Final Report: Homeland Security Information Network Advisory Committee Meeting* (Washington DC: U.S. Department of Homeland Security, March 27, 2009), 5.
72. Ibid., 15.
73. Ibid., 21.
74. Ibid., 26.
75. Barack Obama, *Presidential Policy Directive 8: National Preparedness* (Washington DC: The White House, March 2011), 1.
76. Ibid., 3.
77. Voss, *Connecting Our Nation's Crisis Information Management Systems*, 56.

## 9/11 Ten Years After: Command, Control, Communications Remain An Issue

1. Thomas H. Kean and Lee H. Hamilton, *The 9/11 Commission Report* (2004), 298.

2. Barack H. Obama, *National Security Strategy* (Washington DC: The White House, May 2010), 17.
3. Ibid., 18.
4. Ibid., 19.
5. Kean and Hamilton, *The 9/11Commission Report*, 283.
6. Ibid.
7. Kean and Hamilton, *The 9/11Commission Report*, 280.
8. Ibid.
9. *Homeland Security Act of 2002*, Public Law 107-296, 107th Cong. (November 25, 2002), 8.
10. Ibid.
11. *Robert T. Stafford Disaster Relief and Emergency Assistance Act*, Public Law 93-288, as amended, codified at 42 U.S.C. 68. (June, 2007), 1.
12. Ibid.
13. George W. Bush, *Homeland Security Presidential Directive-5, Management of Domestic Incidents* (Washington DC: The White House, February 28, 2003), 1.
14. Ibid.
15. George W. Bush, *Homeland Security Presidential Directive-8, National Preparedness* (Washington DC: The White House, February 28, 2003), 4.
16. U.S. Department of Homeland Security, *National Infrastructure Protection Plan* (Washington DC: Department of Homeland Security, 2009), 9.
17. Ibid.
18. Michael Chertoff, *National Incident Management System* (Washington DC: Department of Homeland Security, December 2008), 1.
19. Ibid., 23.
20. U.S. Department of Homeland Security, *National Response Framework* (Washington DC: Department of Homeland Security, January 2008), 7.
21. Michael Chertoff, *National Emergency Communications Plan* (Washington DC: Department of Homeland Security, July 2008), 6.
22. Ibid, 2.
23. Ibid.
24. Todd M. Keil and W. Craig Conklin, *Emergency Services Sector-Specific Plan* (Washington DC: Department of Homeland Security, 2010), 27.
25. George W. Bush, *A National Security Strategy for Homeland Security* (Washington, DC: The White House, October 2007), 4.

26. U.S. Government Accountability Office, *Emergency Communications: National Communications Systems Provides Programs for Priority Calling, but Planning for New Initiatives and Performance Measurement Could be Strengthened* (Washington DC: Government Accountability Office, August, 2009), 13.
27. Ibid, 16.
28. "Wireless Priority Service," linked from *National Communications System Page* at "Wireless Priority Service," http://wps.ncs.gov/program_info.html (accessed January 26, 2012).
29. U.S. Government Accountability Office, *Emergency Communications*, 17.
30. "Statewide Communication Interoperability Plans," October 13, 2010, linked from *The Department of Homeland Security* page at "Statewide Communication Interoperability Plans," http://www.dhs.gov/files/programs/gc_1225902750156.shtm (accessed December, 15, 2011).
31. FY 2010 Interoperable Emergency Communications Grant Program, linked from *Federal Emergency Management Agency* at "FY 2010 Interoperable Emergency Communications Grant Program," http://www.fema.gov/government/grant/iecgp/index.shtm (accessed December, 15, 2011).
32. Ibid.
33. Chertoff, *National Incident Management System*, 141.
34. U.S. Government Accountability Office, *First Responders: Much Work Remains to Improve Communications Interoperability* (Washington DC: Government Accountability Office, 2007), 9.
35. Chertoff, *National Emergency Communications Plan*, 2.
36. Kean and Hamilton, *The 9/11Commission Report*, 397.
37. Thomas H. Kean and Lee H. Hamilton, *Tenth Anniversary Report Card: The Status of the 9/11 Commission Recommendations* (September, 2011), 14.
38. Andrew M. Seybold, "The Value of the D Block," October 11, 2011, http://andrewseybold.com/2674-the-value-of-the-d-block (accessed November 14, 2011).
39. Linda K. Moore, *Funding Emergency Communications: Technology and Policy Considerations* (Washington DC: U.S. Library of Congress, Congressional Research Service, October 4, 2011), 35.
40. Ibid., 11.
41. Ibid., 3.
42. Ibid., 5.
43. Seybold, "The Value of the D Block."
44. *President Obama Details Plan to Win the Future through Expanded Wireless Access* (Washington DC: The White House, Office of the Press Secretary February 10, 2011), 2.

45. "The Benefits of Transitioning to a Nationwide Wireless Broadband Network for Public Safety" (Washington DC: The White House, November 14, 2011), 5.
46. Moore, *Funding Emergency Communications*, 12.
47. Ibid., 12.
48. "The Benefits of Transitioning to a Nationwide Wireless…", 11.
49. Moore, *Funding Emergency Communications*, 11.
50. Chertoff, *National Incident Management System*, 49.
51. Kean and Hamilton, *The 9/11Commission Report*, 298.
52. Otto J. Guenther, "Blue Force Tracking," *Army*, April 1, 2004, 13.
53. Michael M. Sweeney, *Blue Force Tracking: Building a Joint Capability*, Strategic Research Project (Carlisle Barracks, PA: U.S. Army War College, March 15, 2008), 5.
54. Guenther, "Blue Force Tracking," 13.
55. David M. Halbfinger, "GPS Units so Faulty, they Showed Fire Trucks in New York Harbor," *New York Times*, November 9, 2011.
56. Fire Department of New York, *FDNY Strategic Plan 2011-2013* (New York, NY: Fire Department, City of New York, 2011), 9.
57. Ibid.
58. Ibid.
59. Chertoff, *National Incident Management System*, 23.
60. U.S. Department of Homeland Security, *National Response Framework* (Washington DC: Department of Homeland Security, January 2008), 32.
61. Todd M. Keil and W. Craig Conklin, *Emergency Services Sector-Specific Plan* (Washington DC: Department of Homeland Security, 2010), 61.
62. U.S. Department of Homeland Security, *National Infrastructure Protection Plan* (Washington DC: Department of Homeland Security, 2009), 63.
63. U.S. Department of Homeland Security, *National Response Framework*, 55.
64. "Homeland Security Information Network," linked from *The Department of Homeland Security* page at "Homeland Security Information Network," http://www.dhs.gov/files/programs/gc_1156888108137.shtm (accessed January 26, 2012).
65. U.S. Department of Homeland Security, *National Response Framework*, 51.
66. Sweeney, *Blue Force Tracking: Building a Joint Capability*, 14.
67. Ibid.
68. New York City Office of Emergency Management, New York City Community Emergency Response Team, Standard Operating Procedure (New York, NY:

New York City Office of Emergency Management, August, 2009), Appendix D, 1.

69. "Emergency Response: Geographic Information Systems," linked from *New York City Office of Emergency Management* at "Emergency Response: Geographic Information Systems," http://home2.nyc.gov/html/oem/html/about/about_gis.shtml (accessed January 26, 2012).
70. "NYC OEM Incident Management & Coordination in NYC," briefing slides, Queens Hospital Center, September 18, 2008.
71. Ibid.
72. Ibid.
73. "The Benefits of Transitioning to a Nationwide Wireless…, 11.
74. *President Obama Details Plan to Win the Future through Expanded Wireless Access*, 2.
75. Andrew M. Seybold, "Public Safety Broadband: Real-World Test Results," September 18, 2011, http://andrewseybold.com/2637-public-safety-broadband-real-world-testing-results (accessed November 14, 2011).
76. Seybold, "The Value of the D Block."
77. Todd M. Keil and W. Craig Conklin, *Emergency Services Sector-Specific Plan* (Washington DC: Department of Homeland Security, 2010), 62.
78. Chertoff, *National Emergency Communications Plan*, 22.
79. Ibid, 12.
80. *President Obama Details Plan to Win the Future through Expanded Wireless Access*, 2.
81. Chertoff, *National Emergency Communications Plan*, 17.

## The Role of Military Forces in Disaster Response: Remove the Impediments

1. Arnold Punaro, "The Unfinished Business and the Appalling Gap," in *Before Disaster Strikes: Imperatives for Enhancing Defense Support of Civil Authorities*, The Report of the Advisory Panel on Department of Defense Capabilities for Support of Civil Authorities After Certain Incidents (Washington DC: RAND Corporation for the Department of Defense, 2010), 91-92, http://www.rand.org/content/dam/rand/www/external/nsrd/DoD-CBRNE-Panel/Report-Advisory-Panel.pdf
2. "New USGS number puts Japan quake at 4th largest," *Associated Press*, March 14, 2011, http://www.cbsnews.com/stories/2011/03/14/501364/main20043126.shtml (accessed December15, 2011).
3. William Carwile III, *Earthquake Preparedness—What the United States Can Learn from the 2010 Chilean and Haitian Earthquakes*, before the Senate committee on Homeland Security and Governmental Affairs, 111th Cong., 2nd sess., September 30, 2010, http://www.hsdl.org/?view&did=16908 (accessed January 1, 2012), 7.

4. "About the New Madrid Seismic Zone," http://sema.dps.mo.gov/Earthquake_Preparedness/earthquake_information/about_the_new_madrid_zone.asp (accessed 8 December 8, 2011).
5. Alicia Acuna, "As U.S. Preps for Nuclear Disaster Drills, Scientists Reassure About Quake Zone Facilities," March 28, 2011, http://www.foxnews.com/politics/2011/03/28/preps-nuclear-disaster-drills-scientists-reassure-quake-zone-facilities (accessed January 1, 2012).
6. Federal Emergency Management Agency, homepage, http://www.fema.gov/about (accessed December 12, 2011).
7. Commission On the National Guard and Reserves, "Strengthening America's Defenses in the New Security Environment," March 1, 2007, http://www.hsdl.org/?view&did=236368 (accessed January 1, 2012), 60.
8. Lynn E. Davis and others, *Hurricane Katrina: Lessons for Army Planning and Operations* (Santa Monica, CA: The Rand Corporation, 2007), http://www.rand.org/pubs/monographs/2007/RAND_MG603.pdf (accessed December 12, 2011), 5.
9. Eric S. Blake, Ethan J. Gibney, Christopher W. Landsea, *The Deadliest, Costliest, and Most Intense United States Tropical Cyclones From 1851 to 2010* (Miami, FL: National Ocean Atmospheric Administration, 2011), http://www.nhc.noaa.gov/pdf/nws-nhc-6.pdf (accessed December 16, 2011), 7.
10. Paul McHale, Assistant Secretary of Defense for Homeland Defense, *The Role of the Military and National Guard in Disaster Response before the House of Representative Committee on Homeland Security, Subcommittee on Emergency Preparedness, Science, and Technology,* 109th Cong., 1st sess., November 9, 2005, http://www.dod.gov/dodgc/olc/testimony_old/109_first.html (accessed December 16, 2011), 2.
11. Jeffrey W. Burkett, "Command and Control of Military Forces in the Homeland," *Joint Forces Quarterly* 51 (4th Quarter 2008), https://www.hsdl.org/?view&did=234611 (accessed November 10, 2011), 131.
12. The White House, *The Federal Response to Hurricane Katrina: Lessons Learned* (Washington DC: The White House, 2006) http://georgewbush-whitehouse.archives.gov/reports/katrina-lessons-learned/foreword.html (accessed November 10, 2011), 3.
13. "Hurricanes and Tropical Storms" *The Palm Beach Post*, http://www.palmbeachpost.com/storm/content/storm/2005/atlantic/katrina/day_by_day_archive.html (accessed December 18, 2011).
14. Punaro, "The Unfinished Business," 3.
15. U.S Department of the Army, *Civil Support Operations,* Field Manual 3-28 (Washington DC: U.S Department of the Army, June 29, 2010), http://usacac.army.mil/cac2/FM3-28/FM328.pdf (accessed November 10, 2011), 1-4.

16. Ibid.
17. U.S. Constitution, art. 1, sec. 8.
18. U.S. Constitution, art. 2, sec. 2, quoted in *Civil Support Operations* (Washington, DC: U.S. Department of the Army, June 29, 2010), http://usacac.army.mil/cac2/FM3-28/FM328.pdf (accessed November 10, 2011), 1-3.
19. Department of the Army, *Civil Support Operations,* 1-3.
20. Federal Emergency Management Agency, *National Response Framework,* (Washington DC: FEMA, 2008) http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf (accessed September 15, 2011).
21. Department of the Army, *Civil Support Operations*, ix.
22. Ibid.
23. Defense Science Board Task Force, *Deployment of Members of the National Guard and Reserve in the Global War on Terrorism*," September 2007, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA474519 (accessed November 10, 2011), 18.
24. State of Nevada, "Emergency Management Assistance Compact Chapter 415, Article IV," http://www.leg.state.nv.us/nrs/NRS-415.html (accessed December 23, 2011).
25. Department of the Army, *Civil Support Operations,* 1-4.
26. Ibid., 1-5.
27. Commission on the National Guard and Reserves, "Strengthening America's Defenses," 59.
28. National Guard Bureau Office of Legislative Liaison, "Analysis of the 2012 National Defense Authorization Act for Fiscal Year 2012" (December 31, 2011), http://www.ng.mil/ll/analysisdocs/FY2012/NGB-LL%20Analysis%20-%20FY12%20NDAA.pdf (accessed January 3, 2012).
29. Davis and others, *Hurricane Katrina: Lessons*, 37.
30. Eric Lipton, Eric Schmitt, and Thom Shanker, "Political Issues Snarled Plans for Troop Aid," *The New York Times* online, September 9, 2005, http://www.nytimes.com/2005/09/09/national/nationalspecial/09military.html?pagewanted=all (accessed February 3, 2012).
31. John Brinkerhoff, "Posse Comitatus," November 21, 2005, http://www.military.com/opinion /0,15202,80968,00.html (accessed December 27, 2011).
32. Mackubin T Owens, "Hurricane Katrina and the Future of American Civil-Military Relations," September 2005, http://www.ashbrook.org/publicat/oped/owens/05/katrina.html, (accessed February 3, 2012).
33. Sean Mcgrane, "A new exception to Posse Comitatus Act," *Michigan Law Review* 108, no. 7 (May 2010), 1315.
34. Ibid., 1316.

35. Ibid., 1312.
36. Gallup, "Congress Ranks Last in Confidence in Institutions," July 22, 2010, http://www.gallup.com/poll/141512/congress-ranks-last-confidence-institutions.aspx (accessed December 30, 2011).
37. Mitchell Moss, Charles Schellhamer, and David A. Berman, "The Stafford Act and Priorities for Reform," *Journal of Homeland Security and Emergency Management*, Volume 6, Issue 1, Article 13 (The Berkeley Electronic Press, 2009), http://www.nyu.edu/ccpr/pubs/Moss_03.09.09.pdf (accessed December 28, 2011).
38. Ibid., 1.
39. The White House, *The Federal Response to Hurricane Katrina*, 18.
40. Jennifer K Elsea, *The Use of Federal Troops for Disaster Assistance: Legal Issues* (Washington DC: U.S. Library of Congress, Congressional Research Service, November 28, 2008), 4.
41. Christopher B Walters, "Responding to National Disasters and Emergencies: A Contract and Fiscal Law Primer," *The Army Lawyer*, no. 10 (2007), http://www.loc.gov/rr/frd/Military_Law/pdf/10-2007.pdf (accessed December 29, 2011), 37.
42. Elsea, *The Use of Federal Troops*, 5.
43. Ibid.
44. Federal Emergency Management Agency, *National Response Framework*, i.
45. The Department of Homeland Security, *National Incident Management System*, (Washington DC: Department of Homeland Security, 2008), http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf (accessed September 15, 2011), 12.
46. Federal Emergency Management Agency, *National Response Framework*, 1.
47. Ibid., 12.
48. The Homeland Security Council, *National Strategy for Homeland Security* (Washington DC: Homeland Security Council, 2007), http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf (accessed September 15, 2011), 4.
49. Burkett, "Command and Control of Military Forces," 132.
50. The Homeland Security Council, *National Strategy for Homeland Security,* 4.
51. Ibid.
52. Will Huhn, "The Posse Comitatus Act, The Insurrection Act, the Insurrection Act Rider, and the Lackawanna Six" (July 28, 2009), http://www.ohioverticals.com/blogs/akron_law_cafe/2009/07/the-posse-comitatus-act-the-insurrection-act-the-insurrection-act-rider-and-the-lackawanna-six (accessed December 27, 2011).
53. Brinkerhoff, "Posse Comitatus."

54. U.S. Congress, Committee on the Judiciary United States Senate, *The Insurrection Act Rider and State Control of the National Guard,* 110th Cong., 1st sess., April 24, 2007, 8.
55. Mcgrane, "A new exception to Posse Comitatus Act," 1319.
56. Owens, "Hurricane Katrina and the Future."
57. Lipton, Schmitt & Shanker, "Political Issues Snarled Plans for Troop Aid."
58. Mcgrane, "A new exception to Posse Comitatus Act," 1327.
59. T.A. Badger, "War prompts debate on military law/Posse Comitatus of 1878 bans use of troops for many actions on U.S. soil," November 11, 2011, *The Houston Chronicle*, http://www.chron.com/CDA/archives/archive.mpl/2001_3347917/war-prompts-debate-on-military-law-posse-comitatus.html (accessed December 23, 2011).
60. The White House, *The Federal Response to Hurricane Katrina,* 37.
61. Ibid.
62. Ibid.
63. Lipton, Schmitt & Shanker, "Political Issues Snarled Plans for Troop Aid."
64. Ludwig Schumacher, "Dual Status Command for No-Notice Events: Integrating the Military Response to Domestic Disasters," *Homeland Security Affairs,* volume 7, Article 4 (February 2011), http://www.hsaj.org/?article=7.1.4 (accessed on January 1, 2012), 2.
65. Department of the Army, *Civil Support Operations,* 6-2.
66. Schumacher, "Dual Status Command," 2.
67. Department of the Army, *Civil Support Operations* 3-18.
68. Ibid., 3-19.
69. The White House, *The Federal Response to Hurricane Katrina*, 43.
70. Schumacher, "Dual Status Command for No-Notice Events," 2.
71. Burkett, "Command and Control of Military Forces," 134.
72. Rupert Smith, *The Utility of Force* (New York, Vintage Books, 2007), 345.
73. Department of the Army, *Civil Support Operations,* 3-18.
74. Office of the Press Secretary, "Executive Order 13528-- Establishing Council of Governors," January 11, 2010 http://www.whitehouse.gov/the-press-office/president-obama-signs-executive-order-establishing-council-governors (accessed January 3, 2012).
75. Schumacher, "Dual Status Command for No-Notice Events," 4.
76. Ibid., 6.

77. "32 USC § 325 – Single Status," http://www.vahs.virginia.gov/Agencies/VMAC/docs/071410-meeting/Dual-Status.pdf (accessed January 4, 2012).
78. United States Northern Command Home Page, "Army North springs into action during Hurricane Irene" (August 31, 2011), http://www.northcom.mil/News/2011/083111.html (accessed November 21, 2011), 1.
79. Ibid., 2.
80. U.S. Joint Chiefs of Staff, *Joint Operations,* Joint Publication 3-0 (Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011), III-4.
81. Caroline R. Prosch, *Getting to One From Title 10+Title 32: Unity of Effort in the Homeland*, Naval Post Graduate School Thesis (Naval Post Graduate School, CA: September 2011), 33.
82. Steve Abbot, *Before Disaster Strikes: Imperatives for Enhancing Defense Support for Civil Authorities,* The Report of the Advisory Panel on Department of Defense Capabilities for Support of Civil Authorities After Certain Incidents, Introduction letter (RAND Corporation for the Department of Defense, September 15, 2010) http://www.rand.org/content/dam/rand/www/external/nsrd/DoD-CBRNE-Panel/Report-Advisory-Panel.pdf.
83. Ibid.
84. Ibid.

## The National Guard on the Southwest Border: Defining the Role

1. "Secretary Napolitano's remarks at the Center for Strategic and International Studies: Securing the Border: A Smarter Law Enforcement Approach," June 24, 2010, http://www.dhs.gov/ynews/speeches/sp_1277395237872.shtm (accessed October 4, 2011).
2. Although threats and shortfalls in capabilities and capacities exist on the U.S. Northern and coastal borders, the public and vocal concern is the Southwest border and is the focus of this paper.
3. Todd Steinmetz, "Mitigating the Exploitation of U.S. Borders by Jihadists and Criminal Organizations," *Journal of Strategic Security* 4, no. 3 (2011): 32.
4. United States House of Representatives Committee on Homeland Security, *A Line in the Sand: Confronting the Threat at the Southwest Border* (Washington, DC: 2006), 3-4.
5. U.S. Customs and Border Protection, Office of Border Patrol, *National Border Patrol Strategy* (Washington DC: U.S. Customs and Border Protection, 2005), 11.
6. Committee on Homeland Security, *A Line in the Sand*, 3.
7. U.S. Government Accountability Office, *Border Security: DHS Progress and Challenges in Securing the U.S. Southwest and Northern Borders* (Washington, DC: U.S. Government Accountability Office, March 2011), 5.

8. Ibid., 9.
9. U.S. Department of Justice, National Drug Intelligence Center, *National Drug Threat Assessment* (Johnstown, PA: U.S. Department of Justice, 2011), 2.
10. Ibid., 11.
11. Ibid., 2.
12. U.S. Department of Justice, National Criminal Justice Reference Service, *In the Spotlight*, https://www.ncjrs.gov/spotlight/gangs/summary.html (accessed December 12, 2011).
13. U.S. Department of Justice, *National Drug Threat Assessment*, 11.
14. Steinmetz, "Mitigating the Exploitation of U.S. Borders," 33.
15. U.S. Department of Justice, *National Drug Threat Assessment*, 11.
16. Ibid., 12.
17. Ibid., 2.
18. Committee on Homeland Security, *A Line in the Sand*, 2.
19. Ibid., 4.
20. Krisin M. Finklea, *Southwest Border Violence: Issues in Identifying and Measuring Spillover Violence* (Washington DC: U.S. Library of Congress, Congressional Research Service, August 25, 2011), 1.
21. U.S. Department of Justice, *National Drug Threat Assessment*, 7.
22. Steinmetz, "Mitigating the Exploitation of U.S. Borders," 32.
23. Ibid., 7.
24. Ibid., 4.
25. Committee on Homeland Security, *A Line in the Sand*, 4.
26. Ibid., 6.
27. Ibid., 27, 28.
28. U.S. Border Patrol Apprehension Statistics, Nationwide by Sector and Border Area, FY1999-2010 (December 6, 2011), www.cbp.gov/xp/cgov/border_security/border_patrol/usbp_statistics (accessed December 11, 2011).
29. Committee on Homeland Security, *A Line in the Sand*, 30.
30. Ibid., 29, 30.
31. Jim Miklaszewski and Michelle Acevedo, "U.S. ties Iran to plot to kill ambassador: Two men charged; Treasury Department ratchets up sanctions against Iran," *MSNBC* (October 11, 2011), http://www.msnbc.msn.com/id/44861178/ns/us_news-security/t/us-ties-iran-plot-kill-saudi-ambassador/#.Tu4VAtRWpUM (accessed December 17, 2011).

32. U.S. Government Accountability Office, "Alien Smuggling: Management and Operational Improvements Needed to Address Growing Problem," (Washington DC: U. S. Government Accountability Office, May 2000), 1.
33. Chelsea Schilling, "Foreign 'Terrorists' Breach U.S. Border: Illegals coming from Afghanistan, Iran, Egypt, Pakistan, Sudan, Syria, Yemen," *WND* (November 20, 2011), http://www.wnd.com/index.php?fa=PAGE.printable&pageId=156441 (accessed December 16, 2011).
34. U.S. Customs and Border Protection, *National Border Patrol Strategy*, 4.
35. George W. Bush, Speech at Yuma, Arizona Border Patrol Headquarters, May 18, 2006. http://immigration.procon.org/view.answers.php?questionID=000776 (accessed December 17, 2011).
36. U.S. Department of Homeland Security, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* (Washington DC, 2010), 1.
37. Ibid., vii.
38. Ibid., viii.
39. Jennifer E. Lake, *Department of Homeland Security: Consolidation of Border and Transportation Security Agencies* (Washington DC: U.S. Library of Congress, Congressional Research Service, May 22, 2003), 2.
40. U.S. Government Accountability Office, *Border Security: DHS Progress*, 1.
41. U.S. Customs and Border Protection, *National Border Patrol Strategy*, i.
42. Ibid.
43. Blas Nunez-Neto, *Border Security: Key Agencies and Their Missions* (Washington DC: U.S. Library of Congress, Congressional Research Service, May 13, 2008), 2.
44. Ibid.
45. U.S. Customs and Border Protection, *National Border Patrol Strategy*, 5-6.
46. Ibid., 7-11.
47. Chad C. Haddal, *Border Security: The Role of the U.S. Border Patrol* (Washington, DC: U.S. Library of Congress, Congressional Research Service, July 30, 2010), 2-3.
48. U.S. Government Accountability Office, "Border Patrol: Checkpoints Contribute to Border Patrol's Mission" (Washington, DC: U.S. Government Accountability Office, August 2009), 6.
49. Ibid., 6-10.
50. Ibid., 14.
51. U.S. Government Accountability Office, "Observations on the Costs of an Increased Department of Defense Role in Helping to Secure the Southwest

Land Border" (Washington DC: U.S. Government Accountability Office, September 2011), 3.

52. U.S. Government Accountability Office, *Border Security: DHS Progress*, 5.
53. U.S. Government Accountability Office, "Border Security: Preliminary Observations on Border Control Measures for the Southwest Border" (Washington DC: U.S. Government Accountability Office, February 2011), 5.
54. Ibid., 8.
55. Ibid., 7.
56. U.S. Government Accountability Office, *Border Security: DHS Progress*, 2.
57. Ibid., 10.
58. Ibid., 9.
59. "Obama Administration Announces Aug. 1 National Guard Deployment to Support Federal Law Enforcement Along Southwest Border," July 19, 2010, http://www.dhs.gov/ynews/releases/pr_1279557825445.shtm (accessed December 17, 2011).
60. Ibid.
61. Hugh Holub, "McCain, Kyl Introduce Enhanced Border Security Plan," April 18, 2011, http://tucsoncitizen.com/view-from-baja-arizona/2011/04/18/senators-kyl-and-mccain-propose-new-border-security-plan (accessed Dec-ember 17, 2011).
62. Ibid.
63. Colleen M. Kelley, "The National Treasury Employees Union letter to Senator Joseph Lieberman," September 19, 2011, http://www.dhsunion.org/Documents/Lieberman.pdf (accessed January 29, 2012).
64. Steinmetz, "Mitigating the Exploitation," 37.
65. U.S. Customs and Border Protection, *National Border Patrol Strategy*, i.
66. Chad C. Haddal, *Border Security: The Role of the U.S. Border Patrol* (Washington DC: U.S. Library of Congress, Congressional Research Service, March 3, 2010), 12.
67. Steinmetz, "Mitigating the Exploitation of U.S. Borders," 37.
68. U.S. Government Accountability Office, "Border Security: Preliminary Observations," 5.
69. Ibid., 2.
70. "Border Patrol History, Securing America's Borders" (January 5, 2010), http://www.cbp.gov/xp/cgov/border_security/border_patrol/border_patrol_ohs/history.xml (accessed October 20, 2011).

71. Timothy J. Dunn, *The Militarization of the U.S.-Mexico Border 1978–1992* (Austin, TX: The Center for Mexican-American Studies, University of Texas at Austin, 1996), 11.

72. Matt M. Matthews, OP22, *The U.S. Army on the Mexican Border: A Historical Perspective* (Ft. Leavenworth, KS: Combat Studies Institute, 2007), 78.

73. Dunn, *The Militarization of the U.S.-Mexico Border 1978-1992*, 106, 107.

74. Gerry J. Gilmore, "President Thanks National Guard for Helping Secure U.S. – Mexico Border" (April 9, 2007), http://www.ng.mil/news/archives/2007/04/040907-POTUS_thanks_guard.aspx (accessed October 21, 2011).

75. Michael D. Doubler, *Operation Jump Start: The National Guard on the Southwest Border, 2006-2008* (Doubler Enterprises and Issues Management Solutions, 2008), Forward by H. Steven Blum.

76. Ibid., v.

77. R. Chuck Mason, *Securing America's Borders: The Role of the Military* (Washington DC: U.S. Library of Congress, Congressional Research Service, June 16, 2010), 1.

78. Brian Montipoli, "National Guard Troops Deploying to U.S.-Mexico Border August 1st," July 19, 2011, http://www.cbsnews.com/8301-503544_162-20010952-503544.html (accessed December 17, 2011).

79. Mason, *Securing America's Borders: The Role of the Military*, 2.

80. Staff SGT Jim Greenwell, "National Guard Troops to deploy to Southwest border," June 24, 2010, http://www.army.mil/article/41314/National_Guard_troops_to_deploy_to_Southwest_border.html (accessed October 10, 2011).

81. Ibid.

82. U.S. Constitution, art. I, sec. 8.

83. Ibid., art. II, sec. 2.

84. Ibid., art. IV, sec. 4.

85. Posse Comitatus means "the power of the county," reflecting the inherent power of the old West county sheriff to call upon a posse of able-bodied men to supplement law enforcement assets and thereby maintain the peace. Following the Civil War, the Army was used extensively in the South to maintain civil order and enforce the policies of the Reconstruction era. However, in reaching those goals, the Army necessarily became involved in traditional police roles and in enforcing politically volatile Reconstruction-era policies. The stationing of federal troops at political events and polling places under the justification of maintaining domestic order became of increasing concern to Congress, which felt that the Army was becoming politicized and straying from its original national defense mission. The Posse Comitatus Act was passed to remove the Army from civilian law enforcement and to return it to its role of defending the borders of the United States. For a complete explanation of Posse Comitatus,

see Craig T. Trebilcock, *The Myth of Posse Comitatus*, October 2000, http://www.homelandsecurity.org/journal/articles/trebilcock.htm

86. "Posse Comitatus Act," 18 U.S.C., sec. 1385.

87. Mason, *Securing America's Borders: The Role of the Military*, 3.

88. "Restriction on direct participation by military personnel," 10 U.S.C., sec. 375, http://uscode.house.gov/download/pls/10C18.txt.

89. A "federalized" National Guard unit is one that has been mobilized under Title 10 of the United States Code to perform a federal mission. Command and control rests solely with the President and the federal government.

90. Mason, *Securing America's Borders: The Role of the Military*, 5.

91. Ibid.

92. Ibid.

93. Doubler, *Operation Jump Start: The National Guard on the Southwest Border, 2006-2008*,19.

94. In "state active duty," National Guard Personnel operate under the control of theirgovernor, are paid according to state law, and can perform activities authorized by state law.

95. Stephen R. Vina, *Border Security and Military Support: Legal Authorizations and Restrictions* (Washington DC: U.S. Library of Congress, Congressional Research Service, May 23, 2006), 3.

96. Ibid., 3.

97. Ibid., 4.

98. Ibid., 5.

99. Blas Nunez-Neto, "Immigration Related Border Security Legislation in the 109th Congress" (Washington DC: U.S. Library of Congress, Congressional Research Service, September 19, 2006), 6, 7.

100. Steinmetz, "Mitigating the Exploitation," 31.

101. Ibid., 32.

102. Criminal Activity and Violence Along the Southern Border: Hearing Before the Subcommittee on Investigations of the House Committee on Homeland Security, 109th Congress, (August 16, 2006), 47.

103. Committee on Homeland Security, *A Line in the Sand*, 23.

104. Ibid., 32.

105. Timothy J. Dunn and José Palafox, "Militarization of the Border", May 4, 2007, http://www.uua.org/documents/washingtonoffice/immigration/studyguides/handout4.1.pdf (accessed December 18, 2011).

106. Martin S. Rocha, "Militarizing Our Borders: Our New Immigration Policy," *The 'Lectric Law Library* (January 2, 1994), http://www.lectlaw.com/files/imm01.htm (accessed November 6, 2011).

107. "Should the U.S. Military Patrol the Border?" *ProCon.org* (February 5, 2009), http://immigration.procon.org/view.answers.php?questionID=000776 (accessed January 5, 2012).

108. Doubler, *Operation Jump Start: The National Guard on the Southwest Border, 2006-2008*, 72.

109. Colonel Ted Hildreth, U.S. Army National Guard Bureau, NGB-Mobilization Readiness Branch Chief, telephone interview by author, January 6, 2012.

110. Major General Raymond Carpenter, Acting Director Army National Guard, Small Group Lecture, Anton Myrer Army Leader Day (U.S. Army War College, Carlisle Barracks, PA, October 18, 2011), cited with permission of MG Carpenter.

111. Carpenter, e-mail message to author, November 14, 2011.

112. Hildreth, telephone interview, January 6, 2012.

113. Ibid.

114. "Securing America's Borders, Office of Air and Marine Overview," October 5, 2010, Customs and Border Protection website, http://www.cbp.gov/xp/cgov/border_security/air_marine/cbp_air_marine_overview.xml (accessed January 30, 2012).

115. Major Seth Lampton, U.S. Army National Guard Bureau, NGB-Mobilization Readiness, Executive Officer, e-mail message to author, January 6, 2012.

116. Graham H. Turbaville Jr., "US-Mexican Border Security: Civil Military Cooperation," *Military Review*, July-August 1999.

# Section Two
# Change Continues: Emerging Issues In Homeland Security

## Introduction


1. Shawn Reese, *Defining Homeland Security: Analysis and Congressional Considerations*, Congressional Research Service (January 28, 2013), http://www.fas.org/sgp/crs/homesec/R42462.pdf
2. Christopher Bellavita, "Changing Homeland Security: What is Homeland Security?" *Homeland Security Affairs Journal*, vol. IV, no. 2 (June 2008), http://www.hsaj.org/?article=4.2.1
3. James Jay Carafano, Ph.D., and David Heyman, *DHS 2.0: Rethinking the Department of Homeland Security*, Center for Strategic and International Studies and the Heritage Foundation (December 13, 2004), http://www.heritage.org/research/reports/2004/12/dhs-20-rethinking-the-department-of-homeland-security
4. James Jay Carafano, Ph.D., and David Heyman, *Homeland Security 3.0: Building a National Enterprise to Keep America Free, Safe and Prosperous*, Center for Strategic and International Studies and the Heritage Foundation (September 18, 2008), http://csis.org/files/media/csis/pubs/080918_homeland_sec_3dot0.pdf
5. Keith Bea, coordinator, *Federal Emergency Management Policy Changes After Hurricane Katrina: A Summary of Statutory Provisions*, Congressional Research Service (March 6,2007), http://www.fas.org/sgp/crs/homesec/RL33729.pdf
6. Carafano and Heyman, *Homeland Security 3.0*.
7. Federal Emergency Management Agency, http://www.fema.gov/whole-community
8. Federal Emergency Management Agency, http://www.fema.gov/preparedness-1/learn-about-presidential-policy-directive-8


## Ending the Military's Counternarcotics Mission


1. George H. W. Bush, "Speech Before Joint Session of Congress," (Washington DC, February 9, 1989), http://millercenter.org/president/speeches/detail/3420 (accessed March 25, 2012).
2. Government Accountability Office, "Drug Control: Status Report on DoD Support to Counternarcotics Activities" (Washington DC: U.S. Government Accountability Office, June 1991), 4.
3. Donald Mabry, "The U.S. Military and the War on Drugs in Latin America," *Journal of Interamerican Studies and World Affairs*, 30, no. 2/3 (Summer 1988): 57.

4. Peter Zirnite, "Reluctant Recruits – The U.S. Military and the War on Drugs," Washington Office on Latin America (Washington DC: August 1997), http://www.tni.org/sites/www.tni.org/files/download/Reluctant%20recruits%20report_0.pdf (accessed March 31, 2012).
5. George H. W. Bush, *National Security Directive 18: International Counternarcotics Strategy* (Washington DC: The White House, August 21, 1989), 1.
6. Government Accountability Office, "Drug Control: Status Report on DoD Support to Counternarcotics Activities" 12.
7. Zirnite, "Reluctant Recruits."
8. Bush, *National Security Directive 18*, 2-3.
9. U.S. Secretary of State James Baker, "Guidance on General Thurman's Visit," cable for U.S. Andean embassies (Washington DC, October 3, 1989, DTG 030025Z Oct 89).
10. "Pentagon Expands Mission of Military," *St. Louis Post-Dispatch*, September 19, 1989.
11. Ed Vulliamy, "Nixon's War on Drugs Began 40 Years Ago, and the Battle is Still Raging," *The Observer* (July 23, 2011), http://www.guardian.co.uk/society/2011/jul/24/war-on-drugs-40-years (accessed March 10, 2012).
12. Major Craig T. Trebelcock, USAR, "The Myth of Posse Comitatus," October 2000, http://www.homelandsecurity.org/journal/articles/trebilcock.htm (accessed January 9, 2012).
13. Brig. Gen. John S. Brown, U.S. Army Retired, "Historically Speaking: Border Security," *Army* (December 2007): 86.
14. U.S. Code Title 10, Chapter 18, Sections 371–373, http://www.law.cornell.edu/uscode/text/10/subtitle-A/part-I/chapter-18 (accessed November 9, 2011 and March 29, 2012).
15. Mabry, "The U.S. Military," 53.
16. Zirnite, "Reluctant Recruits."
17. David "Perera, "Cost of Military Deployments along the Southwestern Border Depend on Legal Authority, says GAO," *FierceHomelandSecurity.com*, http://www.fiercehomelandsecurity.com/story/cost-military-deployments-along-southwestern-border-depend-legal-authority-/2011-09-12 (accessed January 28, 2012).
18. Brown, "Historically Speaking," 85.
19. Douglas Stanglin, "Planes, Helos to Replace Guardsmen on Border," *Army Times*, http://www.armytimes.com/news/2011/12/gannett-planes-helos-to-replace-guardsmen-border-122111/ (accessed January 28, 2012).

20. Aliya Sternstein, "Military Surveillance Planes will Begin Patrolling the Southwest Border in January," *Nextgov.com* (December 20, 2011), http://www.nextgov.com/ nextgov/ng_20111220_8137.php (accessed on January 28, 2012).

21. Stanglin, "Planes, Helos to Replace Guardsmen on Border."

22. "Pentagon Weighs Use of Military on the Border," *MSNBC.com*, http://www.msnbc.msn.com/id/12748088/ns/us_news-security/t/pentagon-weighs-use-military-border (accessed March 20, 2012); Patrick Brady, "The Military and Border Security," *Military.com*, http://www.military.com/opinion/0,15202,214573,00.html (accessed March 20, 2012).

23. "Rick Perry Suggests U.S. Military Role in Mexico Drug War," *BBC News* (October 1, 2011), http://www.bbc.co.uk/news/world-latin-america-15140560 (accessed March 25, 2012).

24. U.S. Senators John McCain and Jon Kyl, "McCain, Kyl Announce Border Security Plan, 10-Point Plan to Better Secure the U.S.-Mexico Border in Arizona," Press Release (April 19, 2010), http://mccain.senate.gov/public/index.cfm?FuseAction=PressOffice.PressReleases&ContentRecord_id=18459278-ac95-e53d-0c3a-427b2010565f&Region_id=&Issue_id= (accessed March 24, 2012).

25. Sam Howe Verhovek, "No Charges Against Marine in Border Killing," *The New York Times* (August 15, 1997), http://www.nytimes.com/1997/08/15/us/no-charges-against-marine-in-border-killing.html (accessed November 15, 2011).

26. Deputy Assistant Secretary of Defense for Counternarcotics and Global Threats (DASD CN&GT), Special Operations/Low Intensity Conflict, Office of the Undersecretary of Defense for Policy, "DoD Counternarcotics Program" briefing slides (Washington DC, November 2011).

27. Ibid.

28. William R. Brownfield, "Is Merida Antiquated? Part Two: Updating U.S. Policy to Counter Threats of Insurgency and Narco-Terrorism," House Foreign Affairs Subcommittee on the Western Hemisphere and House Homeland Security Subcommittee on Oversight, Investigations and Management, October 4, 2011, http://www.state.gov/j/inl/rls/rm/175007.htm (accessed November 16, 2011).

29. "Mexico: Organised Crime Fight Drives Backlash," *OxResearch Daily Brief Service* (Oxford UK, August 2, 2011), 1.

30 "Mexican Drug Trafficking" *The New York Times*, (January 19, 2012), http://topics.nytimes.com/top/news/international/countriesandterritories/mexico/drug_trafficking/index.html (accessed March 24, 2012).

31. "One Killed Every Half Hour in Mexico Drug-Related Violence," *MSNBC.com*, January 12, 2012, http://worldnews.msnbc.msn.com/_news/2012/01/12/10138166-one-killed-every-half-hour-in-mexico-drug-related-violence (accessed March 24, 2012).

32. Ibid.
33. Barack Obama, "Chapter 6: Strengthen International Partnerships," in *2011 National Drug Control Strategy* (Washington DC: The White House, 2011), http://www.whitehouse.gov/ondcp/chapter-strengthen-international-partnerships#1 (accessed March 12, 2012).
34. Juan Carlos Llorca and Frank Bajak, "Mexican Drug Cartels Expand Abroad," *Associated Press* (July 21, 2009), http://www.blnz.com/news/2009/07/21/IMPACT_Mexican_drug_cartels_expand_1137.html (accessed March 24, 2012).
35. Bush, *National Security Directive 18*, 2.
36. Eva Bertram, Morris Blachman, Kenneth Sharpe, and Peter Andreas, *Drug War Politics: The Price of Denial* (Berkeley, California: University of California Press, 1996), 13.
37. Ibid.
38. James Q. Roberts, Principal Director for Special Operations and Counterterrorism, Special Operations/Low Intensity Conflict, Office of the Undersecretary of Defense for Policy, interview by author (Arlington VA: November 23, 2011).
39. Vulliamy, "Nixon's War on Drugs Began 40 Years Ago."
40. Government Accountability Office, "Drug Control: DoD Needs to Improve its Performance Measurement System to Better Manage and Oversee Its Counternarcotics Activities," Report to Congressional Committees (Washington DC: Government Accountability Office, July 2010), 35.
41. Deputy Assistant Secretary of Defense for Counternarcotics and Global Threats, *DoD Counternarcotics and Global Threats Strategy* (Washington DC: U.S. Department of Defense, April 27, 2011), 19.
42. Ibid., (emphasis added).
43. Interview with senior DoD official (November 28, 2011).
44. Ibid.; Steven I. Taylor, "Back to the Drug War: The Street Price of Cocaine," *Outside the Beltway*, May 16, 2010 http://www.outsidethebeltway.com/back_to_the_drug_war_the_ street_price_of_cocaine (accessed March 6, 2012).
45. United Nations Office on Drugs and Crime (UNODC), *World Drug Report 2011* (New York: United Nations, 2011), http://www.unodc.org/documents/data-and-analysis/WDR2011/World_Drug_Report_2011_ebook.pdf (accessed March 9, 2012), 81.
46. Ibid, 119.
47. U.S. Department of Justice, National Drug Intelligence Center, *National Drug Threat Assessment 2011* (Washington DC: U.S. Department of Justice, August 2011), 50.

48. Caryn Hollis, Principal Director for Counternarcotics and Global Threats, Special Operations/Low Intensity Conflict, Office of the Undersecretary of Defense for Policy, e-mail message to author, March 28, 2012.
49. Stanglin, "Planes, Helos to Replace Guardsmen on Border."
50. U.S. Department of Justice, National Drug Intelligence Center, *National Drug Threat Assessment 2011,* 50.
51. FY05-07 data, U.S. House of Representatives, "The Department of Defense's Counternarcotics Efforts," Staff Report Prepared for the Honorable Mark Souder, Chairman, Subcommittee on Criminal Justice, Drug Policy and Human Resources (December 2006), http://publicpolicypress.files.wordpress.com/2010/01/dod-counternarcotics.pdf (accessed March 24, 2012), 2; FY08-11 data, DASD CN& GT, "DoD Counternarcotics Program" briefing slides.
52. Barack Obama, *National Security Strategy 2010* (Washington DC: The White House, May 2010), 49.
53. Barack Obama, *Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security* (Washington DC: The White House, July 2011), 14.
54. Leon Panetta, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, DC: U.S. Department of Defense, January 2012), 5.
55. Ibid.
56. Ibid.
57. Barrack Obama, "State of the Union Address" (Washington DC, January 24, 2012).
58. James Clapper, "Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence," (Washington DC: Office of the Director of National Intelligence, January 31, 2012), 24.
59. Ibid.
60. Ioan Grillo, "US Troops Increase Aid to Mexico in Drug War," *National Public Radio*, http://www.npr.org/2011/10/06/141128178/u-s-troops-increase-aid-to-mexico-in-drug-war (accessed March 10, 2012).
61. Roberts Interview.
62. Paul Rexton Kan, "What We're Getting Wrong about Mexico," *Parameters* 41, no. 2 (Summer 2011): 37.
63. Malcolm Beith, "Are Mexico's Drug Cartels Terrorist Groups?" *Slate* (April 15, 2010), http://www.slate.com/articles/news_and_politics/foreigners/2010/04/are_mexicos_drug_cartels_terrorist_groups.html (accessed February 4, 2012).

64. Maggie Ybarra and Daniel Borrunda, "Mexico Attorney General: Juarez Explosion Not Narco-terrorism," *El Paso Times* (July 16, 2010), http://www.elpasotimes.com/ci_15531121 (accessed January 6, 2012).
65. Kan, "What We're Getting Wrong," 38.
66. Robert Valencia, "Mexican Drug Cartels Are Not Terrorists," *World Policy Blog* (October 26, 2011), http://www.worldpolicy.org/blog/2011/10/26/mexican-drug-cartels-are-not-terrorists (accessed February 4, 2012).
67. Elizabeth Harrington, "Republicans Propose Bill to Treat Mexican Drug Cartels as 'Terrorist Insurgency,'" *CNS News.com* (December 15, 2011), http://cnsnews.com/news/article/republicans-propose-bill-treat-mexican-drug-cartels-terrorist-insurgency (accessed March 25, 2012).
68. Ibid.
69. Mike Riggs, "Cartel Involvement in Failed Iranian Assassination Plot Fuels Push for Terrorist Designation," *Reason.com* (October 21, 2011), http://reason.com/archives/2011/10/21/cartel-involvement-in-failed-i (accessed March 25, 2012).
70. Jerry Markon and Karen DeYoung, "Iran Behind Alleged Terrorist Plot, US Says," *The Washington Post* (October 11, 2011), http://www.washingtonpost.com/world/national-security/iranian-charged-in-terror-plot/2011/10/11/gIQAiaYxcL_story.html (accessed March 25, 2012); Warren Richey, "US alleges Iranian Plot to Kill Saudi Ambassador: How It Unfolded," *Christian Science Monitor* (October 11, 2011), http://www.csmonitor.com/USA/Justice/2011/1011/US-alleges-Iranian-plot-to-kill-Saudi-ambassador-How-it-unfolded (accessed March 25, 2012).
71. Valencia, "Mexican Drug Cartels Are Not Terrorists."
72. U.S. Department of State, "Background Note: Colombia" (March 6, 2012), http://www.state.gov/r/pa/ei/bgn/35754.htm (accessed March 30, 2012).
73. Ibid.
74. Ibid.
75. Deputy Assistant Secretary of Defense for Counternarcotics and Global Threats (DASD CN&GT), *DoD Counternarcotics and Global Threats Strategy*, (Washington, DC: U.S. Department of Defense, April 27, 2011), 4.
76. John Rollins and Liana Sun Wyler, "International Terrorism and Transnational Crime," *Congressional Research Service* (March 28, 2010, R41004), http://assets.opencrs.com/rpts/R41004_20100318.pdf (accessed 25 March, 2012), 6.
77. Valencia, "Mexican Drug Cartels Are Not Terrorists"; "Rick Perry," *BBC*.
78. Barack Obama, *Strategy to Combat Transnational Organized Crime: Addressing Converging Threats to National Security* (Washington DC: The White House, July 2011), 15.
79. Obama, *National Drug Control Strategy 2011*, i.
80. Ibid, 15.

81. Ibid.

82. U.S. Department of Defense, "Defense Budget Priorities and Choices" (Washington DC: U.S. Department of Defense, January 2012), 3.

83. Panetta, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, 4-6.

## 21st Century Cyber Security: Legal Authorizaties and Requirements

1. Here the term "Federal" is used to specifically address whole-of-government as opposed to just the Department of Defense or Department of Homeland Security.

2. The United States Government Printing Office Home Page, http://www.gpoaccess.gov/uscode/about.html (accessed November 15, 2011).

3. Ibid.

4. 6 U.S.C. (Domestic Security), Chapter 1, governs the Department of Homeland Security; subchapter II describes DHS's role in information security and critical infrastructure protection.

5. U.S. Joint Chiefs of Staff, *Information Operations*, Joint Publication 3-13 (Washington DC: U.S. Joint Chiefs of Staff, February 13, 2006), I-1. The five warfighting domains are air, land, sea, space, and cyber. Of the five, only cyber is man-made and the domain is dependent upon man's continued, deliberate operation of systems and electromagnetic principles to exist.

6. Remote robotic networks (aka, "botnets" or "zombie army") are the result of several netted computers operating in concert toward an execution – or series of executions – designed by an outside entity without the computer owner/operator's involvement through corruption or usurpation of the computers' access to the network and operating system. Microsoft Corporation agrees with U.S. and NATO definitions of cyber activity of this nature, and their corporate home page offers the following commentary: "Criminals distribute malicious software (also known as malware) that can turn [a] computer into a bot (also known as a zombie). When this occurs, [the] computer can perform automated tasks over the Internet, without [the operator] knowing it. Criminals typically use bots to infect large numbers of computers. These computers form a network, or a *botnet*. Criminals use botnets to send out spam email messages, spread viruses, attack computers and servers, and commit other kinds of crime and fraud. If [a] computer becomes part of a botnet, [the] computer might slow down and [the host] might inadvertently be helping criminals." Microsoft Corporation Safety and Security Center Home Page, http://www.microsoft.com/security/resources/botnet-whatis.aspx (accessed February 12, 2012).

   The true danger of a botnet is that each infected or usurped computer has a traceable entry through the network, but it is figuratively impossible to determine which individual "zombie" is the actual source of the attack, which assumes one

of the attacking computers is, indeed, a source computer. Attack attribution is nearly impossible to determine.

7. Haly Laasme, "Estonia: Cyber Window into the Future of NATO," *Joint Force Quarterly*, 4th Quarter, October, 2011, 58-63.
8. Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian*, May 16, 2007.
9. Laasme, "Estonia: Cyber Window into the Future of NATO," 59.
10. Ibid.
11. Article IV, *North Atlantic Treaty*, http://www.nato.int/cps/en/natolive/official_texts_17120.htm (accessed November 19, 2011).
12. Laasme, "Estonia: Cyber Window into the Future of NATO," 60.
13. Ibid., 61.
14. Phil Stewart and Jim Wolf, "Old Worm Won't Die After 2008 Attack on Military," *Reuters* (June 16, 2011).
15. Ibid.
16. Malcolm Moore, "China's Global Cyber-espionage Network GhostNet Penetrates 103 Countries," *The Telegraph* (March 29, 2009).
17. Ellen Nakashima, "China, Russia Are Main Culprits in Cyberspying, US Agency Says," *Pittsburg Post Gazette* (November 4, 2011).
18. Barrack H. Obama, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World* (Washington, DC: The White House, May 2011), 11-14. Issued in 2011, this document addresses the basic problem scope for nations in today's cyberspace domain: diplomacy, defense, and development. The document articulates seven policy priorities which frame interagency and alliance-based operations rather than a compartmented strategy focused more on geography that the reality of the cyber domain.
19. Robert M. Gates, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: The Pentagon, July 2011), 5-7.
20. Obama, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World*, 10.
21. U.S. Government Accountability Office, Cyberspace: Report to Congressional Committees (Washington, DC: U.S. Government Accountability Office, July 2010), 30.
22. Arthur K. Cebrowski, "Transforming Transformation – Will it Change the Character of War?" May 25, 2004, http://www.au.af.mil/au/awc/awcgate/cia/nic2020/ceb_transformation25may04.pdf (accessed November 15, 2011), 11. See also Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," *U.S. Naval Institute Proceedings* 124, no. 1 (January 1998), 28–35.

23. Julian S. Corbett, *Some Principles of Maritime Strat*egy (New York: Longmans, Green and Co., 1911). Corbett advances the counter-Mahanian argument by stating a Fleet in Being can simultaneously protect trade as well as posture a combatant force along the enemy's sea lines of communication. This strategy, contrary to a singular large fleet existing solely to seek out and destroy the enemy fleet, provides the opportunity for the other elements of national power to be brought to bear and ultimately provide both means and ways to achieve the strategic ends.
24. Nakashima, "China, Russia Are Main Culprits in Cyberspying, U.S. Agency Says."
25. Certainly, organizations like the Defense Advanced Research Projects Agency (DARPA) and the various military department research organizations do, on occasion, "create" technologies or capabilities. The author's point is that the economic and technological base in America is in the hands of commercial corporations and not a nationalized or state-owned entity.
26. Nakashima, "China, Russia Are Main Culprits in Cyberspying, U.S. Agency Says."
27. Ibid.
28. Yaakov Katz, "Iran Embarks on $1B Cyberwarfare Program," *The Jerusalem Post*, December 18, 2011, http://www.jpost.com/Defense/Article.aspx?id=249864 (accessed December 20, 2011).
29. Lukas Milevski, "Stuxnet and Strategy: A Special Operation in Cyberspace?" *Joint Force Quarterly*, 4th Quarter (October, 2011), 64-69. The malicious code (actually a worm designed to target industrial systems and subvert them using a programmable logic controller rootkit) was publicly discovered in August 2010 when Siemans-produced SCADA systems became infected. Approximately 60% of the infected systems reside in Iran, and are employed to control uranium enrichment centrifuges. Out of an estimated 9,000 units, at least 1,000 and as many as 2,000 were destroyed as a result of the attack.
30. Kaspersky Labs, "Kaspersky Labs Provides Its Insight on Stuxnet Worm," *Kaspersky Labs Home Pag*e (September 24, 2010), http://www.kaspersky.com/about/news/virus/2010/Kaspersky_Lab_provides_its_insights_on_Stuxnet_worm (accessed December 20, 2011).
31. "The Stuxnet Outbreak: A Worm In The Centrifuge," *The Economist Newspaper Limited*, September 30, 2010, http://www.economist.com/node/17147818 (accessed December 20, 2011).
32. Dan Williams, "ANALYSIS: Wary of Naked Force, Israelis Eye Cyber War on Iran," *Reuters* (July 7, 2009).
33. Peter Beaumont, "Was Israeli Raid a Dry Run for Attack on Iran?" *The Observer* (September 15, 2007), http://www.guardian.co.uk/world/2007/sep/16/iran.israel (accessed December 20, 2011).

34. John Foley, "Pentagon Unveils Enterprise IT Strategy," *Information Week* Online (December 15, 2011), http://www.informationweek.com/news/government/policy/232300614 (accessed February 12, 2012).

35. J. Nicholas Hoover, "Feds Launch Shared Services Initiative," *Information Week* Online (December 13, 2011), http://www.informationweek.com/news/government/policy/232300440?itc=edit_in_body_cross (accessed February 12, 2012). As the article indicates, the Shared Services initiative by the new U.S. Chief Information Officer, Steven VanRoekel, may go a long way to trimming the cost of interdepartmental IT costs while simultaneously enhancing interoperability. While the DoD is still an insular player – in fact only the Army has formally signed up to a single DISA-managed email server, though the other Services may follow suit – other federal agencies are being driven toward collaboration on software suites, applications, and information management servers. The draft document "Federal Information Technology Shared Services Strategy" was released by VanRoekel's staff to all federal agencies for input on December 8, 2011, with a multi-phased approach and deadlines for initial collaboration as early as February and March of 2012. Whether this will become a viable IT Enterprise solution or merely a cost-cutting venture is yet to be seen.

36. Barrack H. Obama, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, DC: The White House, January 3, 2012), 3-5 & 8. In addition to the National Security Strategy, National Military Strategy, and the previously cited International Cyberspace Strategy, the President has released more detailed (and fiscally relevant) direction regarding Defense Strategic Guidance.

## U.S. Arctic Policy: Climate Change, UNCLOS and Strategic Opportunity

1. Heather Conley and Jamie Kraut, *U.S. Strategic Interests in the Arctic: An Assessment of Current Challenges and New Opportunities for Cooperation* (Washington DC, Center for Strategic and International Studies, April 2010), 2.

2. Ibid.

3. United States Government Accountability Office, *Report to Congressional Committees, Arctic Capabilities* (Washington DC: U.S. Government Accountability Office, January 2012), 4.

4. George W. Bush, *Unified Command Plan* (Washington DC: The White House, May 5, 2006).

5. Barack Obama, *Unified Command Plan* (Washington DC: The White House, April 2011).

6. Barack Obama, *National Security Strategy* (Washington DC: The White House, May 2010), 50.

7. George W. Bush, *National Security Presidential Directive (NSPD)-66/Homeland Security Directive (HSD)-25*, *Arctic Region Policy* (Washington DC: The White House, January 2009), sec. III-A.
8. Robert M. Gates, *Quadrennial Defense Review* (Washington DC: U.S. Department of Defense, February 2010), 86.
9. NSPD-66/HSD-25, sec. III-B-5.
10. *Quadrennial Defense Review*, 86.
11. Franklyn Griffiths, Rob Huebert, and P. Whitney Lackenbauer, *Canada and the Changing Arctic* (Waterloo, Ontario, Canada: Wilfrid Laurier University Press, 2011), 39.
12. U.S. Department of the Navy, *The Commander's Handbook on the Law of Naval Operations*, NWP 1-14M (Washington DC: U.S. Department of the Navy, July 2007), 1-3.
13. Scott G. Borgerson, *The National Interest and the Law of the Sea* (New York: Council on Foreign Relations, May 2009), 23.
14. Ibid.
15. Ibid., 10.
16. Ibid., 23.
17. Ibid.
18. "Testimony of Commandant Admiral Robert Papp, USCG, Defending U.S. Economic Interests in the Changing Arctic: Is There a Strategy?," *Targeted News Service* (July 2011), in ProQuest (accessed November 21, 2011).
19. U.S. Geological Survey, *Circum-Arctic Resource Appraisal: Estimates of Undiscovered Oil and Gas North of the Arctic Circle*, USGS Fact Sheet 2008-3049 (Menlo, CA: U.S. Geological Survey, 2008), http://pubs.usgs.gov/fs/2008/3049/fs2008-3049.pdf (accessed February 27, 2011).
20. Borgerson, *The National Interest and the Law of the Sea*, 28.
21. Ibid.
22. Ibid.
23. Ibid., 29.
24. Papp, "Defending U.S. Economic Interests in the Changing Arctic: Is There a Strategy?"
25. Griffiths, Huebert, and Lackenbauer, *Canada and the Changing Arctic*, 45.
26. NSPD-66/HSD-25, sec. III-D.
27. National Research Council of the National Academies, "Polar Icebreakers in a Changing World: An Assessment of U.S. Needs" (Washington, DC: The National Academies Press, 2007), 35.

28. Ibid.
29. Ibid.
30. Griffiths, Huebert, and Lackenbauer, *Canada and the Changing Arctic*, 20.
31. Dr. Jean-Paul Rodrigue, Dr. Theo Notteboom and Dr. Brian Slack, "The Geography of Transport Systems: Maritime Transportation," http://people.hofstra.edu/geotrans/eng/ch3en/conc3en/ch3c4en.html (accessed December 8, 2011).
32. National Research Council of the National Academies, "Polar Icebreakers in a Changing World: An Assessment of U.S. Needs," 35.
33. Andrew Kramer, "Warming Revives Dream of Sea Route in Russian Arctic," *The New York Times* (October 17, 2011), http://www.nytimes.com/2011/10/18/business/global/warming-revives-old-dream-of-sea-route-in-russian-arctic.html?pagewanted=all (accessed November 13,2011)
34. Commission of the European Communities, *Communication from the Commission to the European Parliament and the Council: The European Union and the Arctic Region*, Brussels, COM (2008), 9, quoted in Griffiths, Huebert, and Lackenbauer, *Canada and the Changing Arctic*, 48-49.
35. Linda Jakobson, "China Prepares for an ice-free Arctic" SIPRI Insights on Peace and Security No 2010/2, March 2010, 3.
36. National Research Council of the National Academies, "Polar Icebreakers in a Changing World: An Assessment of U.S. Needs," 59.
37. Papp, "Defending U.S. Economic Interests in the Changing Arctic: Is There a Strategy?"
38. Ibid.
39. Ronald O'Rourke, "Coast Guard Polar Icebreaker Modernization: Background, Issues and Options for Congress" (Washington, DC: U.S. Library of Congress, Congressional Research Service, November 3, 2011), 2.
40. Ibid., 4.
41. Ibid., 5.
42. Ibid.
43. U.S. Department of Defense, "Report to Congress on Arctic Operations and the Northwest Passage" (Washington DC: U.S. Department of Defense, May 2011), 27.
44. Ibid.
45. Ibid., 16.
46. Ibid.
47. U.S. Department of Defense, "Report to Congress on Arctic Operations and the Northwest Passage," 23.

48. United States Government Accountability Office, "Report to Congressional Committees, Arctic Capabilities," 8.
49. Testimony of Dr. Andrew Metzger, Senate Commerce, Science and Transportation Subcommittee on Oceans, Atmosphere, Fisheries, and Coast Guard Hearing, "Defending U.S. Economic Interests in the Changing Arctic: Is There a Strategy" (112th Cong., 1st sess., July 27, 2011), 50.
50. William Yardley, "Tanker With Crucial Fuel Delivery Is Sighted Off Nome," *The New York Times* (January 13, 2012), 1, http://www.nytimes.com/2012/01/14/us/fuel-tanker-renda-and-icebreaker-healy-are-sighted-off-nome.html (accessed February 1, 2012).
51. William Yardley, "A New Race Of Mercy To Nome, This Time Without Sled Dogs," *The New York Times* (January 13, 2012), 1, http://www.nytimes.com/2012/01/10/us/icebreaker-slowly-carves-path-for-tanker-to-bring-emergency-fuel-to-alaska.html?_r=1&scp=1&sq=nome&st=cse (accessed January 23, 2012).
52. Conley and Kraut, *U.S. Strategic Interests in the Arctic*, 13.
53. Ibid.
54. NSPD 66/HSPD 25, sec. III-C.
55. Griffiths, Huebert, and Lackenbauer, *Canada and the Changing Arctic*, 241.
56. Conley and Kraut, *U.S. Strategic Interests in the Arctic*, 13.
57. Ibid.
58. Ibid., 14.
59. U.S. Department of Defense, "Report to Congress on Arctic Operations and the Northwest Passage," 17-18.
60. Borgerson, *The National Interest and the Law of the Sea*, 37.
61. United States Government Accountability Office, *Report to Congressional Committees, Arctic Capabilities*, 35.

U.S. ARMY WAR COLLEGE

STRATEGIC STUDIES INSTITUTE

CENTER for STRATEGIC LEADERSHIP and DEVELOPMENT

U.S. ARMY WAR COLLEGE

PKSOI

# PARAMETERS

U.S. Army War College

# SLDR

Senior Leader Development and Resiliency

SCHOOL OF STRATEGIC LANDPOWER

U. S. Army War College

FOR THIS AND OTHER PUBLICATIONS, VISIT US AT

http://www.carlisle.army.mil/

CSLD

USAWC