

THREATS AT OUR THRESHOLD

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 21 OCT 2006		2. REPORT TYPE		3. DATES COVERED 00-00-2006 to 00-00-2006	
4. TITLE AND SUBTITLE Threats at Our Threshold				5a. CONTRACT NUMBER	
				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) U.S. Army War College, Carlisle Barracks, PA, 17013				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 Same as Report (SAR)	18. NUMBER OF PAGES 236	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			



THREATS AT OUR THRESHOLD

Homeland Defense and
Homeland Security in the
New Century

Edited by

Bert B. Tussing

THREATS AT OUR THRESHOLD
Homeland Defense and Homeland
Security in the New Century

A Compilation of the Proceedings of the
First Annual Homeland Defense and
Homeland Security Conference

Sponsored by:
Eisenhower National Security Series
Executive Agent:
United States Army War College

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

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

Contents

Foreword

vii

Chapter One

The Role of the Department of Defense in Responding to Catastrophe

Foreword

Professor Bert B. Tussing and Mr. Frank J. Cilluffo 1

Setting the Scene for a Discussion of DoD's Role in Responding to Catastrophe

Dr. David H. McIntyre and Professor Bert B. Tussing 9

DoD and the Problem of Mega-Catastrophes

Dr. Paul Stockton 21

DoD – Not the Department of Disaster

Colonel Richard Chavez and Professor Bert B. Tussing 33

Chapter Two

Do We Need a Goldwater-Nichols Equivalent for the Homeland?

Foreword

Mr. Frank J. Cilluffo 39

Goldwater-Nichols for the Executive Branch: Achieving Unity of Effort

Mr. Joel Bagnal 45

Goldwater-Nichols Act for Homeland Security

Colonel Michael Edwards 55

Is a Goldwater-Nichols Act Needed for Homeland Security?

Ms. Christine E. Wormuth 71

The Limits and Prospects of Military Analogies for Homeland Security: Goldwater-Nichols and Network-Centric Warfare

Mr. Daniel Prieto 85

Chapter Three

Creating a State and Local Preparedness Revolution

Foreword

Governor James S. Gilmore 111

Equipping the Army National Guard for the 21st Century

Ms. MacKenzie M. Eaglen 117

Transformation of the Reserve Component: Opportunity for Real Change

Ms. Christine E. Wormuth 129

Transformation of the Reserve Component

Mr. Peter Verga 143

Chapter Four

Finding the Enemy Within

Towards a Framework for Domestic Intelligence

Mr. David Heyman 149

Chapter Five

The Role of Information and Communication in Disaster Response

Foreword

Professor Dennis Murphy 175

The Role of Information and Communication in Disaster Response: An Overview

Professor Dennis Murphy 179

Hurricane Katrina: Communications & Infrastructure Impacts

Dr. Robert Miller 191

Public Communications: Vital Link to Maintaining the Public's Trust During Crisis

Mr. Michael Perini 205

Foreword

BERT B. TUSSING AND FRANK J. CILLUFFO

There is no more compelling issue to the government and people of the United States today than Homeland Security. Likewise, there is no more compelling mission for the military than Homeland Defense. But centuries of relative security for a people protected by two oceans and benevolent neighbors to the north and south have left us culturally ill-prepared for a new and ominous era of transnational terrorism that has brought danger to our door. Since the terrible wake-up call of 9/11, we have tried to overcome cultural malaise with institutional renovations, which has led to the greatest reorganization of government since 1947, a reexamination of the direction and focus of our intelligence community, and a renewed concern for domestic defense that has laid near dormant since the early 19th century.

In short order this has led to the development of the Department of Homeland Security, the Homeland Security Council, the United States Northern Command, the Office of the Assistant Secretary of Defense for Homeland Defense, a new Director for National Intelligence, the National Counterterrorism Center, two committees devoted to Homeland Security oversight in the United States Senate and House of Representatives, and a host of other institutional adjustments in the federal government. These changes were reflected and complemented by an equal commitment to renewal in our states, territories, and local governments, along with an essential commitment by much of the private sector to become active partners in the protection of the country's infrastructure.

A great deal has been done, but a great deal remains to be done. Issues of security must be continually pursued consistently with issues of individual liberties. The parallel commitments to law enforcement and defense must remain complementary, but distinct in a country who has never wanted its soldiers to be policemen or its police to be soldiers.

The balance of the federal application of power in a very federalist union, even in the name of support to state and local governments in times of crisis, must always remain in the forefront of our thinking, whether that support is extended from a civil entity or a uniformed contingent. Our institutions and our processes must be continually developed with these and other issues in mind. Similarly, as suggested by Secretary Chertoff in releasing his “Second Stage Review,” we must remain ready to adapt, as our enemy adapts.

In the spirit of these compelling commitments, the U.S. Army War College’s Center for Strategic Leadership, in partnership with The George Washington University’s Homeland Security Policy Institute, the Center for Strategic and International Studies, the Heritage Foundation, and the Association of the United States Army conducted what is envisioned to be the first of an annual Homeland Defense/Homeland Security conference under the sponsorship of the Eisenhower National Security Series. The event featured three guest speakers, Lieutenant General H. Steven Blum, the Honorable John Lehman, and Admiral James Loy, whose direct contributions to the cause of homeland security and homeland defense hardly need referencing. In addition, the forum convened five panel discussions, focused on vital issues surrounding the security of the country’s domestic environment, and the defense of her shores. This volume is a reflection of those discussions.

The first panel, sponsored by the Army War College, brought together three experts to address the question of whether or not the Department of Defense should ever be called upon to assume the position of “lead federal agency” in responding to a catastrophic event. The Department’s role in “support of civil authorities” is well-known, and has been played out on hundreds of occasions in responding to natural disasters from forest fires to floods, tornados to earthquakes, and—certainly, almost annually—hurricanes. But the devastation wrought by Hurricane Katrina rose to a new tier of destruction that overwhelmed not only state and local capabilities, but likewise the federal response in the earliest days of our efforts. Viewed against that background, and beneath the specter of a manmade threat that could wreak similar or even greater destruction, the question has been raised as to whether any agency

other than DoD has the manpower, transportation, communication and logistical wherewithal to effectively respond to catastrophes of this magnitude. Our panelists offered insights as to why DoD should take charge in these most extreme circumstances, and why not.

The second panel, convened by The George Washington University's Homeland Security Policy Institute, focused on the challenge of effectively coordinating homeland security and homeland defense efforts across the expanse of the federal government and beyond. In spite of the fact that the Department of Homeland Security (DHS) was established to bring together the preponderance of agencies nominally charged with homeland security issues, the federal effort that genuinely addresses those ends by far exceeds the boundaries of those 22 agencies housed at DHS. That diversity, characterized in institutional cultures as dissimilar as the Federal Bureau of Investigation and the Centers for Disease Control, has frequently resulted in bureaucratic friction that has no place in the face of the challenges surrounding the domestic security of our country. This friction is reminiscent to some of the less-than-smooth coordination that existed in our Armed Forces prior to the Goldwater-Nichols Act of 1986, the landmark legislation that forced a spirit of "jointness" on those forces that extended from their educational institutions, through their operational employment, on to the strategies that would sustain them and their mission. In that light, a call has gone forth for a "new Goldwater-Nichols," instilling a similar spirit of "jointness" not only in DHS, but throughout the interagency structure and in partnership with the State and local levels, to include both the private and nongovernmental sectors, and the citizenry as a whole. This panel examined the feasibility, advisability and desirability of such an effort, drawing from the DoD example, and acknowledging where that example cannot be applied.

Panel Three, sponsored by The Heritage Foundation, addressed the essential, and evolving role of the National Guard in Homeland Defense and Homeland Security. More than one official has referred to the National Guard as the military's first responders in times of domestic crisis. Theirs is a long and proud history of serving the citizenry from within the citizenry, and in recent times their soldiers have served as the first and last elements of the military's response to natural disaster.

Without question, the Guard will retain a central role in responding to disaster; but if that disaster becomes a deliberate, man-made variant, how will that role be affected? What mechanisms will be required to successfully integrate command and control of the Guard with their active component counterparts in response to a crisis in the homeland? What will be the nature of that relationship when significant numbers of a state's National Guard force become victims themselves; or when the scope of a catastrophe transcends state borders? And how will the Guard meet all of these challenges while fulfilling a role as the operational reserve to this country's current crises overseas? This panel addressed all of these issues, examining the precarious balance of an asset equally vital to the nation as a whole, and to its individual states and territories.

The Center for Strategic and International Studies sponsored the fourth panel, represented in this volume with a careful study of the intricacies surrounding domestic intelligence in a new era. No other entity in the United States government has undergone more scrutiny following 9-11, or attracted more blame, than the Intelligence Community. In the wake of that scrutiny, the community has been re-structured, resulting in the designation of a new Director of National Intelligence, the establishment of a National Counterterrorism Center, the re-tooling of an Office of the Assistant Secretary for Intelligence and Analysis in DHS, and numerous other changes and realignments. In spite of these changes, a significant challenge remains as the country seeks to steel itself from enemies 'without and within' while simultaneously preserving the rights and liberties of our citizens and those who reside lawfully within our shores. Insights drawn from the panel's discussions are reflected here in a paper provided by its moderator, David Heyman, Director and Senior Fellow of CSIS' Homeland Security Program.

The fifth and final panel of the forum was sponsored by the Association of the United States Army. In it the panelists devoted their attention to the growing importance of information and communication in responding to disaster. One of the most basic responsibilities a government has to its people in times of crises is to convey a sense of understanding of what has occurred, what is occurring, and what they can expect in continuing response and recovery operations. Left silent, the retention

of the public's confidence will remain an elusive, if not impossible goal, in spite of what the government has accomplished on their behalf. Balancing the public's "right to know" against security issues framed to protect that very public is a growing challenge, made more so by ubiquitous sources of information outside the government which are rightly beyond regulation, and too frequently beyond responsibility. Part of bridging the gap between the two sides of this quandary is a responsible press, brought in as partners against the disquieting void of information and the threat of disinformation. But the government itself must assume the primary responsibility for "putting out the word"—crafting and disseminating a consistent and clear message for the edification of the people. This panel focused on those challenges, our current means of meeting them, and the additional steps that may need to be taken in this critical aspect of retaining and sustaining the faith of our people in our institutions.

The conference was an ambitious endeavor, designed to draw on a cross-section of experience from the partner institutions, their supporters, and their audiences. Particular thanks go out to The George Washington University, whose staff and facilities provided an ideal environment for an inaugural event. The response to that event was enough to convince the coalition that the partnership should be preserved, and brought together annually for future examinations of vital issues surrounding the security of our country, within our country. Accordingly, in November of 2008, the partnership will convene again, this time on the campus of the United States Army War College.



Chapter One



*The Role of the Department of Defense in
Responding to Catastrophe*



Foreword

PROFESSOR BERT B. TUSSING

Director, Homeland Defense and Security Issues
The United States Army War College, Center for Strategic Leadership

On September 15, 2005, as we were just beginning to assimilate hard lessons surrounding our nation's response to the hurricane, President Bush declared in immediate hindsight that within the federal government only the Department of Defense (DoD) could effectively bring to bear the forces, resources and logistical expertise to respond to an event like Katrina. The hurricane had surpassed our traditional notions of "disaster" and entered into a whole new level of destruction that we were beginning to characterize as "catastrophic." As though paying testimony to the President's assertion, the Department of Homeland Security (DHS) (through the Federal Emergency Management Agency) had turned to DoD on September 1, 2005, and requested that they assume responsibility for logistics distribution functions, by conservative estimates amounting to a "billion dollar mission." Laid along side other support functions—from search and rescue, to support to law enforcement and beyond—an easy case could be developed for the commander of the U.S. Northern Command's assertion to law makers that active duty forces should be given complete authority for responding to catastrophic disasters.

Quickly following Admiral Keating's assertion, however, was one from another member of our uniformed leadership, Major General Timothy Lowenberg, the Adjutant General for the state of Washington. In a missive to his colleagues, General Lowenberg suggested that the Admiral's position amounted to a "policy of domestic regime change."

The purpose of this panel is to step away from immediate assertions and immediate responses to promote an understanding of a more

fundamental question: Should there ever be an occasion in which the DoD is the lead federal agency in responding to a catastrophic event?

Of course, before we can examine that notion, we must first come to grips with what we mean by “catastrophe.” The Catastrophic Incident Annex of the National Response Plan (NRP) attempts to help us by defining a “catastrophic incident:”

Any natural or manmade incident, including terrorism, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions.

A catastrophic event could result in sustained national impacts over a prolonged period of time; almost immediately exceeds resources normally available to state, local, tribal, and private-sector authorities in the impacted area; and significantly interrupts governmental operations and emergency services to such an extent that national security could be threatened.

The delineation between ‘disaster’ and ‘catastrophe’ is obviously designed to alert responding officials at all levels to another set of criteria, signaling another tier of destruction that may well call for procedures beyond the norm. And while the above definition is helpful, it is less than satisfying, because it doesn’t do much for us in identifying “trip wires” that will key a response or, in particular, an extraordinary response.

This, at least, begins our discussion on common ground, because no one on either side of the question would ever suggest that DoD would be considered as the lead federal agency in responding to a catastrophic event under anything other than extraordinary circumstances. Conventional wisdom holds that the NRP sufficiently meets response and recovery requirements following a major natural disaster in the vast majority of cases. The ‘tiered response’ envisioned in the NRP, envisioning a progressive introduction of local, state, and federal capabilities as each preceding tier is overwhelmed, has served the nation well on the average of 40-60 times a year following Presidential Disaster Declarations. In recent years through the course of that progression, DHS has been envisioned as the lead federal agency, not necessarily

“taking over” response and recovery operations from state control, but certainly leading the federal effort in support of that response.

Fairly or unfairly, Hurricane Katrina caused a number of observers to question that paradigm. Described by some officials as representative of “the low end of catastrophe,” Katrina nevertheless led first to questions of whether the federal government should take charge of response and recovery operations, and then whether there might be catastrophes at the “high end” that would outstrip DHS’ efforts to coordinate the federal response. The most frequently cited alternative, of course, postulated DoD assuming that lead.

The intent of this panel was to examine that alternative in terms of necessity, feasibility, and advisability. The three panelists undertaking that examination were imminently qualified to address it.

Dr. David H. McIntyre is the Director of the Integrative Center for Homeland Security at Texas A&M University, where he also teaches homeland security and terrorism at the Bush School for Government and Public Service and directs the graduate Certificate for Homeland Security program. A nationally recognized analyst, writer, and teacher specializing in homeland security, Dr. McIntyre is a 30 year Army veteran, who has been designing and teaching national and homeland security strategy at senior levels of government for 19 years. In 2001 Dr. McIntyre retired from the U.S. military as the Dean of Faculty at the National War College. During his eight years there, he taught strategy, operations, and interagency coordination, leading seminars through individual analysis, group exercises, and experiential learning. From 2001 and 2003, Dr. McIntyre served as Deputy Director of the ANSER Institute for Homeland Security, the nation’s only not-for-profit think tank focused solely on homeland security. In that capacity he contributed to dozens of conferences and exercises for audiences ranging from the leadership of the Department of Agriculture, to congressional staff members, to members of Washington DC universities and think tanks, to international visitors sponsored by the Department of State. He is a Fellow with George Washington University’s Homeland Security Policy Institute, and on the steering committee of the Homeland Security/Defense Education Consortium.

Dr. Paul Stockton is a Senior Research Scholar at Stanford University's Center for International Security and Cooperation. Prior to joining Stanford, Stockton served as Associate Provost of the Naval Postgraduate School in Monterey, California, and was the founder and Director of its Center for Homeland Defense and Security. Dr. Stockton's research has appeared in *Political Science Quarterly*, *International Security and Strategic Survey*. He is Co-Editor of *Reconstituting America's Defense: America's New National Security Strategy* (1992). Mr. Stockton has also published an Adelphi Paper and has contributed chapters to a number of books, including James Lindsay and Randall Ripley, Eds., *U.S. Foreign Policy After the Cold War* (1997). Mr. Stockton received a B.A. *summa cum laude* from Dartmouth College in 1976 and a Ph.D. in Government from Harvard University in 1986 after which time he served as a Legislative Assistant to US Senator Daniel Patrick Moynihan. Dr. Stockton was awarded a Postdoctoral Fellowship for 1989-1990 by the Center for International Security and Arms Control at Stanford University. In August 1990, Dr. Stockton joined the faculty of the Naval Postgraduate School where he served first as Director of the Center for Civil-Military Relations, and then as the Acting Dean of the School of International Graduate Studies. He was appointed Associate Provost in 2001.

Colonel Richard M. Chavez, United States Air Force, is currently assigned as Director, Civil Support in the Office of the Assistant Secretary of Defense for Homeland Defense. He leads a staff of senior military and civilian subject matter experts that develop and coordinate DoD strategic policy regarding civil support response operations with 32 Federal agencies, the Joint Staff, National Guard Bureau, Service component staffs, and DoD Agencies. Domestic support operations under Colonel Chavez' oversight include: Protection of the President, Military Assistance for Civil Disturbances, disaster mitigation, mission assurance, National Special Security Events/Special Events, Chemical, Biological, Radiological, Nuclear, and High Yield Explosive event response, and critical infrastructure protection. Colonel Chavez also executes oversight of DoD's policy for manning, equipping, training, and employment of DoD assets to include the National Guard's Weapons of Mass Destruction Civil Support Teams and the Services' Emergency Preparedness Liaison Officers. He is responsible for co-

ordinating requests for DoD assets from other federal departments and agencies for Secretary of Defense approval. Colonel Chavez' operational experience in the Air Force includes over 35 overseas deployments in support of operations around the world and three Squadron Commands on as many continents. He is a graduate of East Carolina University and holds Masters degrees from Golden Gate University (Public Administration) and the United States Air Force Air War College (National Security Strategy). Prior to assuming his current position, Colonel Chavez was Director, Department of Defense, Emergency Preparedness Course and Chief, Homeland Security Readiness Branch at United States Army Forces Command at Fort McPherson, Georgia.



Setting the Scene for a Discussion of DoD's Role in Responding to Catastrophe

DR. DAVID H. MCINTYRE

Director, Integrative Center for Homeland Security, Texas A&M University

PROFESSOR BERT B. TUSSING

Director, Homeland Defense and Security Issues
The United States Army War College, Center for Strategic Leadership

The intellectual development of homeland security is beginning to move outside the beltway and Washington D.C., past the issue of training firemen and other first responders, and into the realm of academia. We are finally beginning to engage the intelligencia of the United States, within the university system. This is going to change the nature of the debate, because these experts in research and teaching have things to say that you might not want to hear about what constitutes homeland security, and what we should or should not be doing.

This leads to a second point. I want to suggest to you a narrative – how to think about homeland security. I am certainly moved by 9/11. Many of my students are moved by 9/11. But my faculty, by and large, is not. It does not do me any good to begin with a slide that talks about 9/11. I have quit talking about the global war on terrorism. Many people in the Unites States are not moved by that argument. In fact, there is a certain counter or backfire building against this argument as to why we are at war and isn't it in fact our own fault. So, I use a different narrative to explain our situation. I offer it to every audience because I think it is important that we have a common understanding of what we are doing and why.

My first point is that the current problems of homeland security have nothing to do with whether or not there are Arab fundamentalist here and whether or not we are facing Islamic radicalism. It has everything

to do with the maturity of technology so that **small people now have access to big weapons**. Timothy McVeigh was only the opening shot in this new world. All over this nation today, you can do in a really good high school lab DNA experiments that could not have been done by Soviet bio-weapons experts twenty five years ago. The FBI spent seventeen years chasing the Unabomber, and in my lifetime I fear the FBI will have to chase the Unageneticist. Dramatic new threats that result from a dramatic new flow of information are coming, so whether you like the concept or not, whether you consider terrorism a valid cause for an overseas war or not, we have to rethink the structure of homeland security, potential disasters and potential catastrophes within the United States. I will tell you, the audiences I speak to resonate with this message much better than they resonate with an opening picture of the Twin Towers.

Secondly, beyond that, it is important to realize that **we do have an enemy**. I think MI5 did the right thing in stepping out to arrest plotters in London recently, before they could put their plans into action. I wish our FBI and the Department of Justice would step out and say what they are seeing, what have they encountered, what kind of radical groups they are tracking in the United States—and whether they see a real threat or not. You cannot simply collect all the information, say, “It is classified, trust me....There is a threat, but it will be OK.,” and expect the American people to just come along.

Thirdly, we need to understand that **we are up against a new type of terrorism**. I speak over and over to terrorism workshops, terrorism seminars, and terrorism faculties. I am sure I will offend some people, but it’s part of my job as an academic. I will tell you that people who were working hard in the subject of terrorism prior to 9/11, are frequently less useful on the subject than they could be because they are locked onto a vision shaped two decades ago. They want to talk about “Shining Path,” they want to talk about the “Red Brigade” or they want to talk about the fundamentals of terrorism of 20 years ago. Today we see a different approach to terrorism—a different way of thinking by terrorists. The father of my best friend in elementary school was a copilot when the first aircraft was hijacked from the United States. What he was told was “Give up the airplane.” That was the rule for pilots for

40 years—because terrorists mainly just wanted publicity. No more. It's a different form of terrorism. This group is out for large numbers of casualties—no alternatives, no negotiations. These are not my words. These are from the 9/11 Commission.

Finally, technology and history have produced **new vulnerabilities within the United States**. This brings us to the issue of disasters and catastrophes. We are a “just-in-time” society now. There was a time about twenty years ago, before deregulation for example, when you drove down the road and saw big storage tanks of gasoline, diesel and fuel—there was a time when there was somewhere between 21 and 24 days of fuel available in those tanks on any given day. That's gone because of deregulation and just in time delivery. Today, those tanks are holding about eleven days of fuel and the bottom four days are not usable because they are required to keep the tanks erect. So, the flexibility, the structure of the United States, is much more fragile than it was twenty years ago because of movement in industry.

Expectations have also changed in the United States. When Hurricane Carla blew ashore and went over Texas when I was young, nobody expected the school bus to show up with a cooler of ice from the federal government to carry us out of the storm. We thought we were on our own. Today, people expect that support, and they expect it right away. It's been reported now that in the state of Florida people line up as soon as the storm is over looking for free ice—when it's for sale across the street. There are different expectations, and it is going to affect the way we respond to a catastrophe.

Lastly, in case you haven't heard it at some other conference, there is a growing division within the homeland security community over whether we need to be focused on prevention and protection (as suggested by those who approach this from a security perspective, worried about terrorism), or mitigation (the more traditional approach of civil defense, the Federal Emergency Management Agency [FEMA], and emergency management). There is a growing split about who should be in charge and how the money should be spent, or what we should be doing to prepare for catastrophes and disasters. Those two groups are building different parallel intellectual universes, and it is important to understand this.

This brings me to my most important scene setting point. We could lose this fight!

I understand and applaud the comments about the impact the National Guard is having with its deployments overseas, how we set a different standard for the world when we show up and take the fabric for America into foreign countries. But if you haven't noticed lately, the correlation of forces is not moving in our direction. In spite of what we did to win friends during the earthquakes in Pakistan three years ago, the tribal areas are not lining up on our side today. They are lining up against us. People are selecting the Taliban today. Think about that! So what I would suggest to you is that we've got a problem for the foreseeable future, and we need to be serious about what is going to happen in the United States.

Now by losing, I do not mean that Osama Bin Laden shows up on Independence Avenue with a flag and takes control of the White House. What I mean are the ways in which the modern world could unwrap—costing us friends, markets, and national power. Eventually what we could see is the loss of the character of the modern world, which I would define as the free flow of people, things and ideas across borders. This is already happening.

When I was the dean at the National War College, we took students to travel during the year all over the world—from the southern Philippines, to the Malaysian Peninsula—down south of Jakarta to the tea plantations—just a load of American government employees in civilian clothes in a van. I don't see how you can do that safely anymore. The world is closing down to American business. We have got a problem we need to address.

So, with those two scene setters—the new world in which we live, and the fact that we could lose this war—let me articulate what you already know, so we can put it in some sort of framework where we can discuss it reasonably and rationally. On the left hand side of the chart depicted in figure 1 (opposite page), I talk about what I see as the types of disasters – yes **CBRNE** (Chemical, Biological, Radiological, Nuclear, Explosive), but other things as well:

- First, though, by **explosives**. I don't just mean an explosion, but extremely powerful explosives, or a campaign of explosions.
- We need to include **Cyber**, which we rarely mention because we are not sure the military can really address it in the homeland—but from a homeland security perspective we have to think about it.
- **EMP** (electromagnetic Pulse), which I think achieved respectability with congressional hearings about two years ago, but we don't talk much about because we are not sure what to do.
- And then finally, **natural disasters** which fall into categories of the normal storm, mega storm and then the earthquake and volcanic eruption.

Across the top of the chart, I would suggest, is the way the Department of Homeland Security (DHS) talks and thinks about responding to these disasters: mitigation from the emergency response community, then prevention, protection, response and recovery.

Let me tell you, I find **definitions** still in motion. Just because there is a definition in the book doesn't mean we are using it. The definition of homeland security which resides in the National Strategy published

Some basic concepts

Types of Disasters

	Preparedness: The ability to...				
	Mitigation	Prevent	Protect	Respond	Recover
Chemical					
Biological					
Radiological					
Nuclear					
Explosive					
Cyber					
EMP					
Natural					

Mitigation: Actions taken to reduce the effects of future disasters.

Figure 1: Some Basic Concepts

in 2002 has no mention of natural disasters, so I am not sure that is an operable definition anymore.

In the same respect, I am not sure there is a clear definition of **mitigation** in the National Response Plan. I would suggest that it is “those actions taken to reduce the effects of future disasters and future catastrophes.” For that reason, I would take mitigation out of the realm of DoD, because—until something happens—I am not sure DoD ought to be in the business of directing mitigation. That is a civilian function except (possibly) in support of some areas.

Additionally, the definition of **preparedness**, I think, has been changing over the past eighteen months. Today, George Foresman is suggesting that Preparedness is not a specific duty for just a particular group. He says FEMA for a long time didn’t have preparedness for a mission. Now he says they do have preparedness as a mission. I would suggest that preparedness means getting ready to do all four required homeland security actions: prevent, protect, respond and recover. Preparedness permeates every phase. For example, members of the business community in Galveston learned from last year’s storm that they should be pre-qualifying for loans before disaster strikes. That’s a form of preparedness—preparing to recover, where previously we thought of preparedness as “preparing for the blow.”

Concerning the evolving **DoD role**—let me lay it out. I am sure you all read the DoD strategy and know it, but we need to refer to it here to establish the framework for the future discussions. The DoD role according to the strategy published in July, 2005 really falls into two areas:

- **Homeland Defense** in which the military (actually DoD), takes the lead. This is under extraordinary circumstances when the actual defense of the homeland is in question.
- And secondly, **Homeland Security**—denoting issues where DoD is in support and not in the lead. Increasingly, we are seeing all those actions that fall into the area of homeland security referred to as Defense Support to Civil Authorities.

You can’t really address this subject if you don’t have a clear understanding how the **National Guard** works on a daily basis for the governors; of

what Title 32 status means (that the Guard still works for the governor, but the federal government pays for it), or of Title 10 status (when the governor loses control of his Guard forces). By the way, this is why we had a conflict in Katrina when the governor refused to relinquish control of her Guard and it remained on the scene, but outside the control of the President of the United States.

Lastly, to understand the evolving DoD role, you have to at least have a brief background understanding of **Posse Comitatus**. This 19th century law generally forbids using the military for law enforcement purposes – with some important exceptions. The law was originally focused on the Army, but the Air Force was included by extension when DoD was formed in 1947. And the Navy and Marines are covered (and restricted) by DoD regulations. Of course, as most of you know well, there are lots of exceptions to these laws, so I do not view this as a huge barrier to the use of DoD forces for homeland security. Perhaps some of our other panels will discuss this issue.

Depicted in figure 2 is DoD's definition of Defense Support to Civil Authority. I will point out that there are three operational missions:

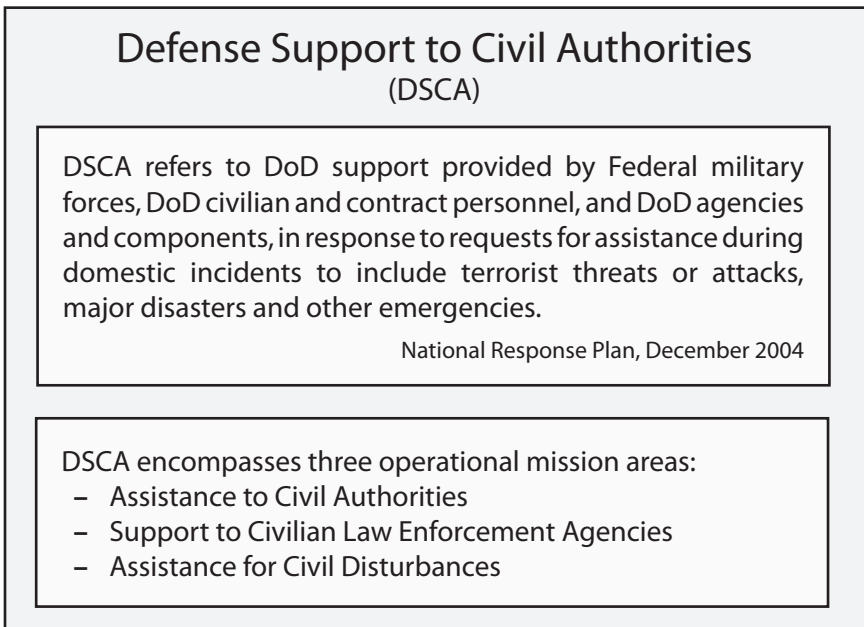


Figure 2: Defense Support to Civil Authority

assistance to civil authorities, support to a civilian law enforcement agency, and assistance for civil disturbances.

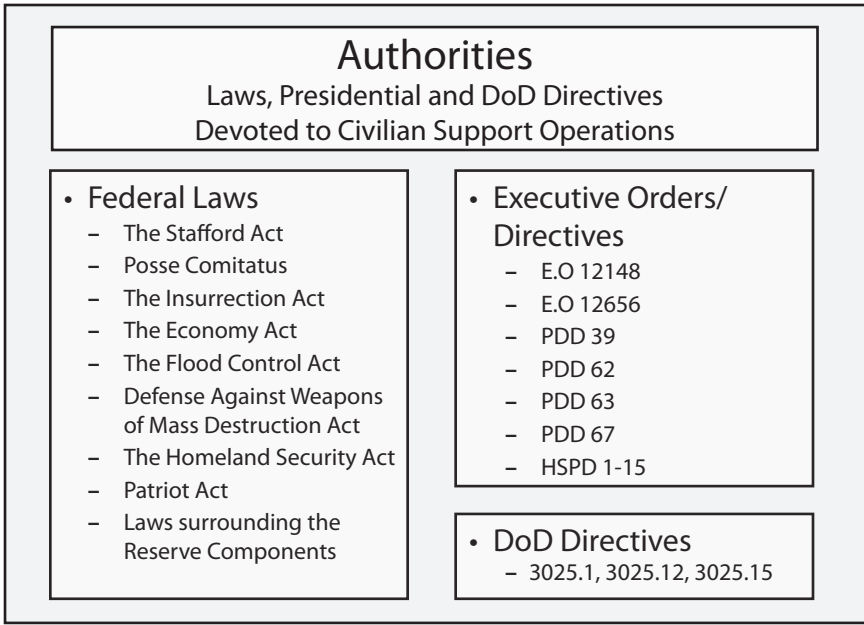


Figure 3: The Authorizations for DoD Support to Civil Authorities

Listed in figure 3 are the authorities you may wish to go to for research to see exactly what DoD is allowed to do or required to do under laws concerning disasters or catastrophes.

Now, as for the basic concepts. Out of this basic range of missions, what I hope you're seeing is that "all-hazards" is a great way to prepare firemen, but I not necessarily a great way to prepare strategies. If you look across all these matrices on figure 4 (opposite page), you will see that different people do have different roles according to whether we are preventing, protecting or responding, and according to whether the crises is biological, or chemical, or explosive in nature. Different groups are involved for these different events, and they take different actions, so while I understand and like the idea of trying to build a central framework, it's not a case of "one size fits all." In fact I'd say there are some things we could take off the table in our discussion of the role of DoD:

Some basic concepts

Role of the Military in Disasters

& Preparedness

	Mitigation	Prevent	Protect	Respond	Recover
Chemical	X	X	X	✓	✓
Biological	X	X	X	✓	✓
Radiological	X	X	X	✓	✓
Nuclear	X	X	X	✓	✓
Explosive	X	X	X	✓	✓
Cyber	X	X	X	✓	✓
EMP	X	X	X	✓	✓
Natural	X	X	X	✓	✓

X = Not DSCA . . . By definition

Figure 4: The Military's Role and Non-Role in Disaster Response

- **Mitigation**, for example, is somebody else's job—DoD does not do this for anyone but DoD.
- We **Prevent** overseas, but I don't see a big role of DoD preventing at home, except perhaps in the contribution of some intelligence.
- **Protecting** is an interesting point, because it seems to me that DoD may have a role in protecting some point targets—especially those that support the defense industrial base. But for those cases that are not point targets, it's hard for me to conceive how DoD is going to have a protection role in the U.S. as a whole.
- The DoD role in **Response and Recovery** is somewhat case specific. For example against biological threats, DoD might have a very strong role.

So the question for DoD will be: lead or follow in a catastrophe? What can the military do? It can apply its broad range of capabilities to include intellectual capabilities, and especially planning. I think this is an area

where DoD has really stepped up to contribute, both in developing plans and developing organizations culturally. But these should be temporary responsibilities—DoD does not want the permanent job of planning and the permanent job of shaping the culture of DHS.

The most important thing DoD must do, I believe, is balance the need to stop of loss of life and property, while protecting the nation's centers of gravity. I don't think this idea is an easy sell, especially to a military officer, but we do have centers of gravity—like the economy, the legitimacy with which our people regard the federal government, and the ability to project power overseas. We have to think about balancing what we can do at home with maintaining those centers of gravity.

Then finally, we have to recognize there are some things we will do. There are simple realities about life for a great power. For example, the reality is that politicians in a crisis are likely to turn to the first organized group they can find that has the culture and the capability to get something done. This happens to the U.S. Coast Guard all the time. So those in DoD better plan for this reality, whether you like it or not.

One last point I am going to raise because it is important: there a difference between a *catastrophe* and a *disaster*.

There are some definitions on the street, but I don't see those definitions being couched in useful language. There is a difference. What we had in New Orleans was not a disaster, it was a catastrophe. The difference is not just scale or loss of life—because we had the same scale of destruction right down the coast line in Mississippi. But, I am not sure we had the same catastrophe.

It seems to me the difference may reside with the ability of traditional government agencies to exercise their authority, and exercise their traditional functions. So, that takes the discussion a little different direction, if we say, "Let's look at those same potential threats, let's look at those same potential responsibilities, let's look at those same military roles" and ask, "Is there a difference between *a disaster when we are clearly in support*, and *a catastrophe when there may be no local government?*" This, I think, is a very serious and important question.

And the key for DoD in the future is going to be, “How do we balance traditional international responsibilities with protecting centers of gravity within the U.S.?” My concern is our loss of balance, either over reacting and putting too much time and effort into this field, or under reacting and being unprepared when we are called on domestically.

My last point when I give my narrative of why we have to face the challenge of homeland security up front—the reason that universities and the rest of the United States have to be involved—is **not** that we can lose, but that **we can win**. If we do this right, we can reshape how government and industry serve the people of the United States, and reinvigorate local patriotism and involvement in government. I am seeing this with students on the university campus. They are signing up to take our homeland security courses. The question is whether our leaders and our bureaucrats are as committed to our security at home as are our rank and file. They can win, if we give them the intellectual tools they need.



DoD and the Problem of Mega-Catastrophes

DR. PAUL STOCKTON

Center for International Security, Stanford University

The organizers of this conference made a strange choice in selecting me to advance the argument that the Department of Defense (DoD) ought to take the lead role in responding to catastrophes. For the overwhelming majority of incidents that may confront the U.S. response system in the future, I believe that the current, civilian-led system is structurally sound (and in many respects, ideal). The same civilian-led system also provides the best framework for building the sort of response system necessary for what I will call “normal catastrophes”—that is, catastrophes on the scale of Hurricane Katrina. But the United States should plan for the unlikely possibility that a catastrophe of a vastly larger scale may strike. In such a “mega-catastrophe,” DoD will face unwanted but ineluctable pressures to temporarily assume the lead of U.S. response operations. That is not a particularly desirable thing. Still worse, however, is the prospect that DoD would take the lead without having planned for the challenges it will confront, including the imperative to return leadership responsibilities to civilian officials as rapidly and effectively as possible.

My argument is built around a typology of very bad events, ordered in terms of their destructiveness: 1) major disasters (as defined in the Robert T. Stafford Disaster Relief and Emergency Assistance Act); 2) normal catastrophes (as defined by the National Response Plan and its Catastrophic Incident Annex); and 3) mega-catastrophes, which differ qualitatively from normal catastrophes in ways that will require a different architecture for the response system, and a different role for DoD.

I will begin by examining why a subordinate role for the DoD is so appropriate in major disasters. Second, I will distinguish disasters from

normal, Katrina-scale catastrophes, and reassess the degree to which keeping DoD in support of civilian authorities makes sense for such events. The third section examines how mega-catastrophes differ from normal ones, and why those differences make it imperative that the DoD plan for the very low probability, very high consequence risk that the President will assign leadership responsibilities to DoD for response. That section will also explore the problems that are likely to ensue if the Department adopts an ostrich-like approach to the leadership challenges posed by mega-catastrophes, and is left instead to make politically sensitive policy and organizational decisions on the fly.

Incidents, Major Disasters and Presidentially Declared Emergencies: The Virtues of the Bottom-Up System

The Federal government plays little or no role in the vast majority of fires, floods and other incidents that occur in the United States each year. Instead, local and state governments are primarily responsible for dealing with such incidents. The “basic premise” of the U.S. National Response Plan, which lays out the structure of the U.S. response system, is that “incidents are generally handled at the lowest jurisdictional level possible.”¹ Only if local and state resources are overwhelmed will authorities turn to interstate mutual aid compacts for additional assistance, and then—if necessary—the federal government.

The Robert T. Stafford Disaster Relief and Emergency Assistance Act specifies the circumstances under which most forms of Federal assistance flow to states and localities.² Even before a president declares that a disaster has occurred, a governor may request that the president direct DoD, the Department of Homeland Security (DHS), and other federal departments to commit resources to preserve life and property in an incident.³ The more typical trip-wire for federal assistance lies in the designation of an incident as a major disaster. The Stafford Act specifies

1. National Response Plan, 4 December 2004 (U.S. Department of Homeland Security): 10.
2. For a concise description of the Stafford Act and the flow of Federal resources for which it provides, see “Federal Stafford Act Disaster Assistance: Presidential Declarations, Eligible Activities, and Funding” (Congressional Research Service, 28 April 2006), especially pp. 2-6.
3. Federal Stafford Act: 2.

that in response to a request for aid from a governor, a president may declare that an incident is a major disaster when it stems from a hazard such as hurricanes, tornados, or other natural hazards or, “regardless of cause, [after a] fire, flood or explosion.”⁴ The Act also specifies the destructive impact that an incident must have before it can be eligible to be declared a major disaster.⁵ The Act also provides that the president can declare that an event is an “emergency” and provide assistance even if a governor has not yet requested aid (and gives the president enormous leeway in determining whether an emergency exists).

The Stafford Act does provide an exception to the specifies in that a president can exercise the authority over response operations he deems necessary when “primary responsibility for the response rests with the United States because the emergency involves a subject area for which, under the Constitution or laws of the United States, the United States exercises exclusive or preminent responsibility and authority.” But the president has never invoked such authority for a major disaster.

More typically, federal aid flows to state and local authorities in major disasters to supplement their own capabilities, and in accordance with the assistance priorities those authorities have laid out. The critical role that state and local authorities play in requesting federal assistance and specifying the nature of that aid leads some observers to characterize the resulting process as “demand pull”—that is, one driven by the demands of state and local officials. I prefer the term “bottom-up,” because that term reflects not only the process by which requests for assistance flow, but also the degree to which state and local agencies provide the foundation on which the remainder of the response system rests.

Four factors help make the resulting response system so effective in most disasters. First, because the system is structured to function in a “bottom-up” process, in which local and state officials drive the initial response process, the system can take advantage of the familiarity that local officials have with their particular circumstances and operational constraints. Second, under the National Incident Management System (NIMS), that is designed to guide U.S. response operations, those local

4. 42 U.S.C. 5122(2).

5. For the specific criteria used in determining wither an incident constitutes a major disaster, see 44 CFR 206.48.

and state officials who direct initial response operations continue to help determine assistance priorities if their local capabilities prove inadequate.⁶ That not only keeps the system tied to an on-the-ground assessment of assistance needs but also provides a scalable command and control architecture that provides for interoperability among disparate local, state and federal entities as a disaster grows. Third, the mechanisms for mutual aid that supplements the bottom-up system provides for efficient utilization of resources. Mutual aid obviates the need for each state to build and maintain the capabilities necessary to deal with unusually destructive disasters. Through the Emergency Management Assistance Compact (EMAC) system, states stand ready to supplement each other's capabilities in a fashion that for decades has proven increasingly effective and efficient for disaster response.

Mechanisms to provide for more federal-heavy, top-down disaster response efforts do exist, however. Incidents caused by acts of terrorism automatically elicit the involvement of the Department of Justice (and especially the Federal Bureau of Investigation) in criminal justice and terrorism prevention-related activities during response operations, such as the preservation of evidence at the incident scene. The Stafford Act also provides for larger-scale federal response operations. The Act specifies that the president can exercise those authorities over response operations he deems necessary when "primary responsibility for the response rests with the United States because the emergency involves a subject area for which, under the constitution or laws of the United States, the United States exercises exclusive or preeminent responsibility and authority."⁷

A prime example of preeminent federal authority – and one of special importance to this article—lies in the realm of homeland defense. The DoD's *Strategy for Homeland Defense and Civil Support* specifies that under most circumstances, disaster response activities will go forward within the category of homeland security—that is, under the purview of DHS. Through an amended Executive Order, President George W. Bush assigned responsibility of administering most of the provisions of

6. National Incident Management System (Department of Homeland Security, 1 March 2004).

7. Robert T. Stafford Disaster Relieve and Emergency Assistance Act. 42 U.S.C.5191(b).

the Stafford Act to the Secretary of DHS. DoD provides support to the Secretary of DHS and other civilian authorities as directed by the president (and as provided for in the Emergency Support Functions specified by the National Response Plan). But the Strategy also reserves for DoD the lead role in providing for Homeland Defense. Homeland Defense is the “protection of U.S. sovereignty, territory, domestic population and critical defense infrastructure against external threats and aggression, or other threats as directed by the President.”⁸ To reiterate, the DoD is responsible for homeland defense.

This definition of homeland defense creates an exception to the primacy of DHS (and state and local authorities) through which a president could drive an armored division. At the operational level, the ability of DoD to fit into the NIMS command system that is becoming so deeply ingrained in state and local agencies is at issue. The DoD has yet to adopt NIMS as its source of guidance for response operations (and may never do so, preferring to stick to its own military-oriented command and control arrangements). The distinction between homeland defense and homeland security creates some potential puzzles in terms of “who would be in charge of what” in disaster response – especially if (as in the case of bio-terrorism) it might not be immediately clear whether an event stemmed from natural causes or natural hazards. The short answer to questions over who is in charge will always be “whoever the president wants,” under the wide latitude for presidential decision-making that the Stafford Act provides. But as we move up the ladder of destruction from major disasters to catastrophes, that latitude (and the associated uncertainties for planning response operations) becomes increasingly problematic.

Normal Catastrophes: No Need for DoD Leadership

The National Response Plan (NRP) defines a catastrophe as:

Any natural or manmade incident, including terrorism, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions. A catastrophic event could result in sustained national impact

8. The Strategy for Homeland Defense and Civil Support (U.S. Department of Defense, June 2005): 5.

*over a prolonged period of time; almost immediately exceeds the resources normally available to State, local, tribal and private-sector authorities in the impacted area; and significantly interrupts governmental operations and emergency services to such an extent that national security could be threatened.*⁹

This definition has two components. It is based in part on the scale of an event's destructiveness (though the term "mass casualties" is not further defined in terms of numbers of deaths or injuries), and on the kind of effects the event has on government operations and other functional categories. The definition also rests on the degree to which the usual bottom-up system will be disrupted. A catastrophe "almost immediately exceeds the resources normally available" to the state and local agencies on which the disaster response system rests.

Hurricane Katrina exemplifies what the NRP would term a catastrophe. Hurricane Katrina wreaked destruction across such a wide area, and with such terrific impact, that it differed from major disasters in most of the ways that the NRP envisioned would distinguish such a catastrophic event. Perhaps most important, Katrina washed away the local foundations on which the bottom-up system rests across wide swaths of the Gulf Coast. The United States Senate heard compelling testimony (especially from Bill Carwile) on the ripple effect that this destruction had on the broader response system.¹⁰

Reacting to the failures of the response system in Katrina, the administration began to consider proposing a more federal-heavy, top-down approach to catastrophes. On September 15, 2005 in New Orleans, President Bush first suggested the possibility of the DoD taking the lead in response to stress on the bottom-up system: "It is now clear that a challenge on this scale requires greater federal authority and a broader role of the armed forces, the institution of our government most capable of massive logistical operations on a moment's notice."¹¹ He also raised the possibility that here might be

9. National Response Plan: 63.

10. U.S. Senate Committee on Homeland Security and Governmental Affairs, Hearing, Hurricane Katrina: Perspectives of FEMA's Operations Professionals (Federal News Service Transcript), 9 December 2005: 16.

11. Herman, Ken. "Let GIs Run Storm Relief?" *Atlanta Journal-Constitution*, September 26, 2005.

“a circumstance in which the DoD becomes the lead agency. Clearly, in the case of a terrorist attack, that would be the case, but is there a natural disaster...of a certain size that would then enable the Defense Department to become the lead agency in coordinating and leading the response effort?”¹²

President Bush’s suggestions raised a firestorm of opposition. Some of the loudest objections came from Florida governor Jeb Bush, who emphasized “The most effective response is one that starts at the local level and grows with the support of surrounding communities, the state and then the federal government. The bottom-up approach yields the best and quickest results—saving lives, protecting property and getting life back to normal as soon as possible.”¹³

But the question of whether to move towards a top-down system for normal catastrophes is far from settled. With Congress’s recent change to the U.S. Code in the Defense Authorization Act for fiscal Year 2007—something that has gotten little attention—it seems that there may already be a movement in that direction. Section 1076 of this act clarifies the President’s authority to use armed forces in response to a disaster when public order has broken down, even if a governor has not requested the President to do so. Now, I do not think we need to panic. There is no reason to believe that storm troopers are coming in the door. However, I do have some questions about the president’s being able to deploy forces *without* a governor’s request. First of all, what are the standards to identify when public order has broken down? When are local authorities considered “incapacitated”? This is not really spelled out in the legislation, or in what the members said in their statement accompanying the law. For example, is Hurricane Katrina a case in which public order broke down sufficiently that the President should have been able to send federal troops in without the request of Governor Blanco? Secondly, I wonder who in the course of things makes that assessment. Does the governor have a say in deciding whether public order within his or her own jurisdiction has broken down? Clearly, that assessment is going to be political, and it is going to be problematic. In the aftermath of Katrina, CNN displayed

12. Ibid.

13. Bush, Jeb. “Think Locally on Relief.” *Washington Post*, September 30, 2005.

allegations that public order was breaking down left and right, and ultimately, those claims turned out to be greatly exaggerated. Does this issue—once we clarify the President’s authority to act in absence of a governor’s request—put us on a slippery slope towards federalizing the catastrophic response system?

The need to focus on the core missions of DoD is an equally important rationale against assigning lead responsibility to the Department. DoD has big jobs—most of which involve expeditionary warfare—and we should husband the Department’s resources for its principal tasks, which cannot be outsourced to anybody else. Even more important, I think the current system, actually, can work very well in dealing with the stress posed by normal catastrophes on that system. That is, if we strengthen the EMAC system, and if the administration, rather than spending money on the federal government, invests heavily in building robust state and local capabilities, we are going to have most of what we need in order to respond to normal disasters. The types of additional capabilities I am envisioning include command and control mechanisms, and interoperable communications, and other measures designed to improve locality-to-locality, state-to-state reinforcement. In addition, DoD must empower its local partners by way of planning and help build within the existing infrastructure that greater strength that lies within DoD.

Although the EMAC system is sufficient for normal catastrophes, the third category of disasters along the escalatory ladder, “mega-catastrophes,” poses a different kind of threat that is likely beyond EMAC’s scope. These catastrophes differ from normal catastrophes not so much in the scale of destruction, but in *kind*. They differ qualitatively in a couple of respects. I am talking about very low probability, ultra-high consequence events where multiple, geographically dispersed and near-simultaneous incidents produce mass casualties on a scale, way beyond the scale of what we saw in Katrina or 9/11. Included in this category would be terrorist attacks—that is, man-made catastrophes—devastating earthquakes that decimate entire cities, and the newer threats of pandemic flu or biological terrorism, for which we still remain largely unprepared.

The key difference is that, unlike in Katrina, where the EMAC system worked very well—especially with regard to bringing in National Guard forces—the *qualitatively different* severity of these scenarios may cause the system to break down. Mutual aid may break down because governors are so concerned about hustling in resources to deal with the reach of the catastrophe into their own states, that they will tend to be less willing to commit resources to those who are suffering elsewhere. During Katrina, for example, you pretty much knew your state was not going to get hit by the hurricane if you were in Massachusetts, and therefore states like Massachusetts were able to send a lot of assistance down to the Gulf Coast. In a mega-catastrophe, however, when the status of every state's stability is uncertain, that willingness to share breaks down. In cases like these, the resources and competencies of the DoD will be in great need.

Even in the case of Hurricane Katrina, where the EMAC system was able to anticipate the needs of disaster response, the complex nature of the disaster led to many unforeseen problems. According to Admiral Thad Allen, then the federal official in charge of recovery efforts in New Orleans and now Commandant of the United States Coast Guard, 30-40 percent of the NRP failed because it did not take into account the possibility of two *simultaneous* catastrophes—in this case, the hurricane and the subsequent flooding: “The issues of the levees breaking and the catastrophic events that happened in New Orleans are the equivalent, in my view, of a terrorist attack by Mother Nature overlaid on a natural disaster.”¹⁴ If a “normal” disaster like Katrina is able to chip away at the EMAC system, we can only imagine the type of damage and disorder that an abnormal catastrophe would cause; EMAC, in this case, would become paralyzed.

Situations involving viral pandemic and biological attacks—because of their potential to cause a massive loss of life—represent a key area of catastrophic response where DoD should take a lead. Assistant Secretary of Defense for Homeland Defense Paul McHale said, “It is conceivable that a... biological event would be so large, so catastrophic, that every agency of the federal government, most especially to include [the Defense Department], would be involved in a comprehensive federal

14. Strohm, Chris. “Officials consider quicker federalization, use of military in disaster.” *GOVEXEC.com*, September 20, 2005.

response.”¹⁵ These situations are especially challenging to manage since they call for quarantines, which require numerous strategies for identifying and limiting the movement of the infected population, including screening of travelers, prohibition of large gatherings, and enforcement of incubation periods. President Bush has emphasized, “If we had an outbreak somewhere in the United States, do we not then quarantine that part of the country? And how do you, then, enforce a quarantine? And who best to be able to effect a quarantine? One option is the use of military that’s able to plan and move.”¹⁶ To many, this choice is sensible. After all, U.S. military culture possesses many of the “intangibles” necessary for comprehensive consequence management, such as leadership, professionalism, value of service and discipline. “When one looks around at institutions that have the size and the equipment and the capacity and the ability to deploy people,” asserted former Secretary of Defense Donald Rumsfeld, “the military is unmatched.”¹⁷

Now this is where the second qualitative factor differentiating mega from abnormal catastrophes becomes clear: as the EMAC system breaks down and fear and disorder become widespread, there will be an enormous demand from the American people and their Congress for the DoD to take the lead. Alexander Hamilton recognized this tendency early in American history, citing it in *The Federalist Papers*:

*Safety from external danger is the most powerful director of national conduct. Even the ardent love of liberty will, after a time, give way to its dictates. The violent destruction of life and property incident to war, the continual effort and alarm attendant on a state of continual danger, will compel nations the most attached to liberty to resort for repose and security to institutions which have a tendency to destroy their civil and political rights. To be more safe, they at length become willing to run the risk of being less free.*¹⁸

15. Mazzetti, Mark. “Military Sees Limits to Role in U.S. Disasters.” *Los Angeles Times*, October 13, 2005.

16. Brown, David. “Military’s Role In A Flu Pandemic.” *Washington Post*, October 5, 2005.

17. Herman, Ken. “Let GIs Run Storm Relief?” *Atlanta Journal-Constitution*, September 26, 2005.

18. Hamilton, Alexander. Federalist Papers No. 8, in Hamilton, James Madison, and John Jay, *The Federalist Papers* (New York: Penguin Books, 1961): 67.

Interestingly enough, many local leaders have indicated support for a stronger military leadership role. A recent meeting of the U.S. Conference of Mayors declared that the military should be playing a greater role in disaster response efforts: “The current legal paradigm is that the military is viewed as the ‘resource of last resort’ deployed to restore order. Because of the sheer magnitude of the hurricane events recently experienced, and because acts of terrorism may spring up during or in the wake of such natural disasters, it is advantageous to consider an increased role for the military in disasters response.”¹⁹ I believe that this is *precisely* the dynamic that we define in a mega-catastrophe, and it is the factor that will make it *politically irresistible* for the president to stand up against calls in Congress by the American people for that institution which appears to be most capable, the DoD, to assume the lead.

So, we have a choice. We can either plan for that eventuality, or we can be like ostriches and stick our heads in the sand. The danger here is that absent advanced preparation the military is going to hunker down into force protection mode and simple planning. It will lack the action plans to implement what it needs in order to most efficiently handle a particular situation and, once the military has gotten in, it will not have the plans that it needs to hand off authority *back* to civilians and exit the mission. The reality is that the military is constantly planning for low probability, high consequence events. The military may not want this mission, the DoD may not want to be in the lead—but that is all the more reason to plan for it. The costs of not doing so, as we have seen over the last few years, can be devastating. If there is anything that might be learned from events like 9/11 and Katrina, it is that shrewd planning—be it for prevention or response—is key to preserving our national security. We can run, but we can’t hide, so let’s go on with the planning process.

19. Wodele, Greta. “Mayors’ group urges bigger military role in emergency response.” *GOVEXEC.com*, October 24, 2005.



DoD – Not The Department of Disaster

COLONEL RICHARD CHAVEZ

Director, Consequence Management
Office of the Secretary of Defense for Homeland Defense

PROFESSOR BERT B. TUSSING

Director, Homeland Defense and Security Issues
The United States Army War College, Center for Strategic Leadership

The notion that the Department of Defense (DoD) should serve as the lead federal agency for major disasters and catastrophic events is not new. In 1992, in the aftermath of Hurricane Andrew, discussions took place regarding this issue, and more recently, the topic resurfaced after Hurricane Katrina devastated areas of Louisiana and Mississippi in 2005. DoD is certainly capable of serving as the lead federal agency for catastrophic events and major disasters; but examining this issue from an operational rather than an academic point of view leads to the conclusion that a more useful and appropriate role for the department would be to enable and support other federal agencies—equally, or even better suited to lead the federal response efforts.

In the event of a catastrophe, the DoD has three combatant commands which would be more than capable of anchoring the lead in a response to catastrophe: the United States Northern Command, the Pacific Command, and (perhaps less intuitively) the United States Southern Command. The experience and competence of the commands' leadership—coupled with the department's ability to conduct a wide variety of missions such as civil affairs, civil administration, reconstruction and restoration—lead many people to automatically default to the position that the DoD should serve as the lead agency in the event of a major disaster or catastrophe. The inherent capacities the department carries in the realms of communication, transportation, and a wide range of logistics capabilities only serve to reinforce this

notion. Unfortunately, while this position is convenient from an operational point of view, this is not necessarily the best alternative.

In the military we like to approach issues in terms of “ends, ways and means.” The truth is that the DoD possesses capabilities and resources to respond to catastrophe in terms of “means;” but we do not routinely focus on “ways.” The agency charged with addressing that part of the issue is, of course, the Department of Homeland Security (DHS), chiefly through the auspices of the Federal Emergency Management Agency (FEMA). Indeed, that is what the National Response Plan (NRP) (and the Federal Response Plan before it) is all about. FEMA has developed expertise in these areas, and in times of most crises will have personnel on the ground well before any DoD forces or supplies arrive in an affected area. Depending on the nature of the disaster—or worse, the catastrophe—DoD will respond to support requirements, regardless of which agency serves as the lead. But having the capability to rapidly deploy needed assets in *support* of an effort does not mean the Department has to be *in charge* of the effort.

Let’s examine what we’re really talking about here. The NRP envisions having a set of officials, to include a Principal Federal Officer, a Federal Coordinating Officer, a State Coordinating Officer, and others (including a Defense Coordinating Officer) all respond to a given disaster or catastrophe. Ideally, they will be co-located at the scene of the crisis, and will have established a working relationship through varying degrees of planning sessions and exercises prior to the event. Having the DoD roll in on top of these officials to assume the federal response lead would totally negate the advantage, and likely return the response effort to far more of an “ad hoc” character than the crisis’ victims deserve. By way of illustration, I would remind you that following Hurricane Katrina, Admiral Thad Allen did an outstanding job of orchestrating the response that saved thousands of lives, well before Lieutenant General Honoré and his fine staff arrived.

We would remind you as well that the DHS is not just Secretary Chertoff, or Secretary Jackson, or Secretary Stephan, or Secretary George Foresman or any other individual. Rather, it is a large organization consisting of individuals of immense talent and expertise. If operators are needed to serve as principle federal officials, then members of the

U.S. Coast Guard are the ideal candidates because they possess not only the leadership, but also the expertise to serve in this capacity. The Coast Guard not only trains to do operational missions, but is also authorized to conduct law enforcement tasks that are required when responding to a major disaster or catastrophe. Given these unique capabilities, we would suggest that flagged leadership from the U.S. Coast Guard might constitute the ideal choice for bringing together all 32 federal departments to effectively respond and mitigate the consequences of a disaster or catastrophe.

The area which the DoD can and should continue to provide the most assistance to other federal agencies is in the area of deliberate planning. Deliberate planning is a part of our culture; we depend on it for program development, resourcing, operational and contingency plans in the combatant command theaters, and so on. Moreover, our planning is cyclical: on a set schedule, by very deliberate design, we will review the plans we have made to ensure they are current with respect to requirements, the world environment, or the posture of our enemies. Without meaning to sound parochial, DoD is the only department in the federal government that has such a planning mindset. The DHS, however, has shown signs of wanting to instill this kind of mindset into their institutional culture. Accordingly, the DoD has provided and will continue to provide planners to DHS and FEMA (as well as Health and Human Services and the Department of State who have occasionally expressed similar interests) to teach, train and assist these agencies with the deliberate planning process.

We in DoD have learned over time that crisis action planning can best be accomplished as a derivative of this deliberate planning process. With a deliberate plan in place as a firm “line of departure” it is far easier for our planners to take an abbreviated approach to responding to individual events, empowered as it were with a lot of questions already answered, a lot of decisions already made. We have learned these lessons by way of hard experience, and would like to share our lessons with as many other members of the interagency community as possible. This is occasionally a difficult sell as a great deal of manpower and time—the two most precious resources we have—must be devoted to the type of planning we envision here. But—again as a function of hard won experience—

DoD has come to understand that the question is not whether we can afford expending such effort—but whether we can afford not to. I would suggest that the cost of being ill-prepared for another Katrina, or another Murrah Building, or any number of other scenarios is not something we would want to justify to the American people.

Another issue we have to take into account in determining whether DoD should serve in a supporting or enabling role rather than the lead in a federal response has to do with the types of missions federal military forces are permitted to perform. For instance, the way the DoD employs civil affairs forces overseas would hardly be appropriate in the domestic environment; there are currently 54 “Commanders in Chief” living in their respective Governors’ mansions that would take severe umbrage against that sort of breach of state/territorial sovereignty. Law enforcement is another big concern, one frequently revisited around discussions of the Posse Comitatus Act. As we think you all know, Posse Comitatus famously prohibits federal military forces from performing most law enforcement functions, and any exceptions to the Act are always carefully delineated and painstakingly scrutinized. As you also know, legislation is currently being negotiated to change the most noteworthy exception to Posse Comitatus, the Insurrections Act, but you may be sure that the question of how and when active component military forces will be used in law enforcement missions will never be taken lightly.

Now we’re going to ask for your patience for a moment as we appear to back off from our previous stance. We have tried to make it clear that we don’t think DoD should necessarily become the lead federal agency in disaster/catastrophic response, given our policies, plans and the inherent capabilities and responsibilities of the Departments of Homeland Security and Defense. But let’s stop again to look at those plans—particularly the NRP. The NRP, as you know, is basically designed as a tiered approach to response—beginning at the local level, continuing to state response if the local capabilities are overwhelmed, proceeding on to a federal response if the state, in turn, is outstripped. But that response plan is effectively based on political boundaries—literally state borders, if you will. When the disaster or catastrophe belies those boundaries (such as was the case with Katrina) the answers

and the responses become less clear. And what happens if the response mechanisms we are dependent upon are immediately overwhelmed; or if the human dimension of those mechanisms—the first responders—are among the victims of the event? These are the sorts of questions that are leading some people to make a distinction between “disaster” and “catastrophe.” And, these are the sorts of issues that are leading some people to say, “Well yes, 98% of the time the regular process and the regular agencies should be able to meet the requirement—but can anyone other than DoD respond effectively to that remaining 2%?”

To be honest with you, we’re not sure what the “right answer” is to inquiries of this sort. But we will suggest that, if we feel we have to make these kinds of distinctions, we are going to have to begin by identifying certain “trip wires.” Is the DoD the proper choice for lead federal agency in responding to a catastrophe as opposed to a disaster? Well then, what’s the trip wire that sends us from disaster to catastrophe? And if the DoD assumes the lead, will it remain in that position, or will it occupy that lead only as long as it takes other agencies or duly constituted authorities to retake the reins of civil response and recovery? Incidentally, this kind of thinking is in perfect consonance with the way we respond to foreign disaster response and recovery operations. The military always walks into a response effort with a mindset toward establishing an “exit criteria.” And it is not a matter of avoiding responsibility; it is a function of wanting to restore control to those who should be in control, and then going back to our “day job.”

Of course, in this admittedly “worst case scenario,” there is still one other remaining issue: in the transference of authority and responsibility back from the military to civil authorities (or, if you prefer, civil agencies), who is setting the transition requirements? Who is orchestrating the turnover of authority? Is it the DoD saying, “Okay, DHS, you got it!”? Or is the DHS, saying, “Okay, DoD, give it to me!”? Or is it the National Security Council, the Homeland Security Council, or the guy in the big house that they work for? Whatever the case, we had better be thinking of the answer before nature, or malevolent men, send the question.

If we had to leave you with one certain commitment on how military forces should be employed within the territorial confines of the United States, we would say that homeland defense is the only mission where the DoD domestically would and should be the lead. That's a pretty easy call, really, when you consider that no one else can effectively accomplish the mission. Only DoD has the ability to launch combat air patrols; we won't be asking Customs and Border Patrol to pick up the mission anytime soon. While the Coast Guard is a vital partner in Maritime Domain Awareness and Maritime Security as our concerns approach our shores, no one outside of the United States Navy is going to be seriously considered for "blue water" maritime interdiction operations. In the highly unlikely event that a robustly armed threat should breach our borders, no one is expecting anyone other than the Army or the Marines to convince them of the error of their ways. The "defense" in "homeland defense" pretty much clarifies who has the call in these instances.

But when it comes to "homeland security," I don't believe the federal government or the people it represents should cast their eyes too quickly to the Pentagon. Our own strategy for the challenge, *The Department of Defense Strategy for Homeland Defense and Civil Support*, makes it pretty clear that the DoD is ready to lead when it comes to defense, and to support when agencies designed specifically for response and recovery operations need us. In the meantime, it is in the best interest of the DoD and the country it serves to enable – to train, and to assist the leaders and supporting personnel of the DHS along paths we have already walked. As much as we can, we should assist them in acquiring skills we have already developed, so that when the time comes they can orchestrate a coordinated federal response to future catastrophes.

Chapter Two



*Do We Need a Goldwater-Nichols
Equivalent for the Homeland?*



Foreword

FRANK J. CILLUFFO

Director, Homeland Security Policy Institute
George Washington University

*In preparation for battle I have often found plans to be useless,
but planning indispensable.*

—General Dwight D. Eisenhower

The Goldwater-Nichols Department of Defense (DoD) Reorganization Act of 1986 was a major watershed for the defense community. Previously, each service acted and planned largely in isolation. There was division and duplication of efforts, competition over resources, and few economies of scale. Planning and execution occurred independently, which could negatively impact operational success.

Goldwater-Nichols changed all this. Procurement, planning, training and action became more unified, rather than competitive, processes. Most importantly, the Act fostered a sense of “jointness”—the idea that the United States Armed Services exist to get a job done, not to perpetuate themselves. “Thinking purple” is about more than just cooperation—it is about the creation of a truly unified structure in which each service asks how it can best contribute to the overall mission.

Although caution should be exercised when transposing aspects of a military model into the civilian context, there is substantial merit in looking to the military environment for lessons learned and key features that might be translated and imported into the homeland security context in order to enhance the nation’s safety. In both contexts, however, processes established in peacetime may provide a framework for effective response in times of crisis. For the military, this can mean successful prosecution of a war.

The challenge of successfully executing interagency coordination is age-old. To the extent that the various moving parts in our preparedness and response system are not working well together or are not doing so in an optimal way, it is necessary to remedy these deficiencies and weaknesses, because the price to be paid for not doing so is simply too high, and the costs are not simply monetary. A Goldwater-Nichols equivalent may therefore be needed for the homeland context—and not only at the federal level, but also between and among the states themselves and their local counterparts.

This is not to suggest that such change must be mandated at the state level or that the military should be tasked with primary responsibility for providing security for the homeland. Rather, this chapter explores from different perspectives—including that of the military and the policy community—what the military culture/mindset, structures, procedures, and so on may have to offer as we seek to bolster our civilian security posture. To this end, the papers in the chapter examine and address a range of relevant practices and elements including logistics, training, transfer of expertise and knowledge, strategy and the regional approach.

To help us puzzle through these challenging issues, in a series of policy papers, is a distinguished group of scholars and practitioners from the fields of homeland security and defense:

Joel Bagnal, Deputy Assistant to the President for Homeland Security, emphasizes the importance of achieving unity of effort across the agencies of the federal government in order to plan and execute catastrophic disaster response operations effectively. He argues in favor of a regional approach to homeland security, with “integrated...offices where interagency staffs would regularly work together...with State and local governments and private sector organizations...” Additionally, he contends that federal agencies should institute an interagency professional development program to heighten the effectiveness of both planning and response efforts.

Colonel Michael Edwards, Director of Operations, Air Force Combat Support Office, examines the need for the Goldwater-Nichols Act prior to its enactment in 1986, and reviews the

positive outcomes the Act has had on U.S. armed forces. He supports a Goldwater-Nichols equivalent for homeland security purposes that would leverage capabilities for prevention and robust response, and forge the Department of Homeland Security and other relevant entities into a cohesive force – one bolstered by cooperation with the DoD and the necessary funding to push forward change.

Christine Wormuth is a Senior Fellow at the Center for Strategic & International Studies. She was a contributing author for the Center's "Beyond Goldwater-Nichols Phase II" study. In this chapter, she makes recommendations for instilling in the homeland security context the core achievements of the Goldwater-Nichols Act, including "establishment of strong, unified leadership at the federal level, empowerment of operational leaders in the field, strengthening of the strategy development and planning process, and the creation of a more joint cadre of homeland security professionals..."

Daniel Prieto is Vice President for Homeland Security and Intelligence at IBM. He suggests that more than another reorganization is needed to promote the jointness that the Goldwater-Nichols Act encouraged. In his paper, Prieto advocates, among other things, a network-centric approach to finesse our homeland security coordination and management efforts. Such an approach "recognizes the limits of hierarchical command-and-control structures, and seeks to improve decision-making by leveraging improved information and communications among participants distributed throughout a network."

Jointness. Regionalization. Strengthened leadership and investing in our people through continued and expanded education and training opportunities. A network-centric approach. Adequate funding. These are just a few core ideas that merit serious consideration as we move forward and grapple with the challenge of how best to achieve homeland security.

My own views on this issue, expressed at our symposium and in other forums, are well known. A Goldwater-Nichols equivalent for the

homeland security community would bring together all of the now largely disparate components of our disaster preparedness, response and management efforts. Regional homeland security offices would maximize the various components of homeland security in cooperation, integrating all levels of government and all relevant agencies at each level, as well as building relationships with private sector and non-governmental entities that could and should be involved in preparedness, response, and information sharing. At the same time, we need to foster a culture of preparedness that is truly all-hazards and risk-based in nature, that encompasses a range of threats and crises from terrorist attack to infectious disease to natural disaster—all while bearing in mind that response must be flexible, capable of integrating ad hoc, entrepreneurial and creative elements when circumstances demand. Learning from those incidents that we have seen will help us better prepare for those over the horizon.

Admittedly, this is a tall order. Thoughtful consideration of these issues by leading figures in the policy world, the military and beyond will take us closer to our goal, however—and it is my hope that this chapter constitutes one small but significant step forward in that direction.

Goldwater-Nichols for the Executive Branch: Achieving Unity of Effort

JOEL BAGNAL

Deputy Assistant to the President for Homeland Security
The White House

The United States military's successful return to dominance following the Vietnam War was marred by a series of setbacks during the 1980s that revealed a need for further improvement in the way the various branches of the military fought together in battle. One of the most compelling examples is Operation Desert One, the failed attempt in 1980 to rescue the Americans held hostage in Iran. Of the many problems that plagued the aborted attempt to rescue the American embassy hostages, a core lesson was the need for the armed services to better train and exercise their ability to conduct joint, complex operations.

Three years later, when the U.S. military invaded the island of Grenada, several mishaps again demonstrated that while the Services each possessed impressive individual capabilities and strengths, they still did not operate together well as a team. Inter-Service rivalries led to friction among leaders, and incompatible communications systems and operational doctrine hampered cohesion among the many units involved.

To address these problems, Congress passed the landmark Goldwater-Nichols Department of Defense Reorganization Act of 1986. A chief objective of the legislation was to force the disparate Services to forge themselves into a true joint force able to operate with their collective and unified might, seamlessly weaving together their capabilities for a common purpose.

Just as Desert One and the invasion of Grenada were catalyzing moments for our military, the devastation that Hurricane Katrina wrought on the Gulf Coast must serve as the impetus for change in how the various branches of the federal government operate together in time of crisis. There is a great need for our interagency homeland security community to undergo the same kind of transformation that the Goldwater-Nichols Act brought to the Department of Defense (DoD). On February 23, 2006, the White House released its report, *The Federal Response to Hurricane Katrina: Lessons Learned*. The report makes 125 specific recommendations to remedy the shortcomings in how the federal government responded to the storm's deadly aftermath. Among these are a core set of initiatives that seek to do for the federal government what the Goldwater-Nichols Act did for DoD. Many of these actions are already underway, but more needs to be done. Furthermore, whether created by man or by nature, the next major national catastrophe could happen at any time, and there is no time to lose.

Interagency Organizations

A key objective of the Goldwater-Nichols Act was to change the organizational structure of DoD, strengthening the Office of the Secretary of Defense, and creating "Combatant Commands" with staffs comprising military personnel from each of the four Services. These joint, integrated Combatant Commands now form the nucleus that brings the four Services together to achieve unity of effort, fusing their collective capabilities into a single, unified force. Rather than coming together at the eleventh hour to develop complex plans on an ad hoc basis, the military organized itself into permanent, joint commands that better reflected the reality that joint warfare was the new paradigm, rather than the exception to the rule.

Central to the success of the Combatant Command construct is that these commands are independent, neutral organizations, separate and distinct from the various branches of the Armed Forces. For example, while the U.S. Central Command (USCENTCOM) has a large contingent of Army personnel, the other Services do not perceive it to be merely a proxy of the Army, serving only Army interests with only an incidental consideration of the interests and capabilities of the other Services. Similarly, the U.S. Pacific Command (USPACOM)

comprises a large Navy contingent, but it is viewed first and foremost as a joint command, serving the collective interests of DoD and of the nation, rather than only those of the Navy.

Today's widespread acceptance of the new Combatant Commands was by no means inevitable. In addition to requiring significant legislation, it required visionary leadership at the highest levels to ensure that the new Combatant Commanders did not put one Service above the others, and that the particular skills and capabilities of each were both recognized and valued. After two decades, joint warfare concepts are largely second nature to the military, but the interagency processes of the federal government are still in the nascent stages of applying similar principles to interagency operations. We are still organized and aligned largely in the same manner as DoD found itself prior to the Goldwater-Nichols Act—as separate, distinct departments that attempt to come together on an *ad hoc* basis to develop synchronized plans to conduct complex and critical operations at home and abroad. The interagency community arguably finds itself *in an even more challenging circumstance* than that which DoD faced, for the various federal departments and agencies—each with its own authorities, mission, and culture—are far less similar than were the various branches of the armed forces.

The challenges that the interagency community experienced in achieving unity of effort during the response to Hurricane Katrina reflect the inherent organizational difficulties related to disparate Federal agencies working together to respond to crises. Importantly, none of the difficulties should be attributed to lack of will or energy among the leaders and civil servants who have valiantly thrown themselves into highly challenging situations. Just as the mishaps that plagued the invasion of Grenada were not the result of any lack of motivation among the soldiers, sailors, airmen, or Marines who fought there, the challenges that the federal government faced, and continues to face, in the Gulf Coast stem primarily not from the people, but from the manner in which the federal government is organized.

To overcome these problems, we must consider applying the key principles embodied in the Goldwater-Nichols Act to the interagency community at large. We must find a way to establish joint, *interagency organizations* that synchronize all the elements of national power to

achieve common objectives. As we continue to develop our ongoing efforts to establish a more robust national emergency management capability, we would be well advised to consider the points discussed above. Any interagency organization, such as the National Counterterrorism Center or the National Operations Center, must represent and serve the interests and needs of the entire interagency community, not just those of a particular department or agency. Just as the Defense Department's Combatant Commands must make sure that they provide maintenance support not only for Army tanks but also for Air Force fighters, so must the National Counterterrorism Center and the National Operations Center support the information requirements of all relevant Executive Branch departments and agencies.

Any successful interagency organization must be supported by a staff of professionals from throughout the interagency community that are the best in their respective fields, not merely token representatives. The staff must include senior officials from a variety of departments and agencies with the years of experience and expertise necessary to handle a very complex range of issues. Importantly, the role of the interagency staff is not to serve a passive liaison function, simply communicating information and issues back to their home department or agency. For example, the Air Force personnel assigned to USPACOM are not there to watch what the Navy is doing and channel Air Force issues back to the Department of the Air Force for action; they are the staff of USPACOM, just as much as their Navy counterparts.

Similarly, the interagency personnel assigned to the National Operations Center are not there to support their "home" departments; they are the National Operations Center staff. Furthermore, a successful interagency organization should have the requisite representatives, procedures, and resources to ensure all elements of national power are integrated and synchronized to achieve a common purpose—this means incorporating State and local governments and relevant private sector entities into the interagency organization.

A Regional Approach

Another key aspect of the Combatant Command construct is the concept of regionalization. Recognizing that the likely trouble spots

in the world are far too diverse to effectively manage and engage with from a centralized headquarters, DoD has assigned five Combatant Commands with responsibility for a different global geographic region (U.S. Northern Command for North America; U.S. Southern Command for Central and South America; U.S. Central Command for the Middle East; U.S. Pacific Command for the Pacific and Far East; and U.S. European Command for Europe and Africa). This approach allows each geographic command to become familiar with the particular issues and problems associated with the area of responsibility, developing relationships with the leaders and gaining their trust.

Similarly, our approach to homeland security must emphasize a regional approach to managing the complex security environment that we now face. While the regions of the United States are not divided by language and cultural barriers, each has its own sets of particular concerns (e.g., hurricanes for the Gulf Coast; snowstorms for the Northeast; wildfires in the West), in addition to the common threats that we face everywhere, such as terrorism and pandemic influenza. Moreover, a regional approach provides more opportunity for familiarization and relationship development. No military staff officer working out of the Pentagon could be expected to visit all of the nations in the world, but a U.S. Southern Command officer might very well travel to most of the countries in South America. By the same token, it is unrealistic to expect Department of Homeland Security (DHS) staff or Department of Health and Human Services staff in Washington D.C. to form connections in each state and territory, but their respective regional offices can do so, developing relationships with the more manageable number of state and local counterparts in the region.

Consistent with the interagency organizational principles discussed above, our regional homeland security construct should be based on joint, interagency organizations. Encouragingly, many of our Federal departments already have regional offices. However, we need to promote integrated regional offices where interagency staffs would regularly work together at the regional level with state and local governments and private sector organizations to develop and synchronize plans, just as the Armed Services work together within the regional Combatant Commands, which work together with officials from the Department

of State, the Intelligence Community, the law enforcement community, and the economic community toward accomplishing common United States foreign policy objectives.

Interagency Assignments

Finally, and perhaps most importantly, the Goldwater-Nichols Act focused not only on commands and units, but also on the *people* serving in them. The Act established an occupational category—the “joint specialty”—for managing officers trained in joint operations, and provided important incentives for the Services to send their best officers to joint assignments, including making joint experience in a joint tour a prerequisite for promotion to the rank of general or admiral. It also required advanced education in joint operations for certain officers, and, perhaps most boldly, required a tour in a joint assignment for promotion to the rank of general or admiral. All of these initiatives created strong incentives for the Services to adopt a “joint” mindset that would gradually transform the way we fight and win our nation’s wars.

These joint assignments served two main purposes. First, from a training and professional experience standpoint, officers in these assignments learned a wealth of information about their sister Services—about their capabilities, their strengths, and how they fight. Second, and just as important, from a personal standpoint, the joint assignments broke down cultural barriers and inter-Service rivalries, as professional relationships and personal friendships formed between military personnel from different Services. The value of this latter benefit should not be understated. As people from different Services were encouraged and at times forced to work together, obstacles to unity were gradually overcome and the green, khaki, and blue colors of the military branches were slowly transformed into a true “purple” force.

Interagency assignments for federal employees would produce similar benefits. For example, the federal government needs to do a better job, collectively speaking, of following Socrates’ dictate, “Know thyself.” To state the obvious, the span of the federal government is enormous and contains a tremendous amount of resources and capabilities that are available to respond to a crisis—critically, however, there is not a collective federal knowledge of exactly what these vast and deep

capabilities and resources are. In the aftermath of Hurricane Katrina, we needed flat-bottomed boats in the flooded areas of the Gulf Coast, but it took the federal government too long to identify that the U.S. Government, within the Department of the Interior, already had just these sorts of boats ready for use. Just as an Army officer might not have known during the invasion of Grenada what equipment his Marine Corps counterparts carried into battle, some key parts of our government did not have a clear understanding of what the various departments and agencies could contribute to the Katrina response mission.

Part of the solution lies simply in doing a better job of leveraging technology such as databases to understand what assets are available to us. *But piecemeal reforms will not achieve the overall end goal.* We need to move beyond merely collecting data and information because in dealing with catastrophic events there is a need for key homeland security officials to develop a greater familiarity with the various components of the federal government. To this end, the White House report on Hurricane Katrina recommends that we institute an interagency professional development program, akin to the one that DoD developed in response to the Goldwater-Nichols Act.

Such a program must be founded to provide the opportunity for appropriate homeland security professionals to develop their knowledge of interagency capabilities and organizations. Just as the Goldwater-Nichols Act requires certain military officers to acquire expertise in joint operations through advanced schooling opportunities, we must ensure that our homeland security leaders are able to broaden their knowledge through a variety of educational opportunities, including long-distance learning programs and short-term seminars and courses. While we should take advantage of advances in technology that enable virtual education programs, we should not undervalue the benefits of people coming together in a classroom or seminar environment to learn from and exchange ideas with each other as well.

In addition, we should create appropriate incentives for a number of homeland security professionals to participate in interagency assignments. It is not enough to create joint interagency organizations without ensuring that these organizations are populated by the highest caliber personnel. Such assignments will enable homeland security

professionals to understand the roles, responsibilities, and cultures of other organizations and disciplines—as well as see their own organizations in a clearer light.

For example, a DHS official could serve for six to twelve months in an assignment with the Department of Justice, or a U.S. Northern Command officer could serve a tour at DHS headquarters. Such assignments would provide great opportunities for “cross-pollination” of ideas and perspectives between homeland security professionals. Interagency and intergovernmental assignments would inherently build trust and familiarity among homeland security professionals from differing perspectives. These assignments would also help break down barriers between organizations, thereby enhancing the exchange of ideas and practices.

At the same time, we should use caution in not stretching the analogy of the Goldwater-Nichols Act too far. The interagency community cannot, and should not, adopt this approach wholesale. We must recognize that the Army and the Air Force are, in spite of their differences, much more alike than, say, DHS and the Department of the Interior will ever be. The armed services have always been united by a common core mission—to protect and defend our nation on the battlefield. In contrast, each of the federal departments and agencies has a unique purpose and mission that it often does not share a great deal of in common with the others. Accordingly, interagency assignments will not be appropriate in all cases, and should be tailored to an appropriate number of homeland security professionals, rather than adopting a “one-size-fits-all” approach. Nevertheless, improved operational capabilities are a must, and Goldwater-Nichols does provide some compelling lessons for massive efforts at joint operations.

Conclusion

Since September 11, 2001, we have made significant strides in creating a “joint” homeland security community. The PATRIOT Act and the Intelligence Reform and Terrorism Prevention Act of 2004 greatly enhanced the flow of information between our law enforcement community and our intelligence community. We have created joint interagency organizations, such as the National Counterterrorism

Center, which is primarily composed of employees on temporary assignment from federal departments and agencies. In preparing for the 2006 hurricane season, DHS formed a series of interagency task forces to address the key problems facing the Gulf Coast—evacuation, sheltering, and communications.

There is also a greater interagency presence within our departments. For example, DoD has provided experts in operations and logistics on temporary assignment to DHS to assist in developing DHS's planning capabilities. As another example, DHS has led the formation of an interagency Incident Management Planning Team that includes representatives from a variety of departments and agencies. The ten FEMA regions—somewhat akin to domestic versions of the Combatant Commands created by the Goldwater-Nichols Act—now include DoD officials assigned on a permanent basis to assist in coordinating mutual plans, resources, and operations. DHS's National Operations Center serves as a hub for linking together the various Federal departments and agencies, along with key State and local officials.

Events, both man-made and natural, are driving steps that collectively are forcing us in the right direction, toward an integrated federal government that is able to effectively respond in a crisis. While we must accept that we may never achieve the sort of clearly defined “command and control” chain of authority that is found in the military throughout the interagency community, we also must accept that 21st century challenges require more modern and integrated preparedness and operational capabilities. Just as DoD learned the lessons of Desert One and Grenada more than two decades ago, so too must the Federal government learn the lessons of 9/11 and Hurricane Katrina. These changes will not come easily, and will no doubt be the subject of debate and criticism, but we must be determined in our effort to bring about these changes. The time is now, and the American people deserve nothing less than the best, most effective governance possible.



Goldwater-Nichols Act for Homeland Security

COLONEL MICHAEL EDWARDS, USAF¹

Director of Operations

United States Air Force Combat Support Office

Why is a Goldwater-Nichols Act Needed for Homeland Security?

All cabinet-level departments need to join together in a Goldwater-Nichols type reform to look at man-made and natural threats and government responses in an integrated manner. By creating better communication and synergistic efforts our government will be better equipped to handle, in a cost effective manner, the outcome of a terrorist act or natural disaster. This course of action will drive a holistic approach for the development of capabilities that will be flexible and resilient while providing a proactive capability to prevent some of the threats facing us today and in the future.

History of the Goldwater-Nichols Act

The attempted rescue of U.S. hostages held captive by Iranians in 1980 was categorized as unsuccessful, not just for its failed effort, but also because of a plethora of interoperability issues. For example, Marine Corps pilots were operating unfamiliar Navy helicopters, covertly inserting Army Special Forces to waiting Air Force refueling platforms, and while its joint concept appeared fluid, the operation was nevertheless chaotic. Interoperability issues would also plague the U.S. efforts in Grenada three years later. “Who,” asked Colonel O. E. Jensen, “hasn’t heard about the soldier who called from a phone booth on Grenada back to the States to get a message passed to U.S. Navy ships lying in sight offshore? Who doesn’t know that the ATO [Air Tasking Order]

1. Lieutenant Colonel Sean Cook, Major Mark Foley and Major Heath Bope also contributed to the research for this paper.

in the Gulf War had to be printed, copied, and carried to the Navy by hand because communication systems were incompatible? Such incompatibility could cost lives in the next war.”²

Congress created the Goldwater-Nichols Act in 1986 to force the Department of Defense (DoD) to be more responsive to the Commander-in-Chief and more efficient in the conduct of interservice matters. Lines of communication between president, cabinet, and service chiefs were fragmented and fundamentally separated. These divisions caused unhealthy competition between DoD organizations ranging from procurement to operations. Competition among air, land, and sea assets gave rise to:

- Waste, redundancy and inefficiencies in procurement;
- Overlap and inefficiencies in the development of new technologies;
- Network, software and equipment interoperability failures; and
- Issues with manpower and capabilities integration.³

Consequently, each service developed distinctive customs and practices; the “teamwork” atmosphere essential for conducting synergistic warfare was lacking. The objectives of Goldwater-Nichols for the military were many to include:

- Establishing clear responsibility;
- Assigning commensurate authority;
- Enhancing joint strategy formulation;
- Better providing for contingency planning;
- Strengthening the effectiveness of service members through Joint Professional Military Education (JPME) and Joint Duty Assignments (JDA); and
- Defining promotion eligibility requirements for general and flag officers.

2. “Information Warfare: Principles of Third-Wave War,” Col O.E. Jensen, *Aerospace Power Journal*, Winter 1994.

3. “Beyond Goldwater-Nichols, New Proposals for Defense Reform,” Clark A. Murdock and Richard W. Weitz, *Joint Force Quarterly*, issue 38: 34-41

All would lead to wide and sweeping changes within DoD. This reorganization allowed the Commanders-in-Chiefs (CINCs) [known as Combatant Commanders (COCOMs) after 2002] complete and total discretion over employment of all military assets in their particular region or “theater” of command. COCOMs are now responsible for assigned Army, Navy, Marine Corps and Air Force resources and report directly to the Secretary of Defense and the President of the United States. Goldwater-Nichols, a landmark in bureaucratic change, streamlined the military for greater efficiency in mission accomplishment. The overwhelming success of Operations JUST CAUSE and DESERT STORM revealed the extent to which the act unified the armed forces, enabling the military to be a more effective fighting force.⁴

Goldwater-Nichols also included integral elements within the legislation to provide DoD guidelines for Joint Officer Management (JOM) by establishing requirements for JPME and JDA categorization, and promotion rates/prerequisites within the service components to develop military officers with the skills needed to effectively integrate and operate within a joint environment. The objective of JPME is to educate officers in strategic thinking and planning, military history, and operational warfare. JPME is implemented in two distinct phases during selected officers’ careers when they become eligible for intermediate and senior service schools. Phase one emphasizes the fundamentals needed for joint operations, while phase two emphasizes joint perspectives, focusing on planning, operations and procedures.

In order to not disadvantage officers for promotion within their respective service, Goldwater-Nichols established promotion rate and eligibility requirements to be considered during an officer’s promotion selection board. Officers who are currently serving in JDAs, or who became Joint Specialty Officer (JSO) qualified through Joint Staff positions, are expected on average to be promoted to the next higher grade at a rate not less than the rate for the officers in the same military service in the same grade and competitive category who are serving, or who have served, on the headquarters staff of their respective military service. Lastly, effective

4. “Taking Stock of Goldwater-Nichols,” James R. Locher III, 1996: 15.

September 30, 2007, to be eligible for promotion to the rank of a general or flag officer, an officer must be designated as a JSO.⁵

Joint Officer Management within the Department has not been without its shortfalls and the 2003 Government Accountability Office (GAO) study, *A Strategic Approach Is Needed to Improve Joint Officer Development* (GAO-03-548T), concluded that DoD needs to continue refining its JOM processes. The study found that a significant impediment affecting DoD's ability to fully realize the cultural change is the fact that DoD has not taken a strategic approach to develop officers in joint matters, especially as it relates to the total force concept of operations integrating the active, guard and reserve components of the military services. Further, DoD has also not determined the number of officers who should complete the joint education program and has not filled all of its critical joint duty positions with officers who hold a joint specialty designation.

While the GAO has highlighted areas for improvement, DoD's Joint education and assignment process can provide a template and lessons for development of similar programs across many organizations of government. The benefits of Goldwater-Nichols go beyond education, equipping and training, to name a few. This is an evolution born out of necessity that is becoming more critical with the increased power for destruction by the non-state actor, pace of technological change and constrained budgets. We must seek new relationships and integration opportunities for cost effective development of capabilities that achieve their full potential.

Historical Military Capabilities

Current U.S. military capabilities and competencies encompass an arsenal of firepower like no other in the world. This fighting force is composed of highly skilled men and women dedicated to defending this country from hostile threats through the application of various competencies across the full spectrum of warfare. Today's National Military Strategy calls for unity of effort to defeat an enemy in two near simultaneous theaters of operation with resounding success.

5. "Joint Assignments and Policies," <http://www.fa-57.army.mil/newsletter/online/Winter2005/assignment.htm>.

Historically, DoD developed war making capabilities based on the assessment of the “traditional” battlefield—the U.S. military services trained and equipped for large-scale campaigns to defeat fielded forces. Military strategy has been influenced through the application of Carl von Clausewitz’s general principle; “take possession of [the enemy’s] material and other sources of strength, and direct operations against the places where most of those sources are concentrated.”⁶ Military, political and economic actions against an enemy state have been the tools of influence for our nation. World War I and II characterized conventional military operations in which the strategy was to use large maneuver forces to defeat our enemies through attrition, breaking lines of communications and destroying their strategic war-making capability.⁷

During the Korean and Vietnam conflicts, DoD had indications that the face of battle was starting to change. U.S. forces were limited in their ability to attack rear echelons because of political boundaries or political limitations. Some of the techniques employed by the Vietnamese irregular forces confounded the use of conventional tactics—resulting in the development of the swift and agile Air Cavalry.⁸ As the United States moved into the Cold War, deterrence and containment became the scope of U.S. military operations and posture. The projected threat of nuclear force created a military trump card for generating favorable foreign responses. The military also developed large conventional forces capable of rapid engagement and smaller units, such as special operations forces or tailored conventional force packages, creating a wider range of options to achieve national objectives.

The application of U.S. tools of influence on our enemies was predicated on the ability to leverage their infrastructure through the threat or use of actual force. Because “America’s potential enemies are

6. “Principles of War, Carl von Clausewitz,” <http://www.clausewitz.com/CWZHOME/PrincWar/Princwr1.htm#IIIa>.

7. “Iraq: Heavy Forces and Decisive Warfare,” *Parameters*, William R. Hawkins, Autumn 2003: 61-67.

8. “Winged Sabers: The Air Cavalry in Vietnam: 1965-1973,” Lawrence H. Johnson.

no longer exclusively established states with physical assets at risk,”⁹ returns on the use of strategic threats associated with traditional military capabilities have diminished. Nevertheless these capabilities can still be viable for unconventional warfare.

The development of lighter, agile and more lethal forces adapted for speed is not a new phenomenon in the employment of combat forces. Seeking to transcend the static trench warfare tactics of World War I, a German officer by the name of Hans von Seeckt set out to promote the idea of a tactical, more mobile military force. Envisioning the simultaneous maneuver of integrated tanks, aircraft, artillery, and a motorized infantry, von Seeckt paved the way for a new concept known as *Blitzkrieg*, or “lightening war.” In the early stages of World War II, Germany used this new tactic to great effect on the Eastern and Western Fronts. As General Erwin Rommel employed his 7th Panzer Division into France, smashing through Belgian resistance, he described transforming his forces “into a steel juggernaut emphasizing speedy movement and maximization of battlefield opportunities.”¹⁰ The German army set a historical precedent for the employment of armored troops and changed the nature of warfare by implementing a new ability for speed. Similarly, following this *Blitzkrieg* conceptual mindset, warfighting based on technology can not only create an advantage of speed and precision, but also foster new requirements such as the need for rapid intelligence during all phases of combat.

Blitzkrieg did not just create advantages of speed and precision, but also created new intelligence requirements. Information must meet precision targeting requirements to minimize collateral damage and be timely enough to target quickly emerging and fleeing targets. Non-kinetic resources, Information Operations, unmanned aerial systems (UAS’s) and space capabilities now play key roles in the effective and rapid employment of firepower. These advances are a result of the natural progression of technology and allowed campaigns from Operation Desert Storm to Operation Enduring Freedom to be more effective in destroying targets while reducing instances of unintended

9. “Sustain the Mission. Secure the Future,” <http://www.sustainability.army.mil/overview/ArmyEnvStrategy.pdf>.

10. “Blitzkrieg, 1940,” EyeWitness to History, www.eyewitnesstohistory.com (2002).

collateral damage. Consequently, intelligence gathered for these new capabilities allowed rapid assessment and targeting of “emerging” targets while enabling stringent rules of engagement to be employed with little or no effect on the surrounding civilian population.¹¹

Prior to 2001, the U.S. had a fighting force that was very capable of meeting conventional and non-traditional warfare requirements. The services were continuing to hone their joint and coalition operations while shortening the timeline from actionable intelligence to mission execution.

11 September 2001

The attacks of September 11, 2001 on the United States revealed a new threat and represented the opening salvo in the Global War on Terrorism (GWOT). Although unique in character, particularly for its conduct on our shores, the blurring of crime and war is a concept involved in fighting “non-traditional” enemies similar to hostile combatants in Afghanistan and Iraq (see Figure 1). Compelling a response with overlapping traditional warfighting roles, a new capability construct is emerging to address these threats. Although riddled with unique challenges, combating insurgents operating in the mountains

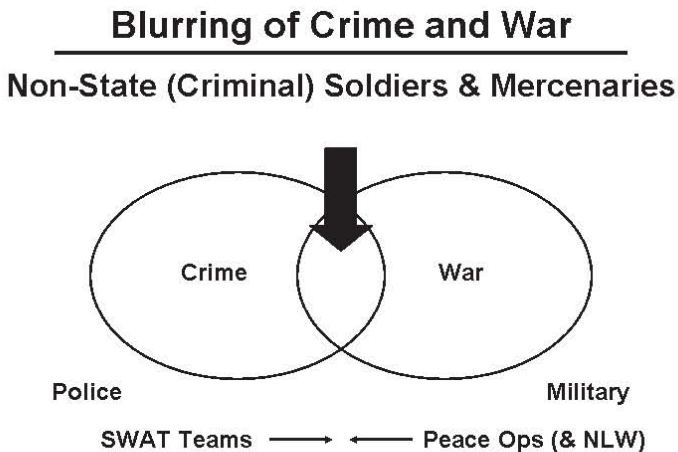


Figure 1: Blurring the Distinction between Crime and War

11. “Understanding Collateral Damage,” Carr Center for Human Rights Policy, John F. Kennedy School of Government, (June 2002).

of Tora Bora or the urban environment of Baghdad are achievable. The Vietnam conflict produced an enemy employing unconventional tactics. They blended into the battlefield using guerrilla tactics to fight American soldiers on “their terms.” Analogous to insurgent forces in the GWOT, the soldiers of the People’s Army of Vietnam (PAVN) were lightly equipped with small arms, mortars, and antitank weapons, no close air support, and perfectly camouflaged within their surrounding environment.¹²

The development and establishment of enemy non-state actors embedded within a nation, not necessarily sympathetic to that states’ objectives are also a tangential issue for the GWOT. The means of exerting influence over a nation, prior to using military force, has traditionally presented itself through the use of political, economic, and other instruments of national power. Unfortunately, some traditional methods of influencing desired behavior have limited effects on extremist since their views on national autonomy, the importance of freedom, and the universality of human rights are not always consistent with western thinking or understanding.

Determined to fight on our shores, terrorists are globally networked through ideology, well funded for their goals/methods, organized by cells, and cannot easily be deterred through conventional methods of national influence. They are steeped in radical anti-American ideology, with some of them being financially secured in measure by various criminal enterprises, some Muslim charities, banks and mosques. They are educated in schools that are “instrumental in creating an ideological climate which generates terrorism.”¹³ Such an enemy is difficult to fight, especially under today’s operational constraints.

The combination of DoD material and non-material solutions, kinetic and non-kinetic capabilities, competencies, and lessons learned have created a military evolution toward fluid tactics required for combating threats presented in the GWOT. Conducting military warfare under

12. “After Action Report,” Commanding Officer of 1st Battalion, 7th Cavalry, Lt Col Hal Moore, (November 1965), http://www.au.af.mil/au/awc/awcgate/vietnam/ia_drang.pdf.

13. “Fueling Terror, Institute for the Analysis of Global Security,” <http://www.iags.org/fuelingterror.html>.

the current global conditions requires a quick response to actionable intelligence with a precise and measured response in order to fight non-traditional enemies. Services are now focusing on future capabilities that will incorporate cyber warfare and non-kinetic weapons. DoD is also addressing asymmetric threats that potentially give non-state or state actors an advantage on the battlefield. One significant gap in our response to an elusive enemy is a coordinated effort bringing to bear all capabilities across all components of government. U.S. forces will need the competencies of the other arms of our government to complement and create greater effects.

A precise and measured response from an expeditionary force demonstrating power through rapid response, decisive projection of power, and a sustainment of troops is vital to the execution of combat operations. The combination of precision munitions and information operations provide the U.S. military with offensive capabilities to influence the battlefield within seconds, thus conforming to necessary operations on an accelerated timetable. Adhering to the ideals of transformation, the Army has created a more mobile, rapid, and less massive fighting force better suited to counter the urban warfare tactics employed by a non-traditional enemy. The new strategy of lighter and more technologically advanced units is the by-product of the natural selection of warfare for speed and agility, transforming service CONOPS and allowing for more rapid global retaliatory responses to secure tactical and strategic objectives in GWOT.

The military is evolving along lines that will improve GWOT capabilities and natural disaster response, but military solutions will not achieve full potential unless the process includes a team approach from government. There are conditions that exist throughout our government that are similar to conditions within DoD prior to 1986. Under the new demands of GWOT and natural disaster response, the cabinet-level departments of the U.S. government need an act that will create the same type of synergistic effects that have been beneficial to the DoD. For example, inclusion of the Department of Education will provide opportunities for expanding public understanding of our nation's struggle with terrorism.

Current Conditions

The military maintains core competencies and capabilities that support domestic GWOT and natural disaster response. They range from manpower to airlift, medical capacity, communications and more. DoD's recapitalization of equipment and manpower downsizing may remove military capabilities from the solution set because domestic requirements are not being captured or articulated to the right communities. Goldwater-Nichols was enacted within DoD to force the services to operate as a single war fighting entity and to develop officers skilled in attaining unity of effort between and among services, agencies, non-governmental organizations, and multinational forces. Its focus was to increase "jointness," interoperability, planning, and acquisition, and to transform all of these into cohesive functions. This new direction allowed service chiefs to concentrate on supporting regional combatant commanders by organizing, equipping, and training their forces to fight and win wars, instead of trying to outsmart their sister service counterparts in the budget, equipment, and mission arenas. As a result, regardless of the service, the mission now remains constant across similar organizations. Further, Congress directed this mandate and provided the necessary fiscal resources to accomplish the reorganization and paradigm shift.

Contrary to DoD's attempts at instilling "jointness" and developing its joint personnel force structure, the exact opposite concept of operations exists within the Department of Homeland Security (DHS). The primary mission of DHS is to protect the homeland, but unfortunately there is little unity of effort among the dissimilar agencies that comprise DHS to make it into a cohesive operative organization. While it is a daunting task to stand up an organization that incorporates numerous organizations and agencies, there does not appear to be any thrust to force change or resources to support this task. Communications between agencies is still a challenge, especially from the first responder level through the state to one or more DHS components.

The lessons learned from Hurricane Katrina showed that there were numerous breakdowns in areas such as command and control, unified management, communications, training, and logistics, to name just a few. DHS and other federal command centers had unclear and often

overlapping roles and responsibilities that were exposed as flawed,¹⁴ while the federal response to Hurricane Katrina highlighted various challenges in the use of military capabilities during domestic incidents. Limitations under federal law and DoD policy caused the active duty military to be dependent on requests for assistance. These limitations resulted in a slowed application of DoD resources during the initial response. Further, active duty military and National Guard operations were not coordinated and served two different bosses, one the president and the other the state governors.¹⁵

Therefore, all cabinet-level departments need to join together in a Goldwater-Nichols type reform to look at man-made and natural threats and government responses in an all-encompassing manner. Intra-agency reform will provide unity of effort to leverage departmental competencies. These capabilities can be applied to break threat chains prior to an attack and provide the fullest post-event response possible. While military services are restricted to identification of DoD solutions, there are common threats that need to be dealt with by the whole of our government. Steps are in place to capture all known and published threat documents. Threat documents can then be consolidated and prioritized by a sanctioned effort to help delineate and prioritize work effort and resources of the entire federal government. Solutions can be developed that have the most cost effective and long-term effects for the mitigation of these threats. As we look across the scope of a threat, from manufacturing an explosive device or development/recruitment of the terrorist, through transportation of that capability, to the execution of the act and efforts following the event, our government must determine the best resources and methods to sever the chain leading up to a potential incident. This approach will provide a holistic and cost effective method to determine alternatives for our senior decision makers. The identification of gaps and seams in our capabilities will also be critical to meeting the new challenges our nation faces in light of the potential magnitude of these types of occurrences.

14. "The Federal Response to Hurricane Katrina: Lessons Learned Chapter 5," <http://www.whitehouse.gov/reports/katrina-lessons-learned>.

15. "The Federal Response to Hurricane Katrina: Lessons Learned Chapter 5," <http://www.whitehouse.gov/reports/katrina-lessons-learned>.

DoD Capabilities in Domestic Response

There is a common thread between DoD and the rest of the federal government when it comes to protection against man-made and natural threats. Unfortunately, the divisions and fragmented lines of authority that plagued DoD prior to 1986 exist across cabinet-level departments today because intra-agency coordination and cooperation have not been addressed in ways similar to Goldwater-Nichols. Departments spend precious time and tax dollars in the development of solutions to similar problems. Our government must enact solutions for protection and security that are capable of meeting national requirements. Solutions should provide true capabilities that meet natural, man-made and/or foreign threats. This will be paramount in an era of decreasing and constrained budgets.

The Military’s Integrated Unit, Base and Installation Protection Capabilities Based Assessment (see Figure 2) is fusing material and non-material inter-service, intra-agency, and multi-national solutions to develop force protection capabilities. A similar concept could help to dissolve stovepipes created from natural bureaucratic processes

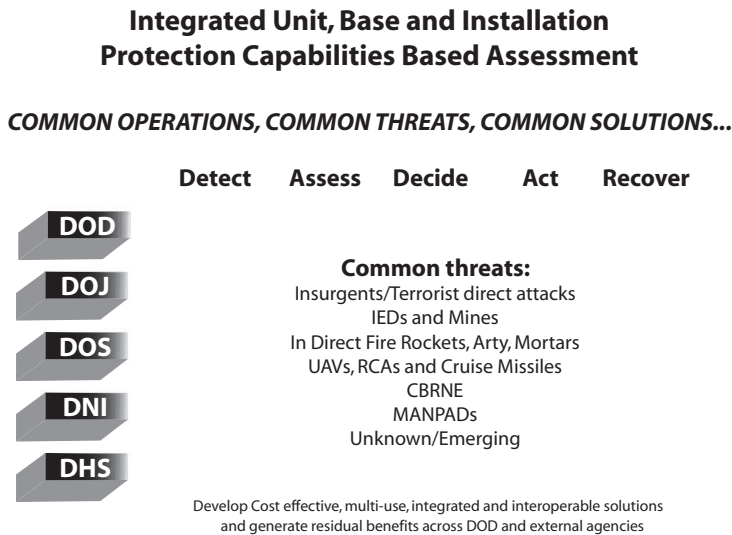


Figure 2: Integrated Unit, Base and Installation Protection Capabilities Based Assessment

within our government. It outlines the integrating operations and functions necessary to describe and apply DoD capabilities, ensuring unity of effort and global synchronization for security at the strategic, operational, and tactical levels. This Joint effort is integrating all force protection solutions to reduce waste and create interoperability across all the services while trying to expand effort across the whole government to meet common requirements.

DoD possesses human, material, and non-material resources and robust capabilities that provide for conduct of military and post natural disaster operations. But under limited budgets, many of these capabilities are at risk of going away or atrophying. Therefore it is critical for organizations to eliminate redundancy and the waste of funds in pursuit of parallel efforts aimed at meeting common department requirements. Goldwater-Nichols for government will help institutionalize the relationships, integration and cooperation required to achieve our government's full potential. This is highlighted again by the military's potential to support our homeland.

DoD Support for the Homeland

The key elements for supporting GWOT have been previously covered, but just as important are the domestic response resources. Land, sea, and air transportation assets can be utilized for transportation of supplies, pre-positioning of personnel and equipment, and aero-medical evacuation. Meanwhile, DoD C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) assets can provide state-of-the-art communication connectivity at all levels of command and provide real-time intelligence and situation assessments. Additionally, DoD search and rescue forces, medical, and civil engineering resources can be used to expedite recovery operations and help mitigate impact to personnel affected in the area of operations. DoD can play a vital role for homeland security beyond material resources. The military can establish training programs on command and control, logistics, and mobilization to non-DoD agencies. NORTHCOM can be the interface between DoD and non-DoD agencies. An example of the kind of transferable concept that could come out of this kind of exchange may be found in the Air Tasking Order Process.

The Joint Forces Air Component Commander (JFACC) is a derivative of joint doctrine developed as a result of the Goldwater-Nichols Act that made it possible to integrate the Desert Storm air effort. Initially, the Navy wanted to operate their strike packages autonomously using organic assets but realized DESERT STORM would be a massive, continuous strike operation rather than a short-term contingency operation. In order for the Navy to complete its mission successfully, they would have to rely on Air Force tankers under the control of the JFACC. The Marine Corps mantra was to support their ground forces through the Marine Air-Ground Task Force (MAGTF) and not support the JFACC, citing the 1986 Omnibus Agreement setting out guidelines for tactical control of Marine air forces.¹⁶ A compromise was agreed upon between the JFACC and MAGTF commander, allowing Marine air to support Marine ground forces as well as JFACC missions.

Due to the logistical problem of limited staging areas and multiple air assets, a joint document was needed to execute the DESERT STORM air campaign. The ATO document covered a 48-72 hour window of opportunity, de-conflicted airspace, coordinated all air assets, specified aircraft type, targets, time-on-target, and communications. This became the primary means to implement all air assets in theater, regardless of service or country of origin.

Likewise, a common document can be used for national resources in the event of a natural or man-made disaster. This type of document would delineate the areas of responsibility, provide clear concise C4ISR, coordinate logistics, etc. Elements will operate cohesively for the command authority but allow individual elements to carry out specific missions within their standard operating procedures.

Barriers to Support

The legal ramifications of the DoD support for DHS lay in Title 10 and Title 32 of the United States Code of Federal Regulations. The Posse Comitatus Act, passed in 1878, limits the powers of the federal government by “prohibiting the use of the Armed Forces as a posse comitatus to execute the laws except in cases and under circumstances

16. “Unity of Control: Joint Air Operations in the Gulf,” by James A. Winnefeld and Dana J. Johnson, *Joint Force Quarterly*, Summer 1993

expressly authorized by the Constitution or act of Congress.” Title 10, Chapter 10 (§331, §332, §333) states that the president may call into service the militia of a state [National Guard] to enforce the law when insurrection, domestic violence, or conspiracy hinders the execution of laws during the ordinary course of judicial proceedings. Furthermore, Chapter 18 (§371, §372, §373, §374) allows for relevant military equipment and resources, base and research facilities, training, and information to be made available to any federal, state, or local civilian law enforcement officials. Title 32, (§215.5) makes it legal, by way of a Presidential Executive Order, to employ DoD resources, Air Force, Army, and Navy [and activate units and members of the Reserve] pursuant to national security objectives. These legal implications are steadfast in structure, akin to chain of command “stovepipes,” and support a working coexistence of the DoD and DHS to combat a catastrophic incident affecting the homeland. The remaining challenge, however, is to remove organizational barriers other than structure.

Title 10 and Title 32 of the United States Code of Federal Regulations provide a conduit for interoperability of military and civilian law enforcement officials, but clear guidelines pertaining to intelligence and information sharing are underdeveloped, and require Congressional oversight. The equilibrium of jurisprudence between security and American civil liberties is difficult to define, and while intelligence and law enforcement officials may attempt to balance the issue, the legislative branch of government must provide the guidance necessary to ensure a positive outcome in the Global War on Terrorism.¹⁷

Summary

In summary, Congress enacted Goldwater-Nichols in 1986 to force the Department of Defense to be more responsive to the Commander-in-Chief and efficient in the conduct and execution of intra-service matters. Further, the Goldwater-Nichols Act broke cultural and organizational barriers thus creating better support and execution of the armed services’ role in national security.

17. “Guiding Lights: Intelligence Oversight and Control for the Challenge of Terrorism,” Jerry Berman & Lara Flint, (2003), <http://www.cdt.org/publications/030300guidinglights.pdf>.

Unfortunately, events have exposed a weakness in the rest of our government's organizational structures, mindsets, methodologies and concepts of operations. They are consistent with the limitations that existed within the military services prior to 1986. Organizational change, strategic vision and effective integration are desperately needed. The remaining cabinet-level departments have different missions yet similar responsibilities and challenges. A 21st century Goldwater-Nichols will enable our nation to handle various homeland defense and natural disaster challenges with solutions that are fully integrated and coordinated, ensuring the most efficient and responsive federal support possible.

Is a Goldwater-Nichols Act Needed for Homeland Security?

CHRISTINE E. WORMUTH

Senior Fellow, International Security Program
Center for Strategic and International Studies

The Goldwater-Nichols legislation that was enacted into law in 1986 is widely viewed as largely responsible for the most significant reform of the Department of Defense (DoD) since the National Security Act of 1946. While not without substantial flaws, the DoD is generally seen as a highly capable cabinet agency; one that is extremely mission-oriented and able to achieve tangible results while other federal departments often lack operational capacity. Five years after the 9/11 attacks, and one year after the disappointing governmental response to Hurricane Katrina, many in the national security community are asking whether a Goldwater-Nichols type reform is needed for the nation's homeland security system. From the dysfunction of the Department of Homeland Security (DHS) to the continuing interagency battles about roles, responsibilities and budget share, it is clear that the United States does not yet have a comprehensive, cohesive and competent system to ensure the security of the homeland. When considering whether a Goldwater-Nichols type reform would be useful or appropriate, it is useful to reflect on the major achievements of the original Goldwater-Nichols Act and how it might or might not translate into the homeland security arena.

Goldwater-Nichols: What Did it Achieve and Why Did it Happen?

The legislation introduced in Congress by Senator Barry Goldwater and Congressman Bill Nichols and ultimately enacted into law in 1986 enabled a wide range of defense reforms, but at a minimum the law resulted in four key achievements that have had lasting positive effects for the modern DoD. First, the law revised roles and responsibilities in the Department to strengthen the Secretary of Defense relative to

the Service Secretaries, and placed a single person—the Chairman of the Joint Chiefs of Staff—clearly in charge of providing military advice to the President. The law also transformed the role of the combatant commanders, placing them squarely in charge of mission accomplishment and providing them the authority over forces to carry out that responsibility. The law forced the Department to pay more attention to comprehensive strategy and planning activities with the goal of achieving a more cohesive strategy that would drive DoD planning and programming efforts. Finally, the Goldwater-Nichols legislation mandated changes to the DoD personnel process that ultimately resulted in the development of military leaders that could look beyond their service affiliations and think “jointly,” allowing the Department to leverage the full range of Service institutional capabilities in order to develop more integrated and effective policies, plans and military operations.

In light of the typically static nature of large bureaucracies and the difficulty of enacting changes in these institutions, it is important to understand how the reforms enacted as a result of the Goldwater-Nichols legislation came about. What made such sweeping changes possible? The U.S. military has not always seen the success it had in Operation Enduring Freedom in Afghanistan or even in the initial phase of Operation Iraqi Freedom that culminated in the topping of the statue of Saddam Hussein in Baghdad. The 1970s and 1980s witnessed a notable handful of operational military failures that shook the confidence of the nation’s leaders, in particular Desert One, the disastrous mission to rescue the Iranian hostages in 1980 and the uncoordinated invasion of Grenada in 1983. Both operations revealed multiple instances of military Services unable to communicate and operate effectively together, despite the high quality of military personnel and tremendous financial investment in all of these institutions.

Although initial efforts to make the case for reform in DoD were met with strong opposition from within the Pentagon, ultimately a critical mass of lawmakers, senior retired military officers and subject matter experts were able to prevail and significantly change how the DoD functions. More than twenty years later, the changes enacted as a result of the Goldwater-Nichols legislation are widely viewed as fundamental

to the success of the nation's military and its ability to conduct operations effectively.

Is a Goldwater-Nichols for Homeland Security Needed?

When considering whether reform on the scale of Goldwater-Nichols is needed in the area of homeland security, it is useful to consider whether there have been operational failures comparable to those the military experienced in the Iranian desert or in the rainforest of Grenada. Certainly the governmental response at all levels—local, state and national—to Hurricane Katrina in 2005 was not an operational success. Although the response was not a total failure, it was not acceptable in the eyes of almost everyone who watched it unfold. President Bush himself said “the system, at every level of government, was not well-coordinated, and was overwhelmed in the first few days.”¹ Of particular concern is that fact despite considerable warning of the hurricane, the response to Katrina was still dramatically inadequate. To truly ensure the security of the homeland, the nation must be able to manage the consequences of a no-warning event, and the response to Hurricane Katrina lay bare how far the homeland security system has to go before it can meet that standard.

Looking beyond the operational realm, it is also clear that the homeland security system as a whole cannot yet function effectively. Strategy, planning and programming activities are not clearly linked together. Roles and responsibilities, within the interagency and among the federal, state, local, private and non-profit sectors remain somewhat murky defined. Perhaps most importantly, there is not yet a common corporate culture at DHS, nor are there sufficient numbers of homeland security professionals who have the training and expertise they need to be effective.

Relative to military operations, homeland security in the post-9/11 environment is a relatively new mission area, but nevertheless it is clear the country needs significant reforms in order to achieve an adequately functional homeland security system. A Goldwater-Nichols approach

1. President George W. Bush, The White House, “President Discusses Hurricane Relief in Address to the Nation,” September 15, 2005, <http://www.whitehouse.gov/news/releases/2005/09/20050915-8.html> (accessed December 15, 2006).

to homeland security may well be part of the solution, but at the same time, the analogy is not perfect.

The Goldwater-Nichols Act greatly reduced the inter-Service infighting inside DoD. While a significant accomplishment, even before Goldwater-Nichols, the military services at least all worked for a single cabinet secretary. A central challenge in the homeland security arena is uniting the efforts of multiple cabinet agencies—each with its own cabinet secretary.

Goldwater-Nichols led to considerably more unity of effort among the various stakeholders inside DoD, but the reforms were only focused on a single level of government—the federal level, and on a single department within that federal government. The homeland security system is characterized by an exponentially larger number of stakeholders located at all levels of government and society—federal, state, local, tribal, private sector, non-profit and individual. Enhancing unity of effort among such a wide and disparate range of actors will be far more difficult than reforming a single cabinet agency at the federal level of government.

While the Goldwater-Nichols experience does not fit the homeland security sphere perfectly, there is a need for a new framework around which to organize the nation's homeland security activities to better ensure their effectiveness. In thinking about how the Goldwater-Nichols example might apply to the homeland security sphere, it is useful to consider what “jointness” really means. In an article marking the 20th anniversary of the Goldwater-Nichols legislation, Mackubin Owens noted that most supporters of the Goldwater-Nichol reforms used the word “jointness” to describe the quest for greater integration, specifically the desire for “improved procedures for combining the unique specialized capabilities of the different services to enhance combat effectiveness.”² Framed in this way, greater “jointness” is also needed in the homeland security sphere. There is a real need for a framework and set of institutional relationships that will promote increased integration among the many actors in this area so that the nation will be better able

2. Owen, Mackubin, “Conformity Needs Competition,” *Armed Forces Journal* (June 2006): 25.

to combine their unique, specialized capabilities into a robust capacity to protect the homeland and manage the consequences when efforts to prevent attacks fail.

What Would a New Framework Look Like?

The reforms enacted by the Goldwater-Nichols legislation are a useful starting point for exploring what a new framework for the homeland security system might look like, but given the significant differences between the defense and homeland security arenas, there will clearly be limits to how completely the Goldwater-Nichols experience can be applied to homeland security.

Stronger, More Unified Leadership at the Federal Level

Reflecting on the major accomplishments of Goldwater-Nichols for the Defense Department, there may be loose analogues to challenges in the current homeland security system. First, the Goldwater-Nichols Act strengthened the Secretary of Defense and Chairman of the Joint Chiefs of Staff relative to the military Services, and also established lines of authority to unify the advice that DoD provides to the President. In the homeland security context, the parallel challenge is the central question of how to ensure that the organization at the federal level with primary responsibility for homeland security is sufficiently empowered to execute this mission. What is the best way to structure the homeland security system so that there is a clear focal point in the federal government for setting policy, convening all of the essential stakeholders and ensuring that policy is effectively implemented? The DHS was clearly established to serve as the focal point for homeland security activity at the federal level, but there are many other federal agencies that play important roles in various aspects of homeland security.³ While Homeland Security Presidential Directive/HSPD 5 gives DHS the responsibility to serve as the principal Federal official for domestic incident management, DHS cannot direct the rest of the

3. Agencies with significant homeland security roles include the Department of Health and Human Services, the Department of Transportation, the Department of Justice, the Department of Defense, the Department of Agriculture and the Department of State, just to name a few.

cabinet to behave in particular ways, whether during an event or on a steady-state basis.⁴

The relative equality of all federal agencies complicates not only the federal government's ability to conduct joint operations inside the United States, but also overseas in the context of complex contingency operations. In its *Beyond Goldwater-Nichols Phase 2 Report*, the Center for Strategic and International Studies (CSIS) examined in detail how to bring greater unity of effort to interagency operations in the overseas context.⁵ A theme that ran through many of the specific recommendations in the report was the need for the National Security Council (NSC) to play a stronger role in both the policy development process as well as oversight at the strategic level of planning for actual operations. Whether operating overseas or inside the United States, the only actor in the federal government that can ensure Presidential intent is being executed, mitigate disputes among cabinet agencies, and minimize instances of log-rolling is the White House in the form of the National Security and Homeland Security Councils. Only the President, or those that speak for him or her, can serve as the arbiter between cabinet secretaries, and for any complex operation to have the potential to succeed, there has to be a mechanism in the system to resolve major disputes. The lead federal agency model cannot be at the core of the homeland security system because it provides no realistic mechanism to broker bureaucratic disagreements at the strategic level.

Empowered Operational Leadership

A second major accomplishment of the Goldwater-Nichols Act that is relevant when considering a new framework for the homeland security

4. HSPD 5 states that "the Secretary of Homeland Security is the principal Federal official for domestic incident management. Pursuant to the Homeland Security Act of 2002, the Secretary is responsible for coordinating Federal operations within the United States to prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies. The Secretary shall coordinate the Federal Government's resources utilized in response to or recover from terrorist attacks, major disasters." See Homeland Security Presidential Directive/HSPD 5: Management of Domestic Incidents (The White House, February 28, 2003).

5. See *Beyond Goldwater-Nichols: U.S. Government & Defense Reform for a New Strategic Era, Phase 2 Report*, pp. 43-53, July 2005.

sphere was the empowerment of the combatant commanders to conduct operational planning and control the operational resources necessary to conduct successful operations. While there is not today an analogue in the homeland security system for the combatant commanders, to be effective in responding to major domestic catastrophes, the Nation does need to conduct joint, interagency operational planning in advance of actual response operations. The nation also needs a framework, if not a single organization, that brings together pre-existing operational plans, capabilities and the many stakeholders in the homeland security system into a clear, transparent process that can set priorities and then implement them effectively during a catastrophe.

Today, the most similar structure in the homeland security system to a combatant commander is the Joint Field Office (JFO), led by the Principal Federal Official (PFO), a position established in the National Response Plan (NRP). Under the NRP, in the event of a major catastrophe, the federal government would work together with affected states to establish a JFO that would allow key federal officials to be co-located with state emergency managers in order to work together to lead the response to a domestic incident. In the case of multiple, simultaneous events or an event that has significant national impacts, the Secretary of Homeland Security has the authority to designate a “national PFO” that would coordinate the response at the federal, strategic level. In stark contrast to DoD’s combatant commanders, however, PFOs do not have directive control over all of the resources and capabilities that would be employed as part of a response to a catastrophe. Principal Federal Officials have coordinating authority only, at the federal level among the many cabinet agencies, but also with state and local authorities. Although combatant commanders can work with coalition forces and non-military organizations such as non-governmental organizations and the private sector, their operational plans do not rely on capabilities from these organizations to succeed. Combatant command plans are based on only those forces that the commanders actually control or know with considerable certainty will

be available.⁶ In contrast, PFOs, while not controlling the resources of other stakeholders at the state and local level, or in the private and non-profit sectors, fundamentally rely on capabilities from all of these sectors in order to carry out a response to a domestic incident. These features of the nation's emergency preparedness system are central differences between the defense and homeland security spheres, and it is not clear whether the empowerment of the combatant commanders that the Goldwater-Nichols Act achieved could be easily replicated in the domestic sphere.

In the absence of a single individual like the combatant commander in charge of an operation, how can the nation—at all levels of government—best create unity of effort? At a minimum, the major stakeholders at all levels have to understand clearly which actors are in charge of which elements of a response effort and have some basic agreement about that division of labor. The current system, based around the NRP and the National Incident Management System (NIMS), is extremely complex for many reasons, but if the existing system is to function more effectively, it is critical that leaders and major “implementers” at all levels need to be much more familiar with the framework envisioned in the NRP and its supporting documents. In order to make such a complex system work, it must be trained and exercised extensively.

Any successful framework for the homeland security system also will need to be sufficiently flexible to accommodate a wide range of potential crisis scenarios. In many catastrophes, the current system, which envisions a response that is led by local, state and federal officials collectively, may be sufficient—particularly if those authorities have exercised and trained the processes outlined in the NRP and the NIMS. At the same time, it is important to consider whether there could be a small number of scenarios that might require a different command and control structure. Could there be instances in which the catastrophe

6. For example, while U.S. Pacific Command does not have command and control over South Korean military forces, it is clear that those forces would be central to any engagement against North Korea and hence are factored into the war plan accordingly. In contrast, while some coalition forces were likely to have been available, when U.S. Central Command developed plans for Operation Iraqi Freedom, the only allied forces that were included in the core war plan were the British Army troops that Prime Minister Blair made clear would be available for the invasion.

is so dire that a federally-led effort is the only way to respond on the necessary scale and with the necessary speed? How will the nation's leaders determine when such a dramatic step might be necessary? Would such a response be possible under existing legal authorities? Are there steps the federal government could take, working with state governments, that would make state governors more comfortable with the concept of a federal lead for certain mega-disasters? Or is the key challenge to work with states to develop more robust capabilities to respond to a catastrophe so that a federal lead would not be necessary to ensure effectiveness? These are critical questions to answer before formulating any sort of Goldwater-Nichols Act for homeland security.

Greater emphasis on regional organizations may be part of the new framework that is needed. By definition, in a catastrophe state capabilities will be exceeded. Under the existing framework, states have a mechanism—the Emergency Management Assistance Compact—to share resources, but what specific resources might be shared under what conditions is often not defined until a disaster is already underway. More emphasis on regional organizations that are focused on assisting state efforts to develop plans and policies for catastrophic incident management—nor only among states in a region, but also between states in a region and the federal level—may help fill the gaps that exist today. Regional structures could also be a tool for working with state and local authorities on a steady state basis to implement policy and planning guidance coming from Washington more consistently and effectively. Regional structures offer a means by which to establish stronger relationships with the state, local, tribal and non-governmental sectors, as well as tool by which to begin cataloguing and assessing capabilities within regions.

For regional structures to be effective, whether they are largely state-centric entities with federal liaisons, or federal organizations with state liaisons, they must add real value and not simply function as an additional layer of bureaucracy. For regional organizations to be useful, federal headquarters in Washington DC will need to be willing to delegate real responsibility and authority, and not just see regional structures as a filtering mechanism.

Finally, determining how to draw the boundaries of regional organizations is another challenge, and one with an analogue in the defense arena. The Unified Command Plan (UCP) outlines how the world is divided up among the various regional combatant commanders. In more than one instance, countries with intrinsic relationships in the real world are allocated to different combatant commanders—in many cases the politics of conflicts place countries on opposite sides of the UCP boundaries. While commands may avoid making difficult choices between countries with adversarial relations by virtue of these divisions, the dividing lines also can make it harder to view and address these precise conflicts in an organic fashion. In the defense realm these dividing lines are further complicated by the fact that other important U.S. organizations such as the Office of the Secretary of Defense and the Department of State do not divide up the world in the same manner as the military combatant commands. The challenge of establishing regional boundaries in the defense sphere is an important reminder that establishing regional divisions inside the United States will require careful thought, and if such a move is to have real hope of being beneficial, the federal government, states, major urban areas, and major private sector and non-profit organizations need to adopt a reasonably uniform approach to such boundaries.

Comprehensive Strategic Guidance and Planning

Another significant contribution the Goldwater-Nichols Act made to the modern Defense Department was to direct much greater emphasis on developing a comprehensive approach to strategy development and planning. Although the DoD reviewed its strategy and planning process as part of the 2006 Quadrennial Defense Review institutional roadmaps, it is certainly true that while not perfect, the DoD has the most robust strategy development and planning system in the federal government. In contrast, despite an array of strategy documents, Homeland Security Presidential Directives and departmental strategy plans, it is clear that the full range of stakeholders in the federal homeland security system are not yet entirely on the same page in terms of priorities and overall focus. As one simple example, the federal government has not yet even developed a common terminology for homeland security matters

that enables the community to communicate clearly when its disparate elements come together.

Without prejudging the issue entirely, one potential way to bring more unity of effort to the strategy development and planning process for homeland security at the federal level would, again, be to ensure a more robust role for the White House. A first step toward a stronger White House role would be a merger of the National Security Council (NSC) and Homeland Security Council. Merging the National Security and Homeland Security Councils into a single, truly National Security Council would greatly facilitate the ability of the federal government to develop strategies, policies and plans that address homeland security challenges in a holistic, integrated fashion and make important linkages between security issues outside and inside U.S. borders. A unified NSC with staff that can address the full suite of security challenges would reduce disconnects that can and have arisen when two, largely separate organizations are responsible for addressing security issues that by definition are inextricably linked.⁷

Even if a future administration chooses to merge the NSC and HSC into a single, true National Security Council, there is still considerable work to be done in developing a more functional policy, planning, budgeting and execution (PPBE) system across the interagency. Although there are a number of White House-issued strategies related to homeland security, they have been developed separately at different points in time—in some areas they overlap and in other areas there are gaps—and it is not clear how to prioritize among the different documents. One means to unify these different concepts would be to conduct at the interagency level a Quadrennial National Security Review (QNSR) that would enable the entire interagency to work together to determine national objectives, develop a strategy to achieve those objectives, determine what capabilities are needed for that strategy and delineate roles and responsibilities inside the interagency so that federal departments can successfully implement those parts of the strategy for which they are responsible. Just as the Quadrennial Defense Re-

7. See *Beyond Goldwater-Nichols Phase 2 Report: U.S. Government & Defense Reform for a New Strategic Era*, pp. 66-70 for a more extensive discussion on the need to merge the NSC and HSC.

view serves as the foundation for the Strategic Planning Guidance that DoD develops as an internal document to guide its efforts, a product of the QNSR would be the development of a National Security Planning Guidance that would provide more detailed direction to federal departments on how to implement their elements of the strategy, to include homeland security planning and activities.⁸

Equally important is determining how and to what degree to integrate state, local and tribal entities, as well as other non-federal actors into the PPBE system undertaken at the federal level. The primary tool the federal government has to shape activity at the state and local level is the DHS Grants and Training program, but it is not clear that the range of grants and training activities are sufficiently connected to strategic priorities or allocated in ways that maximize the degree to which state and local preparedness efforts reflect priorities being articulated at the federal level. Progress has been made in recent years on allocating a larger share of grants and training funding based on risk assessments, but considerable work remains. It is also clear from the DHS Nationwide Plan Review that more must be done to work with states on deliberate planning for catastrophes as well as developing a process by which to assess the readiness of national emergency preparedness capabilities at all levels.

Developing a “Joint” Homeland Security Career Path

The last major accomplishment of Goldwater-Nichols that clearly has applicability to the homeland security sphere is the critical decision Congress made twenty years ago to link service for military officers in joint duty assignments to promotion to general officer ranks. It is widely acknowledged that this step, while vigorously resisted at the time by the Services and only grudgingly supported in the wake of the Act’s passage, resulted in a much higher quality Joint Staff and stronger corps of joint officers.⁹

There is recognition in Washington that there is a need for a much larger cadre of homeland security professionals who have the multi-

8. Ibid, pp. 27-29.

9. James R. Locher III, *Victory on the Potomac: The Goldwater-Nichols Act Unifies the Pentagon*, pp.443-444. (Texas A&M University Press, 2002).

disciplinary expertise necessary to be successful managing the challenges inherent in protecting the homeland and managing the consequences of major domestic incidents. As part of building such a cadre, there is also recognition that there needs to be a professional development and educational system that explicitly focuses on the myriad, complex and in some cases unique features of the homeland security system. In this sense, there is a real need in the homeland security sphere to create a system similar to the joint officer management program that was directed by the Goldwater-Nichols Act.

In its *Beyond Goldwater-Nichols Phase 2 Report*, CSIS recommended that Congress and the interagency should work together to establish a national security career path that would require career civilians to serve in interagency rotations in order to be considered for promotion to Senior Executive Service (SES).¹⁰ CSIS is not the first non-governmental institution to recommend such an approach; the Hart-Rudman Commission called for the development of a National Security Service Corps in its final report published in 2001. A career path of this kind would include traditional national security professionals and homeland security professionals.

In addition to requiring interagency rotations to be considered for promotion to SES, the CSIS Phase 2 study also called for building an education and training program that would be a central element of the professional development system for national security career personnel. The DHS is currently considering how best to develop such an education and training program. One option would be to expand the mandate of the National Defense University to address the full panoply of national security issues (of which homeland security is a part) and change the name of the institution to the National Security University. Critics of this option argue that such a change would likely be more cosmetic than substantive and might not ultimately provide sufficient focus on the non-defense aspects of the curriculum. Another option would be to establish a new institution focused on interagency operations, both domestic and international, or an institution that is focused exclusively on homeland security issues. At a minimum, it is clear that there is a need to provide senior homeland security professionals with a focused

10. *Beyond Goldwater-Nichols Phase 2 Report*, pp. 40-42.

developmental experience at an accredited educational institution that has a curriculum targeted toward the full range of homeland security challenges.

The Goldwater-Nichols Act: An Imperfect Roadmap for Homeland Security

Although there are many differences between the well-established and very mature national defense system and the much newer homeland security system, it is clear that the major reforms achieved as a result of the Goldwater-Nichols Act of 1986 can serve as both goals for which to strive toward and a rudimentary roadmap for how to move the homeland security system toward greater unity of effort and ultimately greater effectiveness. The homeland security environment is even more complex, both organizationally and politically, than the overseas environments in which the military combatant commanders operate. Tempting as it is, it is not possible to simply “cut and paste” the Goldwater-Nichols reforms into the homeland security sphere. The homeland security community will have to consider carefully how to translate the achievements of Goldwater-Nichols effectively into the homeland security environment. Ultimately it may not be possible to achieve the same degree of clarity in certain areas that was achieved in the defense realm as a result of the legislation. The short operational chain of command between the combatant commanders and the President of the United States that was enshrined in the Act may be a bridge too far on the domestic side in light of the complex array of actors at the federal level, the governors at the state level, the diverse models of authority and responsibility at the local level, as well as the presence of critical actors in the private and non-governmental sectors.

At the same time, the core achievements of the Goldwater-Nichols Act—establishment of strong, unified leadership at the federal level, empowerment of operational leaders in the field, strengthening the strategy development and planning process, and the creation of a more joint cadre of security professionals—are clearly much-needed elements of a stronger homeland security system and are reforms the wider homeland security community should seek thoughtfully but aggressively in the next few years.

The Limits and Prospects of Military Analogies for Homeland Security: *Goldwater-Nichols and Network-Centric Warfare*

DANIEL B. PRIETO

Senior Fellow, Global Leadership Initiative, IBM

Senior Fellow, The Reform Institute

Senior Advisor, Commission on the National Guard and Reserve

I. Introduction

*Being in favor of coordination...has come to be like being against sin; everyone lines up on the right side of the question. In fact, coordination has become...a word which defies precise definition but sounds good and brings prestige to the user.*¹

—Ray Cline, former Deputy Director, CIA
and Bureau of Intelligence and Research,
State Department

Since the attacks of 9/11, the United States has sought to strengthen its ability to prevent terrorist attacks and respond to high-consequence events affecting the U.S. homeland. Washington's tactic of choice to improve counterterrorism and homeland security has been to reorganize the federal government. The Department of Homeland Security (DHS) was created in 2003 to rationalize assets and centralize activities related to borders, domestic asset protection, preparedness and response, information integration and dissemination, and science and technology. The Office of the Director of National Intelligence (ODNI) was created to better coordinate the fragmented intelligence community

1. Cline, Ray S., "Is Intelligence Over-Coordinated?" *Studies in Intelligence*, Vol. 1, No.4 Fall 1957.

Washington's decision to turn to far-reaching reorganization in response to new national security challenges has significant historical precedent. The National Security Act of 1947 created the Department of Defense (DoD) and the Central Intelligence Agency (CIA) to help the United States meet the security challenges it faced after World War II. It took another decade, however, to establish the North Atlantic Treaty Organization (NATO), deterrence and various other critical institutions and concepts to fight the Cold War effectively. For every step in the right direction, there were missteps, trial and error.² It took another 39 years before Congress passed the Goldwater-Nichols Act to foster "jointness" among the military services, something that Dwight Eisenhower had lobbied for both as a general and as President.

U.S. efforts to address homeland security and counterterrorism represent the most significant federal reorganization since 1947. But the "big bang" creation of both the DHS and DNI are not sufficient. Reorganization is only a step in refashioning government and society to meet the challenges of global terrorism and homeland security. The failures of Katrina demonstrated significant DHS shortcomings in preparedness, response and recovery. Bad intelligence on Iraq's WMD, the slow progress of the intelligence community in retooling to meet terrorist threats,³ and the slow pace of information-sharing initiatives⁴ tell us more about what the DNI still needs to achieve than what it has accomplished.

To meet the demands of counterterrorism and homeland security, the goal of government reform and of new policies and programs is to:

- Provide greater clarity of roles and missions; improve coordination among stakeholders;
- Enhance the speed and decisiveness of decisionmaking; and

2. Carafano, James and Paul Rosenzweig, *Winning the Long War*, Heritage Foundation, 2005, p. 11.

3. Baker, James A. and Lee H. Hamilton, *The Iraq Study Group: The Way Forward - A New Approach*, Page 60. Available at http://www.usip.org/isg/iraq_study_group_report/report/1206/iraq_study_group_report.pdf.

4. Reylea, Harold C. and Jeffrey Seifert, *Information Sharing for Homeland Security, A Brief Overview*, Congressional Research Service, January 10, 2005. Available at <http://www.fas.org/sgp/crs/RL32597.pdf>.

- Promote jointness of purpose within the federal government and between and among the federal government and non-federal actors.

It has become a popular shorthand to describe these aspirations by calling for a Goldwater-Nichols for the homeland. In the 9/11 Commission Report, Secretary of Defense Donald Rumsfeld argued that agencies should “give up some of their existing turf and authority in exchange for a stronger, faster, more efficient government wide joint effort.”⁵ Subsequently, he called for:

*A Goldwater-Nichols process for the national security portions of the U.S. Government.... The broader [U.S. Government] structure is still in the industrial age and it is not serving us well. It is time to consider... ways to reorganize both the executive and legislative branches, to put us on a more appropriate path for the 21st century. Only a broad, fundamental reorganization is likely to enable federal departments and agencies to function with the speed and agility the times demand.*⁶

General Peter Pace, Chairman of the Joint Chiefs of Staff (JCS), similarly argued that the federal interagency process does a good job of presenting the president with options, but that “...once the president decides to do something, our government goes back to stovepipes for execution. Department of State does what they do, DoD does what we do, the Department of Treasury, etc.”⁷

II. Goldwater-Nichols for What?

If Goldwater-Nichols has gained traction in the policy community as an analogy for improving homeland security coordination, it is worth examining what the shorthand implies. Does everyone mean the same thing? What are the limits of the analogy? If the analogy is incomplete or imprecise, what additional or alternative policies need to be pursued to foster “jointness” in U.S. homeland security efforts?

5. National Commission on Terrorist Attacks on the United States, *The 9/11 Commission Report*, W.W. Norton and Company, July 2004, p. 403.

6. Woodward, Bob, “The World According to Rummy,” *Washington Post*, October 8, 2006, p. B05.

7. Garamone, Jim, “Pace Proposes Interagency Goldwater-Nichols Act,” *American Forces Press Service*, September 7, 2004.

To answer those questions, it is worth examining the Goldwater-Nichols Act itself.⁸ Goldwater-Nichols sought to improve coordination and effectiveness within the military chain of command and to improve the joint operating effectiveness of the four military service branches. The defense structure was streamlined and unified, and it became a requirement to align strategy and budgets. The major components of Goldwater-Nichols were to:

- Strengthen civilian authority over the military by affirming the primacy of the Secretary of Defense and designating the JCS Chairman as the prime military advisor to the President, National Security Council (NSC) and Secretary of Defense;
- Clarify the chain of command by creating Commanders in Chief (CINCs)/combatant commanders (COCOMs) with full operational authority and by removing the JCS from the chain of command;
- Create a joint officer management system and joint training programs which tied an individual's career advancement to rotations in billets outside of their own service branch;
- Require the President to annually submit a national security strategy;
- Require the Secretary and JCS chief to align strategy and missions against budgets and resources to ensure efficient use of resources; and
- Seek to improve DoD management and administration.

The first two aspects of Goldwater-Nichols made the military chain of command more effective by delineating clear roles and responsibilities. It is in this area that Goldwater-Nichols is generally considered to have achieved the greatest success.⁹ It is important to keep in mind, however, that Goldwater-Nichols only had to deal with creating the chain of command for a limited set of actors: the civilian leadership of the Pentagon, the Joint Chiefs, and the Service branches.

8. For a fuller discussion and assessment of major components of Goldwater-Nichols, see Locher, James R., III, "Has It Worked? The Goldwater-Nichols Reorganization Act," *Naval War College Review*, Autumn 2001, Vol. LIV, No. 4.

9. Ibid.

Homeland security, on the other hand, involves a far greater number of entities with diverse missions and capabilities. The number and nature of players is far more diverse than what Goldwater-Nichols faced in the military context.

The Department of Homeland Security was created by the combination and reorganization of more than 170,000 employees in twenty-two separate agencies that were formerly in the Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Justice, Transportation, and Treasury, among others. Beyond DHS, and across the federal government, two dozen federal agencies and the military are designated to provide essential support functions for various homeland security scenarios.¹⁰ Outside of the federal government, there are “millions of State and local officials, of which approximately two million are firefighters, police officers, public health officials, [and] EMS professionals who are available to not only respond to events within their jurisdiction, but also respond to events across the country [based on] interstate mutual aid agreements. This “force” of state and local civilian personnel is comparable to the size of the U.S. military.”¹¹ A homeland-security equivalent of Goldwater-Nichols, therefore, would need to attempt to promote jointness at a myriad of levels:

- Within DHS
- Across the federal government
- Among civilian agencies (non intelligence, non-defense)
- Among members of the intelligence community
- Between the U.S. military and federal civilian agencies
- Between federal and non-federal entities
- State and local officials
- The private sector
- NGOs

10. Department of Homeland Security, *National Response Plan*, December 2004, p.33. Available at http://www.dhs.gov/xlibrary/assets/NRP_FullText.pdf.

11. Foresman, George W., “Statement of the Honorable George W. Foresman, Under Secretary for Preparedness, U.S. Department of Homeland Security, Commission on the National Guard and Reserves,” Department of Homeland Security, December 13, 2006.

III. Goldwater-Nichols and the Homeland Security Chain of Command

*Goldwater-Nichols established very, very clear lines of command authority and responsibilities for subordinate commanders, and that meant a much more effective fighting force.*¹²

—General Norman Schwarzkopf
Commander in Chief of CENTCOM
during Desert Storm

A Goldwater-Nichols-like approach to homeland security suggests that a similar opportunity exists to clarify roles and create unified authority within a streamlined homeland security chain of command. Unfortunately, creating a homeland security line of command that matches the clarity of the DoD/military chain of command is probably not feasible. The diverse set of actors and the complex relationships involved in homeland security make the pursuit of jointness a far greater challenge than was faced with Goldwater-Nichols.

The National Response Plan (NRP), required by Homeland Security Presidential Directive/HSPD-5, provided a blueprint for responding to national emergencies and to coordinate the response of various local, state, and federal agencies to natural disasters, terrorist attacks, and other high-consequence events.¹³ Like Goldwater-Nichols for the military, the NRP sought to delineate roles and responsibilities for homeland security and to lay out a definitive chain of command.

12. Ibid.

13. White House, "Homeland Security Presidential Directive/HSPD-5: Management of Domestic Incidents," February 2003. Available at <http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html>. Also see, Bea, Keith, et al., "Federal Emergency Management Policy Changes After Hurricane Katrina: A Summary of Statutory Provisions," Congressional Research Service, RL33729, December 15, 2006. HSPD-5 also established the National Incident Management System (NIMS). NIMS established a framework to guide interagency and intergovernmental responses to complex emergencies. It sought to bring the diverse groups together and better spell out their management roles in a disaster or terrorist attack. The NIMS describes necessary elements of a command structure, but actual structures are not identified ahead of time. It is left up to the participants to work out details and conflicts regarding jurisdiction, roles, and responsibilities at the time of an actual event.

According to the NRP, the Secretary of the Department of Homeland Security holds ultimate responsibility for coordinating all aspects of the federal response to an event of national significance. The NRP indicates that the Secretary can designate a Principal Field Officer (PFO) from any federal agency to act as his representative to coordinate overall federal incident management and ensure seamless integration of federal activities in coordination with state, local, tribal entities, media, non-governmental organizations and the private sector.

As well, the NRP directs the Secretary to assign a Federal Coordinating Officer (FCO) to manage and direct federal assets on the ground at the disaster site.

In effect, the NRP lays out a homeland security chain of command similar to that laid out for the military under Goldwater-Nichols. The Secretary of Homeland Security, or the PFO acting as the Secretary's proxy, plays an equivalent role to the Secretary of Defense, providing civilian leadership for the overall chain of command. The FCO acts as a theater commander and takes on a role similar to that of the CINCs. As well, the NRP borrows a page from Goldwater-Nichols by safeguarding the CINC-like operational prerogatives of FCO by making it clear that the PFO "does not direct or replace the incident command structure established at the incident."¹⁴

The easy comparisons between the Goldwater-Nichols chain of command and the NRP's chain of command end here. The homeland security apparatus is simply not the military. The distributed nature of homeland security assets and actors; the divide between federal and state, local, and private-sector entities; and the unique standalone role of the military prevent federal homeland security officials from having decisive command-and-control authority over assets and actors involved in the homeland security mission.

This fragmentation is evident in the responsibilities that the NRP holds separate from the senior homeland security official/PFO. According to these "carve outs," the DHS Secretary/PFO does not have "directive

14. National Response Plan, *op. cit.*: 33.

authority” over the Senior Federal Law Enforcement Officer (SFLEO),^{15, 16} does not have authority over the state and local incident command structure or other federal and state officials, and “other federal incident management officials retain their authorities as defined in existing statutes and directives.” As well, military assets remain within their own chain of command reporting to the Secretary of Defense and the President.

Similarly, the homeland security FCO role is far weaker than that of the CINC. The FCO does not have authority over federal law enforcement assets (which are directed by the Department of Justice [DoJ]), military assets (which remain under DoD control), or non-federal actors including state, local, tribal and private-sector entities.

The carve-outs in the NRP mean that senior homeland security officials lack control over significant homeland security assets and capabilities: in effect, “you’re in charge of everything, except for the things that you’re not in charge of.” This falls far short of the decisive authority granted to the Secretary of Defense and the CINCs under Goldwater-Nichols.

Herding Cats: Katrina and the Challenge of Coordination

The limitations of the NRP, the lack of definitive chain of command, and the difficulty of coordinating homeland security activities among myriad homeland security actors was in clear evidence during the response to Hurricane Katrina. A number of specific examples of coordination problems between various homeland security actors provides a better understanding of the complexity of the problem.¹⁷

DHS and DoD. Congressional investigations into Hurricane Katrina¹⁸ examined coordination problems between DHS and the DoD. In one

15. Ibid, p. 10. Senior Federal Law Enforcement Official, SFLEO, is part of the Joint Field Office (JFO) structure. The PFO does not have the authority to direct federal law enforcement. There is always a separate law enforcement chain of command.

16. U.S. Congress, “2007 Homeland Security Appropriations Conference Report,” P.L. 109-295, October 2006. p. 43-45. Available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h5441enr.txt.pdf.

17. Most of the examples described herein are drawn from Cooper, Christopher and Robert Block, *Disaster – Hurricane Katrina and the Failure of Homeland Security*, Times Books, Henry Holt and Company, 2006.

18. Select Bipartisan Committee, “A Failure of Initiative, Final Report of the

example, DHS officials conveyed a request from Homeland Security Secretary Michael Chertoff seeking updated information on the New Orleans levees, the status of shelters, and DoD search-and-rescue missions. A response email from the Office of the Secretary of Defense expressed confusion as to why DHS was seeking such information, as the Federal Emergency Management Administration (FEMA, which became part of DHS after DHS' creation) had not yet even generated requests for these missions for DoD. While DoD and FEMA eventually resolved their conflict and worked out a system to streamline communications and requests for aid, initial coordination between the two agencies was poor.

DHS and DoJ. In the original NRP, the DoJ and DHS jointly share responsibility for providing federal support to state and local security and public-safety officials. After Katrina, local authorities were overwhelmed with rescue missions and desperately needed federal assistance to back up state and local police. A senior Immigration and Customs Enforcement (ICE) officer from DHS and the FBI Special Agent in Charge acted jointly as the SFLEO on the ground. Overlapping responsibility and bureaucratic rivalry between DHS and the FBI/DoJ hampered coordination and delayed response. Eventually, the FBI/DoJ took sole control as the SFLEO. When the NRP was revised in May 2006, DoJ was made the sole lead agency for providing federal law enforcement support to state and local officials.¹⁹

Federal and State. Significant coordination issues arose between the federal government and the affected states.²⁰ All aid requests from Louisiana to the military had to pass through FEMA before going to DoD. Exasperated Louisiana officials eventually abandoned the cumbersome process and submitted requests directly to DoD.

Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina," U.S. House of Representatives, 109th Congress, 2nd session, February 16, 2006. Available at <http://a257.g.akamaitech.net/7/257/2422/15feb20061230/www.gpoaccess.gov/katrinareport/cover.pdf>.

19. National Response Plan, op. cit. Also see Department of Homeland Security, "Notice of Change to the National Response Plan," May 2006. Available at http://www.dhs.gov/xprepresp/committees/editorial_0566.shtm.

20. Cooper and Block, op. cit.

Homeland Security Operations Center (HSOC). In the first days after Hurricane Katrina, the HSOC failed to report the levees had broken, even after the National Weather Service had reported the breaches many hours earlier. HSOC leadership repeatedly mistook the New Orleans convention center and the Superdome for the same building, which led to mistakes in estimating the number of people in need of relief and evacuation. The HSOC repeatedly delayed or prevented accurate information reaching more senior decision makers because it refused to trust valuable information that originated from outside of its chain of command and preferred channels.

Federal and Private Sector. Soon after Katrina hit, Wal-Mart called DHS to report looting at one of its stores in New Orleans. A creative DHS employee turned the situation into an opportunity to get Wal-Mart to agree to provide water and other necessary supplies for victims of the hurricane and flooding. In addition, he challenged the company to find a way to track all supplies even though the computer systems were down. DHS would reimburse Wal-Mart later for the costs of whatever it provided. Eventually, the employee was chastised by DHS superiors for circumventing normal procurement channels, and DHS quietly paid Wal-Mart \$300,000 to end the contract.²¹

During Hurricane Katrina, the federal government launched the National Emergency Resource Registry, an online resource to allow companies to offer or contribute goods and services for relief efforts. Nearly 80,000 pledges and donations came in, but DHS acted on fewer than ten percent of the pledges.²² Due to poor communication between the government and the private sector, goodwill either choked the system with unnecessary items or failed to provide what was needed. DHS' web site did not specify what items were needed for collection. No one, for example, foresaw the immense need for diapers and baby formula.

The diverse set of actors and the complex relationships involved in homeland security make the pursuit of jointness a greater challenge

21. Ibid.

22. For a discussion on how the private sector and the federal government can work together using everyday technology to improve homeland security preparedness, see Prieto, Daniel B., "On Harnessing Technology: Why eBay Matters for Homeland Security," *San Francisco Chronicle*, June 23, 2006.

than was faced with Goldwater-Nichols. As such, there are clear limits to the Goldwater-Nichols analogy, and it will only go so far in indicating legislative, policy, organizational, and programmatic fixes for homeland security jointness and coordination. To the extent that the Goldwater-Nichols analogy falls short, it is worth identifying where the analogy is most problematic as well as examining alternative approaches to foster jointness.

Post Katrina: The Limits of an Organizational Fix

DHS and Congress pursued changes to the NRP, FEMA, and the use of the military in a domestic context in an attempt to address some of the chain-of-command problems encountered after Katrina.

Changes to the NRP. After Katrina, criticism of the NRP was widespread. The Office of the Vice President described the plan as an “acronym-heavy document...not easily accessible to the first-time user.”²³ Paul McHale, the Assistant Secretary of Defense for Homeland Defense, argued that, “We have to bring that high-level document down to a more practical level.”²⁴ After Katrina, the NRP was changed to make it clearer and eliminate some of the confusion that arose during Katrina. To address confusion between DHS and DoJ regarding law enforcement activities, the revised NRP designated DoJ as the primary coordinator for law enforcement support functions. The revised NRP also sought to clarify confusion about the respective roles of the PFO and FCO.²⁵

23. Marek, Angie, “Learning the Lessons of Katrina,” *U.S. News & World Report*, June 2006. Available at http://www.usnews.com/usnews/news/articles/060605/5neworleans_2.htm.

24. Bowman, Tom, “Reviews Fault U.S. Disaster Plans,” *Baltimore Sun*. October 2005. Available at <http://www.baltimoresun.com/bal-te.lessons24oct24,0,4703392.story?coll=bal-home-outerrail>.

25. National Response Plan, op. cit. The original National Response Plan was updated to allow further clarify roles and responsibilities and to allow a single individual to act as both FCO and PFO: “The FCO manages and coordinates Federal resource support activities related to Stafford Act disasters and emergencies. The FCO assists the Unified Command and/or the Area Command. The FCO works closely with the PFO, SFLEO, and other SFOs. In Stafford Act situations where a PFO has not been assigned, the FCO provides overall coordination for the Federal components of the JFO and works in partnership with the SCO to determine and satisfy State and local assistance requirements. The Secretary may, in other than terrorism incidents choose to combine the roles of the PFO and FCO in a single individual to help ensure synchronized Federal coordination.

Changes to FEMA. Congress used the 2007 Homeland Security Appropriations Act to legislate changes to the role of FEMA. One change directs the FEMA administrator to serve as the principal advisor to the President, the Homeland Security Council, and the Secretary of Homeland Security on matters of emergency management. The legislative language is almost identical to provisions in the Goldwater-Nichols Act that set forth the role of the Joint Chiefs of Staff in the military command structure.²⁶ In general, this is a beneficial change that adds greater clarity to roles and responsibilities within the homeland security command structure. At the same time, another change allows the President to temporarily elevate the FEMA administrator to the level of a Cabinet official.²⁷ This provision has the potential to confuse matters. If the FEMA administrator were elevated to a Cabinet level position, what would it mean for the authorities of the Secretary of Homeland Security and for the PFO/FCO structure? While the law made sure to reiterate that the FEMA administrator reports to the Secretary of Homeland Security, and that the authority of the Secretary within the President's cabinet remains unchanged, Congress appears

In instances where the PFO has also been assigned the role of the FCO, deputy FCOs for the affected States will be designated to provide support to the PFO/FCO and facilitate incident management span of control."

26. Homeland Security Appropriations Act of 2007, *op. cit.* According to the 2007 Homeland Security Appropriations Act, "(A) IN GENERAL- The Administrator is the principal advisor to the President, the Homeland Security Council, and the Secretary for all matters relating to emergency management in the United States." Furthermore, "(ii) ADVICE ON REQUEST- The Administrator, as the principal advisor on emergency management, shall provide advice to the President, the Homeland Security Council, or the Secretary on a particular matter when the President, the Homeland Security Council, or the Secretary requests such advice. See also, U.S. Congress, "Goldwater-Nichols Act," PL 99-433, October 1986. Available at http://www.jcs.mil/goldwater_nichol_act1986.html. According to the Goldwater-Nichols Act, "(1) The Chairman of the Joint Chiefs of Staff is the principal military adviser to the President, the National Security Council, and the Secretary of Defense. (2) The other members of the Joint Chiefs of Staff are military advisers to the President, the National Security Council, and the Secretary of Defense." Furthermore, "(e) Advice on Request. The members of the Joint Chiefs of Staff, individually or collectively, in their capacity as military advisers, shall provide advice to the President, the National Security Council, or the Secretary of Defense on a particular matter when the President, the National Security Council, or the Secretary requests such advice."
27. Homeland Security Appropriations Act of 2007, *op. cit.*, section 503 (c)(5) "Cabinet Status."

to have opened the door for future uncertainty and confusion in the homeland security chain of command.

The implications of the changes to FEMA are unclear. On the one hand, the change seems to imply a role for FEMA similar to that of the Joint Chiefs of Staff under Goldwater-Nichols, as a “principal advisor” to the White House and the Secretary. At the same time, does FEMA’s increased access to the White House and potential to serve in a cabinet capacity potentially undermine the roles of the Secretary, PFO and FCO, as set forth in the NRP? Do the changes to FEMA add confusion to the already imperfect homeland security chain of command?

Changes to the Domestic Use of the Military. DoD is clearly indispensable when it comes to homeland security. In the midst of a disaster, the public, the media and the government expect the military to take action. DoD’s essential role is reflected in the fact that it is the only federal department that the NRP views as providing essential support functions in all fifteen of its national emergency scenarios.

The role of the DoD in homeland security missions is governed by several important conditions. First, DoD envisions its role as constrained to providing support to civil authorities for emergency management operations during incidents of national significance.²⁸ The limits on DoD to act within the United States stem from a long legal tradition. The Posse Comitatus Act (PCA) of 1878 generally prohibits the military from acting in a law enforcement capacity within the United States. As well, the Insurrection Act seeks to limit the powers of the Federal government to use the military for law enforcement.

Specific exceptions to these constraints include the National Guard, which is allowed to act in a law enforcement capacity while acting under Title 32 or State Active Duty status. As well, the Army can act under Title 10 to provide law enforcement support so long as

28. Department of Defense, *Strategy for Homeland Defense and Civil Support*, June 2005. Available at <http://www.fas.org/irp/agency/dod/homeland.pdf>. See also, NORTHCOM’s description of emergency management operations. Available at http://www.northcom.mil/about_us/vision.htm.

authorities at the State level have explicitly requested such support.²⁹ The Coast Guard is also exempt from the PCA.

In any event, military assets under U.S. Northern Command can only be utilized when directed by the President or Secretary of Defense. As such, they exist in a command structure parallel to and supporting, but not within, the homeland security chain of command established by the NRP.

This arrangement proved successful on some fronts and problematic in others during Katrina.

DoD's deployment of 50,000 National Guard members and 22,000 Title 10 active duty military personnel was the largest and fastest civil support mission ever in the United States.³⁰ During Hurricane Katrina, the Coast Guard and the National Guard operated successfully under Title 32 status. National Guard forces represented more than 70% of the military force for Hurricane Katrina, reinforcing the NRP's designation of the National Guard as the military's first responders to a domestic crisis.³¹ The Coast Guard's flexible, mission-driven approach, ability to work well with other agencies, and history of operating in a domestic context contributed to their effectiveness during Katrina.³²

Nonetheless, Assistant Secretary of Defense McHale³³ admitted that the active-duty military and guard and reserve contingents were not

29. Existing laws, including Title 10, Chapter 15 (commonly known as the Insurrection Act), and the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Title 42, Chapter 68), grant the President broad powers that may be invoked in the event of domestic emergencies, including an attack against the Nation using weapons of mass destruction, and these laws specifically authorize the President to use the Armed Forces to help restore public order.

30. McHale, Paul, Assistant Secretary of Defense for Homeland Defense, speech, "Homeland Defense - Looking Back, Looking Forward," Heritage Foundation, July 14, 2006. Available at <http://www.heritage.org/Press/Events/archive.cfm>.

31. Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, op. cit., p. 202. Available at <http://a257.g.akamaitech.net/7/257/2422/15feb20061230/www.gpoaccess.gov/katrinareport/military.pdf>.

32. Orr, Bob, "Katrina Makes Coast Guard Heroes," *CBS News*, September 19, 2005. Available at <http://www.cbsnews.com/stories/2005/09/19/eveningnews/printable859663.shtml>.

33. McHale, op. cit.

well integrated and not as mutually reinforcing as they should have been. He also conceded that many of the search-and-rescue missions were not executed efficiently, leading to cases where more than one helicopter showed up at the same site. McHale noted that the National Guard needed better interoperability communications and that first responders should communicate seamlessly with the Guard and active duty military forces.

One of the most significant problems faced during Katrina was the trigger mechanism by which military assets are activated in support of homeland security efforts. Much has been made of the critical delay by state officials in invoking federal assistance and how that contributed to delays in rescue and relief missions.³⁴ The White House and Homeland Security officials were under extreme pressure to get control of the situation, but when the President asked the governors of Louisiana and Mississippi to cede their National Guard troops to federal control, both governors refused.³⁵

In response to the conflict between state and federal officials over control of National Guard assets, the 109th Congress modified the Insurrection Act to give the President greater authority to use troops domestically.^{36, 37} Section 1076 of the 2007 Defense Authorization Act gives the President the authority to deploy troops in the event of a rebellion or during disasters when state authorities are overwhelmed and incapable of maintaining public order.³⁸ In those circumstances,

34. Cooper and Block, *op. cit.* p. 213-216.

35. *Ibid.*

36. National Governors Association, "Governors Urge Conferees to Strike Language Federalizing Guard, Reserves During Disasters," September 2006. Available at <http://www.nga.org/portal/site/nga/menuitem.6c9a8a9ebc6ae07eee28aca9501010a0/?vgnextoid=39a9449af77ad010VgnVCM1000001a01010aRCRD&vgnextchannel=759b8f2005361010VgnVCM1000001a01010aRCRD>.

37. Leahy, Senator Patrick (D-VT) speculated that Section 1076 was a direct response to the refusal of Mississippi and Louisiana to cede control of National Guard forces to Federal authority when President Bush requested it. Leahy's statement on the National Defense Authorization act is available at <http://leahy.senate.gov/press/200609/092906b.html>.

38. U.S. Congress, John Warner National Defense Authorization Act for Fiscal Year 2007, S. 2766/ H.R. 5122, 109th Congress. Available at <http://www.govtrack.us/congress/billtext.xpd?bill=h109-5122>. For a general discussion of legal issues and

the President does not have to wait for the state to grant permission to bring in federal troops or to take control of the National Guard.

The military chain of command model, in which the Secretary of Defense and the CINCs have clear and decisive authority over all relevant defense assets, is not readily portable to the homeland security bureaucracy and can not account for military and non-federal assets that will not subordinate themselves to a homeland security chain of command. The lack of a unifying authority makes homeland security distinct from the military.

Going forward, homeland security officials will need to continue to find ways to better coordinate with the military chain of command and military assets. DoD itself will need to continue to clarify its roles and capabilities when it acts in a civil support capacity. As well, the mechanisms by which military assets are utilized by state and local officials, used to support federal homeland security activities, and mobilized by the President for domestic purposes need to be further examined and refined.

IV. Other Goldwater-Nichols Components

Training and Strategic Planning and Budgets

Lacking an easy organizational fix for homeland security, it is essential to focus on measures that can increase the likelihood of efficient collaboration and cooperation. Strengthened “joint-service” training and rotations make sense for homeland security as they proved successful under Goldwater-Nichols.

Human Capital, Training and Rotations

Goldwater-Nichols created a joint officer management system, which included joint training programs and linked individual career advancement to rotations outside of their home organizations. The benefits to homeland security of improved and joint training, out-of-service rotations, and career incentives have been widely acknowledged.

the domestic use of federal troops, see Elsea, Jennifer K., *The Use of Federal Troops for Disaster Assistance: Legal Issues*, Congressional Research Service, September 16, 2005. Available at <http://fpc.state.gov/documents/organization/53685.pdf>.

The Homeland Security Appropriations Act of 2007 sought to promote jointness by providing career incentives for individual homeland security personnel:

*The Rotation Program established by the Secretary shall provide middle and senior level employees in the Department the opportunity to broaden their knowledge through exposure to other components of the Department; expand the knowledge base of the Department by providing for rotational assignments of employees to other components; build professional relationships and contacts among the employees in the Department; invigorate the workforce with exciting and professionally rewarding opportunities.*³⁹

Similarly, other reforms have sought to improve training and create jointness among intelligence professionals, which is essential for counterterrorism and homeland security purposes. The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) requires the ODNI to establish professional intelligence training and to review and revise the curriculum for such training. Additionally, the IRTPA requires the ODNI to provide for the cross-disciplinary education and training of intelligence community personnel, with a particular focus on establishing cross-disciplinary education and joint training.⁴⁰

In practice, joint operating and training efforts for counterterrorism and homeland security are occurring at a number of levels. The FBI's more than 100 Joint Terrorism Task Forces combine federal and local law enforcement professionals to work side by side in shared field offices. The Joint Forces Terrorist Training Center is being developed to combine federal, state, and local first responders to train together to prevent terrorist attacks. In addition, there are 26 Terrorism Early Warning (TEW) Groups modeled after initiatives by the Los Angeles County Sheriff's Department. The TEW Group was started to analyze trends for potential terrorist attacks within Los Angeles but have now been expanded nationwide. These kinds of joint activities are critical

39. Homeland Security Appropriations Act of 2007, op. cit.

40. United States Congress, "Intelligence Reform and Terrorism Prevention Act of 2004," P.L. 108-458 § 1042, December 2004. Available at <http://thomas.loc.gov/cgi-bin/query/D?c108:4:./temp/~c108fz0wAS>.

to ensure that state and local officials are working together to gather information from a wide array of sources.^{41, 42}

Within DHS, training and rotation programs face a number of challenges. Chief among them is the difficulty of creating a stable cadre of career homeland security professionals at a time when DHS, as an organization, is suffering significant integration problems stemming from its creation. DHS continues to suffer retention issues, culture and morale problems,⁴³ heavy reliance on outside contractors and detailees,⁴⁴ shortages of career professionals, and recruiting challenges.⁴⁵

Looking forward, homeland security rotation and joint training programs should be expanded to increasingly include non-DHS agencies involved in homeland security. Programs should regularly provide rotations at other agencies with significant homeland security roles and responsibilities, including Departments of State, Energy, Justice, Defense, Health and Human Services, and the intelligence community, among others.⁴⁶ As well, joint training and rotations should be expanded to increasingly allow temporary personnel exchanges and joint training with state and local offices, the private sector and non-governmental organizations (NGOs).

41. Martin, Robert A., "Joint Terrorism Task Force: A Concept that Works," Anti-Defamation League Law Enforcement Agency Resource Network. Available at <http://www.adl.org/learn/jtjf/default.asp>.

42. Federal Bureau of Investigation, "Protecting America Against Terrorist Attack: A Closer Look at the FBI's Joint Terrorism Task Forces," Federal Bureau of Investigation Press Room, 12/01/2004. Available at <http://www.fbi.gov/page2/dec04/jtjf120114.htm>.

43. Lilly, Scott, "An Analysis of Employee Attitudes at Federal Departments & Agencies," Center for American Progress, October 17, 2005. Available at <http://www.americanprogress.org/issues/2005/10/b1110801.html>.

44. Rabkin, Norman J., "Overview of Department of Homeland Security Management Challenges," U.S. Government Accountability Office, GAO05-573T, April 2005. Available at <http://www.gao.gov/new.items/d05573t.pdf>.

45. Losey, Stephen, "Allen carves out prominent intelligence role for DHS," interview with Charlie Allen, Chief Intelligence Officer, DHS, *Federal Times*, September 04, 2006. Available at <http://www.federaltimes.com/index.php?S=2075300..>

46. Rabkin, op.cit.

Strategy and Budgets

Goldwater-Nichols required DoD to increase its focus on strategic planning. Specifically, it required that the President annually submit to Congress a comprehensive report on U.S. national security strategy. The requirement was augmented and refined over the years with the establishment of the Future Years Defense Program (FYDP)⁴⁷ and with the Quadrennial Defense Review in 1996.⁴⁸

The Homeland Security Act of 2002 requires the DHS to prepare a Future Years Homeland Security Program similar to DoD's FYDP. Congress amended the Homeland Security Act with the Homeland Security Financial Accountability Act of 2004⁴⁹ to make more specific the requirements on DHS to develop long-term strategies, establish priorities, and tie strategies and plans to budgets and resources.

DHS' ability to deliver robust strategies, plans and budgets remains very much a work in progress. We continue to lack a sensible long-term homeland security planning process as well as the ability to measure the performance and efficacy of homeland security programs against objective benchmarks. Congress has yet to require DHS to undertake periodic strategic reviews⁵⁰ similar to the Quadrennial Defense Review required of the DoD.

Currently, defense planning documents treat homeland security as an afterthought: "They are treated, if at all, as separate line items buried deep within the budget."⁵¹ Nor is there mechanism to assess how

47. Taibl, Paul, "The \$60 Billion Defense Modernization Goal: What, When, How Risky?," *Business Executives for National Security*, March 1998. Available at http://www.bens.org/tail_brief1.html.

48. National Defense Authorization Act of 1996, Public Law 104-201, "Subtitle B-Force Structure Review," sections 921-926. Available at http://www.fas.org/man/docs/qdr/quad_leg.html.

49. U.S. House of Representatives, "Department of Homeland Security Financial Accountability Act," H.R. 4259, Public Law No: 108-330, October 2006. Available at <http://www.govtrack.us/congress/bill.xpd?bill=h108-4259>.

50. See, for example, the National Strategy for Homeland Security Act of 2004, S 2708. The bill, sponsored by Senator Lieberman (D-CT), was read twice and referred to the Senate Committee on Government Affairs but never became law. Available at <http://www.govtrack.us/congress/bill.xpd?bill=s108-2708>.

51. Peters, John E., "Understanding homeland Security," RAND Corp., 2002, based

DoD and DHS fit together in the overall national security equation.⁵² Congress should require DHS to conduct quadrennial reviews to assess homeland security risks, strategies, structures, resources, and effectiveness, as well as associated planning budgets.⁵³

V. Beyond Goldwater-Nichols: Network-Centric Homeland Security

The tension between centralization/hierarchy and flattening and empowering distributed nodes in an organization is age-old. It has posed a dilemma ever since the advent of modern organizational and management theory. The problem is well known: Unity of command can lead to excessive chains of authority which hinder communication, innovation and flexibility. Conversely, too much flexibility can lead to lack of decisiveness and create conflicting or inefficient efforts.

Dramatic changes to information technology over the last decade have made distributed models of management increasingly viable as an alternative or a complement to more traditional hierarchical management models. The implications of those changes are in their early stages in the military sphere, and are directly relevant to the homeland security realm.

In general terms, individuals empowered with computing and communications technology and connected by networks 1) have a greater capacity to do more for and by themselves; 2) can do more in loose collaboration with others without having to be organized in traditional hierarchies; and 3) can be more effective within formal hierarchies owing to faster and more efficient information distribution, communications, collaboration, innovation and decision-making.⁵⁴

on excerpts from *Preparing the US Army for Homeland Security: Concepts, Issues and Options*, Eric V. Larson, and John E. Peters, RAND, 2000. Available at <http://www.fathom.com/course/21701714/session5.html>.

52. Carafano, James J., "Seeing the Big Picture: Homeland Security Lacks Unified Control," *Defense News*, March 28, 2005. Available at <http://www.defensenews.com/story.php?F=748746&C=commentary>.

53. Ibid. See also, Housman, Robert, "A Homeland Security Agenda for the First 100 Days of a Democrat-Led Congress," *Homeland Defense Journal*, December 2006.

54. For academic analyses of the social impacts of networks, see, for example, Benkler, Yochai, *The Wealth of Networks: How Social Production Transforms Markets and*

The inherently fragmented nature of the homeland security landscape makes it necessary to find ways to achieve greater unity of effort from actors and assets distributed widely among the federal civilian bureaucracy, the military, federal law enforcement agencies, state and local governments and law enforcement, the private sector, and NGOs.

Given the limits of a top-down Goldwater-Nichols-like approach to streamline the homeland security chain of command, homeland security should look to other areas of military doctrine for valuable approaches, strategy and lessons. Current doctrines of Network-Centric Warfare (NCW) are highly relevant to the homeland security context. NCW recognizes the limits of hierarchical command and control structures and seeks to improve decision-making by leveraging improved information and communications among participants distributed throughout a network.

The implications of networked technologies for military operations began to come to the fore in the mid-1990s. The military's concept of NCW first appeared in the open literature in 1998.

NCW promises faster, more precise, more decisive operations thanks to information sharing....NCW is oriented to increasing the operational freedom of choice for military commanders...[At the same time] the military context is an environment of strict control and direction....If too much operational freedom is delegated to subordinate units, control is lost to commanders; if too much control is retained, operational flexibility is compromised.⁵⁵

NCW has also been defined as "the conduct of military operations using networked information systems to generate a flexible and agile military force that acts under a common commander's intent, independent of the geographic or organizational disposition of the individual elements, and in which the focus of the war fighter is broadened away from individual, unit or platform concerns to give primacy to the mission and responsibilities of the team, task group or coalition."⁵⁶

Freedom, Yale University Press, May 16, 2006. p. 8.

55. Mitchell, Paul T., "Network Centric-Warfare: Coalition Operations in the Age of U.S. Military Primacy," Adelphi Paper 385, International Institute for Strategic Studies, December 2006. p. 27-32.

56. Fewell, M.P. and Mark G. Hazen, "Network Centric-Warfare - Its Nature and

Applied to homeland security, a network-centric approach would mean that the right information must be available to the right people at the right time in the right form, but also it must be put to the right use. It is essential to note that network-centricity is not just about technology and gadgets. Human aspects and relationships are essential. The numerous examples of poor coordination during the response to Katrina illustrate the value of information sharing, empowerment of individuals in the field, and distributed decision-making in the absence of clear unified command authority.

Various components of a network-centric homeland security framework are arguably in place. At a policy level, law and executive orders have called for greater cross-organizational collaboration for counter-terrorism and homeland security via improved business practices and network technologies.⁵⁷ Organizationally, national strategy documents have endeavored to streamline the homeland security chain of command to the greatest extent possible.⁵⁸ At the same time, nascent technology programs are seeking to better link federal and non-federal actors.^{59, 60} Finally, new initiatives are creating intermediate hubs between the federal government and society at large. These intermediary or regional nodes can help distribute information from the federal government to the field; collect, vet and improve information that is sent from the field up the official chain of command; and distribute information laterally to other intermediary/regional nodes.⁶¹

Modeling,” September 2003. Available at <http://www.dsto.defence.gov.au/publications/2596/>.

57. 2004 Intelligence Reform and Terrorism Prevention Act, op. cit. The act calls for the creation of an Information Sharing Environment (ISE) and the creation of the ISE Program manager. See also White House, Executive Order 13356 on “Strengthening the Sharing of Terrorism Information to Protect Americans,” August 2004. Available at <http://www.fas.org/irp/offdocs/eo/eo-13356.htm>.
58. National Response Plan, op. cit. Also see Notice of Change to the National Response Plan, op.cit.
59. Department of Homeland Security, “Homeland Security Information Network,” Available at <http://www.dhs.gov/xinfoshare/programs/>.
60. Thompson, Clive, “Open Source Spying,” *New York Times Magazine*, December 3, 2006. Available at <http://www.nytimes.com/2006/12/03/magazine/03intelligence.html?pagewanted=1&ei=5090&en=46027e63d79046ce&cex=1322802000>.
61. Allen, Richard and Floyd Kvamme, “Regionalizing Homeland Security: Unifying

While nascent, many of the structures for an effectively self-governing network-of-networks for homeland security are being put in place today. One can envision a future where the lack of unitary authority within the homeland security chain of command does not lead to coordination failures in the field following an incident of national significance. Instead, what we lack in definitive homeland security command and control is more than made up for by empowered individuals and nodes in the network. Over time, homeland security players will build established trusted relationships across traditional bureaucratic, regional, and sectoral (e.g. private vs. governmental) boundaries and seams. As well, we will be better able to create effective ad-hoc teams post-disaster because of a more mature set of intermediary institutions, better technology, and a greater ability by Washington to accept that homeland security will never be a unified system, but rather a system of systems, and to increasingly trust information origination and decision-making outside of traditional hierarchies and stovepipes.

In fact, the concept of 'network-centric homeland security' akin to 'network-centric warfare' may be a far more effective model than Goldwater-Nichols to improve homeland security going forward. NCW concepts are highly applicable in a homeland security environment where assets are broadly distributed across a myriad of actors who do not fall under a unified chain of command. Such an approach recognizes the limits of top-down fixes to an environment where the federal government does not have command authority over all of the necessary homeland security assets and capabilities, and where operational effectiveness will be more about collaboration and cooperation than about command and control.

VI. Conclusion

Goldwater-Nichols's ability to improve military jointness relied primarily on its ability to streamline the military chain of command and clearly define roles and responsibilities among key stakeholders. Its successful focus on inter-service rotations and joint training helped reduce inter-service rivalry and foster greater cooperation. Goldwater-Nichols also

National Preparedness and Response," June 30, 2006. Available at http://www.gwu.edu/~dhs/reports/hspi_region_7_10_06.pdf.

stressed the need to focus on strategic planning and align strategies with resources.

While Goldwater-Nichols can provide general lessons to improve homeland security coordination and effectiveness, its ability to serve as a comprehensive model for homeland security reforms has its limits. This paper comes to conclusions and makes recommendations in four areas.

First, homeland security will not be able to develop a chain of command that begins to approach the military command structure articulated in Goldwater-Nichols. Civilian agencies will simply not respond like a military organization. Senior homeland security officials do not wield command authority over components of other federal departments. The military chain of command is separate from the homeland security chain of command. The NRP explicitly put DoJ in charge of federal law enforcement efforts. State, local, private sector and NGO assets do not take orders from DHS. While fixes to the NRP since Katrina address some of the coordination and decision-making problems exposed by Katrina, they obscure the fact that the clarity and decisiveness embedded in the military chain of command by Goldwater-Nichols is unachievable for homeland security.

Second, efforts at homeland-security joint training and rotations need to mature and be increasingly extended beyond DHS and the ODNI. Joint training and rotation programs should provide greater exposure to the full range of federal, state, local and non-governmental actors that play an important homeland security role. Employee turnover at DHS needs to be reduced and recruitment improved in order for joint training and rotations to have the intended effect on promoting jointness within a professional homeland security cadre.

Third, to improve homeland security coordination and effectiveness, it is essential to develop processes for long-term strategic planning. In the absence of a robust strategic planning process, too many homeland security programs are ad hoc, reactive, and do not contribute to a coherent vision. Strategies should be based on comprehensive and up-to-date threat and vulnerability assessments, establish clear national priorities, provide definitive guidance for action, and establish goals

against which activities and programs can be measured. Strategic plans should be tied to robust assessments of capabilities and to a multiyear budgeting process that aligns missions and resources. Congress should require DHS to conduct quadrennial homeland security reviews. Congress should press DHS to fully meet their statutory requirement to produce multiyear budgets in the form of a Future Years Homeland Security Program that links operational and financial requirements together to meet strategic goals. It is essential that a homeland security strategic planning and budgeting process also be informed by the strategic planning of the DoD. Homeland security, homeland defense, and national security must all be viewed as part of a whole. The full national security game plan must do a good job of integrating both offense and defense.

Fourth, since Goldwater-Nichols does not provide a model for the kind of management that homeland security will require, policymakers should increasingly look to current military doctrines of NCW to improve homeland security coordination and management. The wide variety of actors—within federal civilian agencies, the military, federal law enforcement and intelligence, within state and local governments and law enforcement, and outside of the government in the private sector and NGOs—strongly suggest that homeland security will never achieve unified authority like that which exists in the military chain of command. When future disasters strike, the homeland security chain of command will remain fragmented, and management will necessarily be based more on matrixed management than on command and control authority. With centralization of authority unachievable, homeland security will need to rely on distributed but coordinated management. Achieving that requires creating trust among homeland security stakeholders, efficient communication between players at multiple levels, an ability to rely on the edges of the network to gather information, and an empowerment of the edges of the network to make decisions based on the best available local knowledge but within the framework of the overall mission. To complement and address the limits of a Goldwater-Nichols approach to homeland security, the concept of “network-centric homeland security” should increasingly play an important and guiding role.



Chapter Three



*Creating a State and Local Preparedness
Revolution*



Foreword

JAMES S. GILMORE

Former Governor of the Commonwealth of Virginia
National Council on Readiness and Preparedness

How ironic it is that during the Cold War, we thought that if we contain the spread of Communism and promote peace, there would be a more wonderful world. The events that took place not too many years after the end of the Cold War demonstrated that this was not to be the case. Today there are great challenges to the security and lives of the American people; a new threat by international movements that use individuals to potentially infiltrate our communities, to strike at us in stealth attacks using modern weapons and technology, which threaten our very homes and families.

Today's generation is left to cope with this new concept of terrorism. The transformation of the National Guard and Reserves in light of the War on Terror will have to be based upon how we are going to define our society. How the society of the United States responds to these challenges will decide what America will look like in the future. Right now, with respect to the issue of using the military in the homeland, there is tension between American instinct to confront challenges and to fix them. This tension has come up in our "managerial society" many times. The great American instinct is to fix a problem, no matter what the cost. The challenges we have to face are the conflicts between the values of our traditional freedoms, and how they will change in the wake of the War on Terror.

The only way to approach this challenge is to analyze exactly how we should structure a program for using the military in the homeland. This issue is very near and dear to my heart. There are some great, major policy issues before us today due to the attacks of 9/11 and the War on Terror. The War is a major conflict that in its nature is one of culture and civilization. We can only dimly see the direction in which

we should be heading, which leaves us tied up when it comes to doing what is needed to face the current challenges and crises. There needs to be more national attention on preparedness and readiness, so that we do not fail as a society when we take appropriate response within the homeland.

I was Chairman of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, which is impossible to create an acronym for, so it was just called the Gilmore Commission. This was a three-year Commission that was required by law to respond to Congress every December. The Commission's reports were published by the RAND Corporation, and have so far stood the test of time. Also, many of the Commission's recommendations have been adopted.

In our first year, we assessed the threat and found it to be very grave. We sensed that there was likely an attack on the United States coming. The second year, we defined what needed to be done to establish a national strategy in the likelihood of such an attack. The third year, which was 2001, we observed that there was still no national strategy which could help to prevent an attack, nor any process to deal with it.

We suggested five key components that would help to shape a national strategy. The first was how to use state and local authorities; next, we looked at the health care system in the country to see if the public health care program was prepared to handle a major attack. The third area we noted was that U.S. border control was far too porous, making it easier for individuals to sneak across our southern border. Cyber-security was the fourth area we analyzed.

The most important aspect was the fifth, which was the use of the military within the homeland. The questions that confronted us were 'How do you use it?' and 'How don't you?' The philosophy of the Commission was that we should be very cautious when using the regular military within the homeland. The use of the military has proven to be dangerous historically, and so must be treated with the utmost respect.

Instead of the regular military, we must rely on state and local responders—police, fire, and rescue units—to deal with catastrophes. We must help them get equipped, trained and prepared to deal with any circumstances that arise. These are the individuals who, in fact, respond after catastrophe strikes. Second, only when these elements are unable to control the situation, should the Reserve components be called in; particularly the National Guard, since their control lies in the hands of the state governor. We should focus along the lines of a civil response, in order to support the local authorities. The only time the regular military should be called in is when there is a need for specialty units who are already trained and equipped to handle nuclear, chemical, or biological attacks. Control of the situation should not be turned over to the military except as a last resort. During the time the Commission met, the Department of Defense agreed with the finding that the focus should be upon the local elements.

I helped establish the National Council on Readiness and Preparedness because of my abiding sense that the country was not focused upon the challenges that we face of preparing state and local responders. Individuals would say to me ‘Get real Jim, you can’t depend on state and local responders. They’re local cops. They’re local fireman. You can’t really depend on that in a time of a national crisis. You’re going to have to use the 101st Airborne when the crunch really comes. That’s the reality.’ My response to that has been that we are then failing ourselves as a society to prepare ourselves with what I feel is an appropriate response. That response should be one that relies more on the local community than upon the military.

At the Department of Homeland Security, there is currently an attempt to develop a Citizens’ Corps to engage regular citizens in national emergency response. Individuals like local current and former health care providers or anyone with an ability to contribute, would be employed in the emergency response process, to provide support during a mass crisis. There also needs to be representative in every corporation; not only for business continuity purposes, but to fit into the larger response plan for the community. There also needs to be a build-up of state and local responders, as well as intense training, to enable communities to be able to respond using this type of system.

The challenge we face today is how to make policy decisions and how we deal with potential disasters as they occur. We need to find an answer as to how we make sure we're prepared to respond appropriately and to prepare to any crisis that we may face. That is what we are here to discuss and analyze today. The military does have a role to play in this process. The question is how do we define it?

Today's guerrilla-type warfare against terrorism calls for us to use all the elements of national power—soft, economic, military and diplomatic—to remain ahead of those who intend to cause fear and harm within the country. During the Cold War, we were considered righteous in our actions. We have an obligation to the people of the United States to be as prepared as we can be. Only then will Americans understand what their role is, and begin to define the challenge they face from overseas. When that is done, only then will the people of the United States be prepared mentally to understand the challenges they face. This is a necessary element to begin removing the fear and anxiety within our society, and to get citizens to begin to feel secure. Only through this change in mentality will we be able to maintain the freedom and liberties of the American people.

Equipping the Army National Guard for the 21st Century

MACKENZIE M. EAGLEN

Senior Policy Analyst for National Security
The Heritage Foundation

The Army National Guard does not have an equipment modernization program of its own that is specifically designed to meet its unique needs and capabilities. While not ideal, the lack of a modernization program was acceptable when the National Guard was primarily an adjunct force to active units, for use typically in the later stages of conflict. Over the past five years, however, the Army National Guard has contributed nearly half of all Army troops on the ground in Iraq and has assumed an increased role in homeland defense missions.

Somewhat surprisingly, the Army National Guard currently faces a severe shortage of available equipment within the United States. The equipment that is available is typically older, more difficult and expensive to maintain, and not easily deployable or useful in all types of domestic missions. The lack of equipment is negatively affecting readiness.

The Army National Guard needs its own modernization program to buy the equipment that meets both the low-end and high-end mission needs unique to the Guard. The common sense solution to, and only affordable option available for, this equipment modernization program is the Army's Stryker Brigade Combat Team model.

The Army National Guard

The Army National Guard is a dual-purpose force of approximately 350,000 citizen soldiers. While the Guard is considered part of the Reserve Component of the U.S. military, it operates under a unique

legal status because the Posse Comitatus Act does not apply to National Guard troops during domestic missions while under state control.¹

Depending on the situation, National Guard units conduct both federal and state missions, from major combat operations overseas to domestic emergency response. Since 9/11, National Guard units have served in major combat operations, including Operations Enduring and Iraqi Freedom, and have participated in domestic missions, such as the response to Hurricane Katrina, Operation Noble Eagle, border security, counter-drug, disaster preparedness and response, and civil support teams. Twenty-three of the state adjutants general also wear a second hat, simultaneously serving as state directors of emergency management or homeland security.²

A Perfect Storm: Army National Guard Equipment Shortfall

The National Guard's high operational tempo and increased missions have not yielded substantial additional funding and resources, especially in regard to equipment. The demands of overseas missions, particularly in Iraq, have badly depleted the Guard's domestic store of vehicles, weapons, and communications gear, leaving units with one-third of the equipment needed to meet requirements for homeland defense missions. Chief of the National Guard Bureau, Lieutenant General Steven Blum, confirmed that in September 2001 the Guard had 75 percent of its needed equipment "on hand." Today, that number is less than 35 percent.³

Several factors have contributed to the equipment problem. Active duty Army units have traditionally been regarded as "first to fight" and therefore receive the lion's share of funding and equipment. Under this doctrine, the National Guard and Reserves are equipped on a tiered readiness scale after active units have received their equipment.

-
1. James Jay Carafano, Ph.D., "Critics of the Hurricane Response Miss the Mark in Focusing on Posse Comitatus," Heritage Foundation *Executive Memorandum* No. 983, October 3, 2005, p. 1, at www.heritage.org/Research/HomelandDefense/upload/83429_1.pdf.
 2. Lieutenant General H. Steven Blum, "Executive Summary," in National Guard Bureau, "2007 National Guard Posture Statement," pp. 1–4, at www.ngb.army.mil/resources/downloads/2007posturestatement.pdf (November 8, 2006).
 3. *Ibid.*, p. 2.

However, this does not guarantee that the remaining gear is enough to fully equip the Army's Guard units.

Moreover, similar policies of "cascading modernization" tend toward equipping "first to fight" units with the newest state-of-the-art equipment, while Guard units typically receive hand-me-down equipment.⁴ This approach results in National Guard units equipped with vehicles and gear that are worn out, dated, and not as easily supported by logistics structures. For example, some Army National Guard units still use M35 series trucks, M113 armored personnel carriers, and the older M1 tanks with 105mm guns. Other Guard units still rely on radio equipment that cannot change frequencies, use outdated encryption technology, and cannot communicate effectively with active Army units or first responders.

The Army's Force Generation model—designed to schedule more predictable deployments for troops and their families and better equip units preparing to deploy overseas—only exacerbates the problem. The Army provides equipment and other resources to units that are preparing to deploy from units remaining stateside. To meet combatant commanders' mandates that National Guard units deploy with 90 percent–100 percent of their required equipment, the Guard and Reserves have been transferring equipment from non-deployed units to those preparing to deploy to make up for severe shortfalls. As of July 2005, the Army National Guard had transferred over 101,000 equipment items to units deploying overseas, exhausting its inventory of some critical items, such as radios and generators, in non-deployed units.⁵

Transferring equipment from a non-deployed unit to one that is about to leave the U.S. causes a vicious cycle that continues with future deployments, incurring additional disastrous effects on unit

-
4. James Jay Carafano, Ph.D., "The Army Reserves and the Abrams Doctrine: Unfulfilled Promise, Uncertain Future," Heritage Foundation *Lecture No. 869*, April 18, 2005, p. 9, at www.heritage.org/Research/NationalSecurity/hl869.cfm.
 5. U.S. Government Accountability Office, *Plans Needed to Improve Army National Guard Equipment Readiness and Better Integrate Guard into Army Force Transformation Initiatives*, GAO-06-111, October 2005, pp. 3–4, at www.gao.gov/new.items/d06111.pdf (November 7, 2006).

preparedness. Lieutenant Colonel Thomas Plunkett III of the Louisiana Army National Guard tells of his battalion's being called up for deployment to Iraq in 2004 just "one month after he had been ordered to give up his machine guns and other equipment to an Arkansas unit that was deploying sooner."⁶ As a result, his unit had very little training time with the gear that they took to Iraq because they received it just prior to deployment. This story is all too typical for Army National Guard units being called up for overseas combat missions.

In addition, as the conflict in Iraq becomes more protracted, the Guard has had to leave much of its equipment in Iraq so that it can be used by subsequent deploying units. The U.S. Government Accountability Office (GAO) estimates that since 2003, Army National Guard units have left over 64,000 items valued at over \$1.2 billion overseas. Non-deployed Guard units now face significant equipment shortfalls primarily because:

1. Prior to 2001, most Army National Guard units were equipped with only 65–79 percent of their required wartime items; and
2. Guard units returning from overseas operations, most notably in Iraq, have left behind equipment such as radios and trucks for follow-on forces.⁷

The Army's current model for distributing equipment does not account satisfactorily for the possibility of wars lasting four or more years. The Army's current policy is to call Guard and Reserve forces to active duty once every six years. At one point in 2005, half of all combat brigades in Iraq (over 40 percent of all U.S. military personnel in country) were from the Army National Guard. With no substantial reduction in U.S. troop levels in Iraq for the foreseeable future, and with active units being deployed at such a high rate in 2006—in part to relieve the strain on the Guard and Reserves—it appears increasingly likely that the Guard will need to be deployed again to maintain the necessary

6. Steve Liewer, "Reserves Spell Out Problems to Panel," *The San Diego Union-Tribune*, September 22, 2006.

7. David M. Walker, "Reserve Forces: Army National Guard's Role, Organization, and Equipment Need to Be Reexamined," testimony before the Committee on Government Reform, U.S. House of Representatives, October 20, 2005, at www.gao.gov/new.items/d06170t.pdf (November 8, 2006).

troop levels in Iraq, assuming that troop levels remain at or near their current numbers. As a result, the Pentagon may have to abandon the deployment policy that limits the involuntary recall of Guard members for 24 cumulative months.

If the major assumptions in the model used to determine what equipment goes to Reserve Component units are flawed, the National Guard, which is already suffering from a more severe equipment shortage than the active Army, will continue to fall behind in terms of equipment and readiness. General Blum has stated repeatedly that the Army National Guard will need at least \$21 billion to reset and buy the equipment that it needs to do its job.⁸

This multifaceted problem extends beyond the Guard's older gear and equipment shortfalls for domestic mission requirements. Department of Defense Directive 1225.6, *Equipping the Reserve Forces*, requires that replacement equipment be delivered to Reserve units for equipment transferred to the active Army for longer than 90 days. Many equipment transfers were never accounted for properly, and as of June 2006, few plans to replace equipment had been drawn up by the Army, and even fewer had been approved.⁹

Army National Guard Readiness

According to the GAO, the National Guard was forced to transfer large numbers of personnel and equipment among units to provide forces ready to deploy. This has only worsened the existing shortages of equipment for non-deployed units. As a result, "the preparedness of non-deployed units for future missions is declining."¹⁰ With over 53,000 National Guard personnel currently deployed for federal

8. National Guard Association of the United States, "Blum: Equipment Shortages Crippling Army Guard Readiness," *NGAUS Notes*, August 4, 2006, p. 1, at www.ngaus.org/ngaus/files/ccLibraryFiles/File/000000001709/nnnotes080406.pdf (November 8, 2006).

9. Janet A. St. Laurent, "Army National Guard and Army Reserve Readiness for 21st Century Challenges," testimony before the Commission on the National Guard and Reserves, GAO-06-1109T, U.S. Government Accountability Office, September 21, 2006, p. 11, at www.gao.gov/new.items/d061109t.pdf (November 8, 2006).

10. Walker, "Reserve Forces."

missions and thousands more responding to recent natural disasters at home, Army National Guard units cannot afford to operate without all of their equipment stateside.¹¹

In the National Guard's 2007 Posture Statement, General Blum noted that "morale suffers when Soldiers cannot train for their wartime or domestic missions for lack of equipment"¹² Readiness is typically measured by evaluating personnel, training, and the availability of equipment and capabilities needed to support joint operations. Readiness can then be broken down into two broad categories: near-term and far-term. Standards such as unit C-ratings, recruiting goals met, retention, operational tempo, reserve component full-time manning, and installation operations measure near-term readiness. Far-term readiness is measured by additional metrics, such as post facilities, military construction, recapitalization and modernization of equipment, and research and development.¹³

Lieutenant General Clyde Vaughn, Vice Chief of the National Guard Bureau and Director of the Army National Guard, recently commented on the state of the Guard: "From July 2002 through September 2005, overall unit readiness decreased by 41 percent in order to provide personnel and equipment to deploying units."¹⁴ If the preparedness of Guard units is declining and morale is suffering, the ability of the Army National Guard to respond quickly and effectively to domestic emergencies may also be declining. The familiarity of soldiers with their equipment improves both morale and deployment readiness. To remain a trained and ready force, the Army National Guard needs to have the right mix of capabilities and as much equipment as possible available in the U.S.

11. National Guard Bureau, "Army National Guard Fact Sheet: Army National Guard (FY2005)," May 3, 2006, p. 7, at www.ngb.army.mil/media/factsheets/ARNG_Factsheet_May_06.pdf (November 8, 2006).

12. Blum, "Executive Summary," p. 4.

13. Mackenzie M. Eaglen, "A New Look at Readiness: Solving the Army's Quandary," Association of the United States Army *National Security Watch* No. 01-1, March 30, 2001, p. 1, at www.ausa.org/PDFdocs/NSW01-130mar01.pdf (Nov. 8, 2006).

14. Lieutenant General Clyde A. Vaughn, Vice Chief, National Guard Bureau, "Serving a Nation at War: At Home and Abroad," in National Guard Bureau, "2007 National Guard Posture Statement," p. 8.

The Need for Dual-Use Equipment

According to the Congressional Research Service (CRS), “it has been reported that National Guard units responding to Katrina did not have adequate numbers of tactical radios or High Mobility Multi-Wheeled Vehicles...adapted for high water operations because this equipment was in Iraq.” Additionally:

*The extent of the resources needed to deal with the consequences of Hurricane Katrina, on top of the requirements for combat operations in Iraq and Afghanistan, raises the question of what resources would be available in the event of another almost simultaneous catastrophic event.*¹⁵

The recent missions of the Army National Guard highlight the need to provide equipment to the Guard that can be used in all of its mission areas, from domestic disaster response to warfighting. To provide the right type of equipment, it is important, first, to identify the types of capabilities that will be needed for the dual missions of the Army National Guard.

In responding to domestic emergencies, such as a flood or an earthquake, the Guard must possess three core competencies: medical services, security, and critical infrastructure skills.

- Medical teams need to be developed that can deploy on extremely short notice and administer mass-casualty care to victims on site using existing facilities.
- While operating in the chaotic environment of a post-disaster area, Guard units must be able to work with local law enforcement in establishing and maintaining security and order.
- Finally, to facilitate a “return to normalcy,” essential services and critical infrastructure must be available. The National Guard, when partnered with the U.S. Army Corps of Engineers and Federal

15. Steve Bowman, Lawrence Kapp, and Amy Belasco, “Hurricane Katrina: DOD Disaster Response,” Congressional Research Service *Report for Congress*, September 19, 2005, pp. 15 and 16, at www.fas.org/sgp/crs/natsec/RL33095.pdf (November 8, 2006).

Emergency Management Agency, provides the type of expertise and force structure required to speed the recovery of a disaster area.¹⁶

For the National Guard to be able to fulfill both its domestic and overseas wartime mission requirements, Guard leadership identified the “Essential 10” equipment needs. These 10 areas represent the \$4 billion shortfall that the Guard needs to address in order to meet both Air and Army National Guard force modernization needs. This funding shortfall does not include the \$21 billion needed for National Guard equipment repair and reset. The Guard’s “Essential 10” areas are:

- Joint headquarters and command and control
- Civil support teams and force protection
- Maintenance
- Aviation
- Engineer
- Medical
- Communications
- Transportation
- Security
- Logistics¹⁷

These essential components appear to take into account domestic mission capabilities. Equally significant is that the “Essential 10” areas do not entail single-use gear (capabilities that are useful for only one type of mission). The emphasis on dual-use equipment is critical to National Guard modernization because it means that troops will train and deploy with the same gear for both domestic and overseas missions. General Vaughn argues that dual-use equipment “ensures interoperability with

16. James Jay Carafano, Ph.D., “Shaping the 21st Century Role of the National Guard and Reserves,” testimony before the Commission on the National Guard and Reserves, May 4, 2006, at www.heritage.org/Research/HomelandDefense/tst050406a.cfm.

17. National Guard Bureau, Office of Legislative Liaison, “National Guard Equipment Requirements: ‘Essential 10’ Equipment Requirements for the Global War on Terror,” March 16, 2006, at [www.ngb.army.mil/lll/analysis/docs/07/essential10_equiplist\(Mar06\).pdf](http://www.ngb.army.mil/lll/analysis/docs/07/essential10_equiplist(Mar06).pdf) (November 8, 2006).

the active force and increases the Army National Guard's ability to respond to natural disasters or in a homeland defense role."¹⁸

The Need for a Unique Equipment Modernization Program

A new paradigm is needed to ensure that the Army National Guard receives a long-term commitment of resources and funding to rebuild and modernize its equipment. The extent of the resources needed to deal with the domestic emergencies—on top of the requirements for combat operations—demands that the National Guard receive an adequate supply of equipment, a proper mix of capabilities, and the most recent technologies. The Stryker Brigade Combat Team, already used by some active Army units, is a proven model that should be employed to modernize and equip the Army National Guard.

The Stryker unit is a wheeled combat force that is highly mobile and transportable in C-130, C-5, or C-17 aircraft. The Stryker Brigade Combat Team is fast, maneuverable, and includes large numbers of infantry that are particularly suitable for missions within cities and towns like Baghdad or New Orleans. The Stryker platform includes medical evacuation, reconnaissance, fire support, engineer squad, and troop carrier variants. Other benefits include mobile command and control, larger evacuation capacity than other combat vehicles, rapid deployment (no heavy transport required and no damage to roads), and protection for rescue and crowd control missions.

The Stryker framework offers a middle ground of capabilities between heavy and light forces to fulfill all the missions of the Army National Guard. An approach based upon the Stryker model would:

1. Provide a better mix of capabilities to the Army National Guard to conduct state missions that complement the Guard's federal missions;
2. Utilize existing proven technology;
3. Provide savings in reduced training expenses as compared to the National Guard's current heavy mechanized units; and

18. Vaughn, "Serving a Nation at War: At Home and Abroad" in "2007 National Guard Posture Statement," p. 8.

4. Offer both a near-term answer and a long-term solution to many of the Army National Guard's equipment problems.

The Stryker's equipment and vehicle composition are ideally suited for domestic and overseas missions. The Stryker Brigade Combat Team can participate in wartime missions as a subordinate unit or in stability and support operations. The Stryker unit also has unique reconnaissance and networked communications capabilities that provide a "system of systems" approach to comprehensive situational awareness through interlinked command and control capability. These teams have chemical, biological, and hazardous material detection and containment abilities and can be organized with other units and technologies based on specific mission requirements (e.g., adding helicopters), thereby augmenting already existing capabilities. Finally, the Stryker model allows for units to be retrofitted with newer technology as it becomes available.

A Time for Action

Congress and the Administration have a window of opportunity to replace the National Guard's equipment comprehensively and systematically by modeling the Army's successful Stryker Brigade Combat Team. Secretary of the Army Francis Harvey recently committed to spending \$38.6 billion through 2013 for Army National Guard equipment.¹⁹ By identifying a specific program and providing the necessary funding to equip the Army National Guard, the active Army can begin to reverse the trend of underequipping the National Guard and robbing Peter to pay Paul to equip units deploying overseas.

To accomplish this goal, Congress should:

- **Fully fund** programs to reconstitute and modernize the National Guard;
- **Require** the Department of the Army to establish a system-of-systems modernization program, a Future Security System (FSS) designed specifically for the Army National Guard that is

19. Michelle Tan, "Relief for U.S. National Guard? Army Promises Billions for Strained Force," *Defense News*, October 9, 2006, p. 57.

optimized for its role as an operational force for missions at home and overseas; and

- **Require** the establishment of a dedicated program executive office to oversee the FSS.

For its part, the Department of the Army should:

- **Consider** using the proven organizations, equipment, and technology available in the Stryker Brigade Combat Team as the basis for quickly and efficiently fielding the FSS;
- **Ensure** that the FSS can be integrated seamlessly into the Future Combat System, enabling the Army of the future to act as one team both at home and overseas; and
- **Coordinate** FSS requirements with the other armed forces and the Department of Homeland Security to ensure that the nation has a comprehensive and coordinated set of federal capabilities to respond to catastrophic disasters.

Conclusion

The era when America could afford to treat modernization of the Army National Guard as an afterthought is over. The Army National Guard will continue to play a pivotal role in protecting Americans at home and abroad in the decades ahead, and it will need the best equipment for the task.



Reserve Component Transformation: Opportunity for Real Change

CHRISTINE E. WORMUTH

Senior Fellow, International Security Program
Center for Strategic and International Studies

Despite a number of studies and recommendations conducted in the last several years on potential changes to the size, shape, and focus of the National Guard and federal Reserves, the Department of Defense (DoD) has generally made only gradual changes to the Reserve Component. While the transformation of the Guard and Reserves has been particularly gradual in the area of homeland defense and civil support, DoD and Congress now have the opportunity and the responsibility to make real changes that will ensure the future health of the National Guard and Reserves.

Since the September 11th attacks, the spotlight has been shining brightly on the National Guard and Reserves. In the aftermath of the attacks, the nation relied heavily on the Guard and the Reserves to help protect the homeland. National Guard troops provided airport security and critical infrastructure protection in the weeks following the attacks until they could be replaced with civilian security. The Air National Guard flew extensive combat air patrols in the months following September 11th and has continued to play a key role in the air sovereignty mission for the past five years.

The DoD has also mobilized Reserve Component units extensively to serve in overseas operations as part of the war against Islamic extremism. Reserve units were quickly mobilized and deployed to Afghanistan in

the fall of 2001, and since 2003 nearly every combat brigade of the National Guard has been deployed as well.¹

Since the beginning of combat operations in Iraq, thousands of soldiers from the Army and Marine Corps Reserves have also deployed. Currently, Navy and Air Force Reserve personnel are performing what many call “boots-on-the-ground” missions to relieve some of the pressure on Army and Marine soldiers that make up the bulk of troops in Iraq and Afghanistan. In October 2006 the U.S. Marine Corps announced that it was planning to deploy certain reserve combat battalions for a second tour in Iraq to enable DoD to maintain sufficient numbers of troops in the Middle East.

Reserve Component forces also play a critical role at home in the United States. In September 2005, the National Guard sent 50,000 soldiers to the Gulf Coast to assist in the response to Hurricane Katrina. Although federal Reserve forces could not be mobilized involuntarily by law at the time of Hurricane Katrina, many reserve soldiers volunteered to help with response and recovery operations in Mississippi, Louisiana and Alabama.

The prominent role of the National Guard and federal reserves both at home and overseas during the last several years has generated a great deal of media attention. The broader defense community also has focused more closely on Reserve Component issues, recognizing that Guard and Reserve forces have become an important part of the military’s operational force. As part of this enhanced focus on the Reserve Component, the Center for Strategic and International Studies (CSIS) released a comprehensive study analyzing how the National Guard and Reserves can best be organized, trained, equipped and employed in the future.² Congress also has called for more attention on Guard and Reserve issues. The FY05 National Defense Authorization Act

-
1. David M. Walker, “RESERVE FORCES Army National Guard’s Role, Organization, and Equipment Need to be Reexamined,” testimony before the Committee on Government Reform, the U.S. House of Representatives, at www.gao.gov/new.items/d06170t.pdf, p. 1 (November 19, 2006).
 2. Christine E. Wormuth, *The Future of the National Guard and Reserves: The Beyond Goldwater-Nichols Phase III Report*, July 2006, pp. 136-145, at www.csis.org/media/csis/pubs/bgn_ph3_report.pdf.

chartered an independent Commission on the National Guard and Reserves (CNGR) that presented recommendations on recent legislation relating to the Reserve Component to Congress in March 2007 and is expected to release a final report in July 2008.

Making real changes to the Reserve Component requires not only serious study to generate thoughtful recommendations about how to best reshape the Guard and Reserves, but also the political will to implement good ideas. The potential for real change may be greater in the next few years than it has been for some time. While Robert Gates will likely spend most of his time focused on the situation in Iraq, as the new Secretary of Defense he may also bring a new perspective to the challenges facing the nation's ground forces, both active and reserve. The 2006 election returned control of both houses of Congress to the Democratic Party, which may also create new opportunities to examine important issues relating to the health of the Guard and Reserves. Finally, the presidential election in 2008 will bring a new occupant to the White House, and regardless of which party wins the presidency, a new President may have new ideas about how to use the Reserve Component.

Fix the Army First

While the National Guard and Reserves could play an even greater role in homeland defense and consequence management, before the Reserve Component can do more in those areas, fundamental changes must be made to ensure the overall health of Reserve Component forces. In particular, the Army—both active and reserve—is overstretched and must be fixed, or the health of the all-volunteer force could be at risk.

It is clear that even if the United States begins to reduce its military footprint in Iraq in the next few years, the demand for military forces in the future will remain relatively high. The demands of ongoing operations coupled with the need to respond to unforeseen events—such as a potential coup in Pakistan or aggression on the Korean peninsula—means there will be a continuing need to ensure sufficient numbers of combat-ready troops are available at all times. The Army today is too small to be able to do all that it is asked to do as part of the nation's national security strategy. Recent reports that the Pentagon is

preparing to change the mobilization policy for National Guard and Reserve units in order to increase access to these soldiers is further confirmation that the Army cannot sustain its current pace at its current size. Remobilizing Reserve Component forces would not be a small shift in policy. Under existing policy, Guard and reserve soldiers can be involuntarily mobilized for no more than 24 cumulative months. In essence this means that most mobilized Guard and Reserve troops serve one time overseas in places like Iraq or Afghanistan. If the Pentagon revisits this deployment policy, Guard and Reserve troops could be mobilized involuntarily more than once per partial mobilization order, as long as each specific deployment is less than 24 months at a time. While this re-mobilization would be permissible under law, it would represent a dramatic change in practice from how the Pentagon has historically mobilized members of the Reserve Component, which has been one involuntary deployment per Presidential Executive Order. If the active Army were sufficiently sized for its mission, the Pentagon would not be forced to contemplate mobilization policies that clearly go beyond what can reasonably be expected of volunteer, citizen-soldiers who have full-time lives as civilians. This proposed policy change could have significant negative consequences for recruitment and retention during a time in which it is already challenging to sustain Reserve Component end-strength.

Current troop rotation cycles are a further indication of the strain on the Total Army. A sustainable active Army spends two years at home for every one away so that its soldiers can rest, train and get ready for future deployments. Similarly, the Defense Department has determined that Guard and Reserve forces need to spend four to five years at home for every one year deployed. Currently, most active-duty Army soldiers are spending only about one year at home before going back overseas, and Guard and Reserve troops are spending only three years at home in between deployments. The Army cannot maintain this operational pace and expect to recruit and retain the high quality troops on which the all-volunteer force depends. If the Army is going to meet its goal of keeping active soldiers home for two years between deployments and Reserve Component soldiers home for four to five years between deployments, the Defense Department needs to expand the active Army by about an additional four to five combat brigades

and associated support forces. This relatively modest expansion would ease the strain on the current force and allow the Army to maintain an adequate balance between the amount of time soldiers spend at home and overseas.

Not only is the current Total Army too small for its mission, it also is facing very significant equipment shortfalls. This problem is particularly acute for the Army Guard and Reserves as they transition from being a strategic reserve to part of the operational force that is employed on a regular basis. Battle damaged and worn-out equipment from extensive use, coupled with the legacy of equipping National Guard and Reserve units as a strategic reserve rather than part of the operational force, have left the Guard and Reserves ill-equipped for current and future missions. In October 2005, the Government Accountability Office reported that Army National Guard units left behind more than 64,000 individual pieces of equipment, worth \$1.4 billion, in the Iraq theater in order to ensure incoming units from the United States would have sufficient equipment when they arrived in theater.³ Army Reserve units also have left behind and transferred large numbers of equipment in order to equip deploying units adequately for their missions overseas. While understanding the need to have adequately equipped troops overseas, governors and legislators have expressed considerable concern about whether National Guard units returning home from operations in Iraq have sufficient equipment left to respond to domestic emergencies as a result of the leave-behind policy. If the United States plans to continue using the National Guard and Reserves as part of the operational force, the Pentagon needs to develop a new equipment strategy to ensure the Reserve Component can execute this role effectively.

Equipping the Reserve Component to serve as part of the operation force will not come cheaply. In its study on the future of the National Guard and Reserves, the CSIS report recommended that DoD spend at least an additional \$13 billion over the next five years, on top of the \$21 billion already included in the current five-year budget, to

3. David M. Walker, "Government Accountability Office, Reserve Forces: Army National Guard's Role, Organization, and Equipment Need to Be Reexamined," testimony before the U.S. House of Representatives Committee on Government Reform, October 20, 2005.

adequately equip the Army National Guard and Army Reserve.⁴ Although its shortfalls are not as dramatic as those the Army faces, the Marine Corps Reserve also needs substantial funding to reset equipment in need of repair and replacement. Without this additional funding, Reserve Component ground forces will be unable to function as part of the operational force over time.

The Reserve Component in Homeland Defense and Civil Support

When it comes to homeland defense and civil support, the National Guard and Reserves are a tremendous resource. The National Guard of the several States, as the state militia envisioned in the Constitution, exist in all 54 states and territories and work routinely with members of local communities. National Guard soldiers are a part of their local population, they have extensive experience working with municipal authorities, and they have considerable flexibility in terms of the missions they can conduct if they are employed in state active duty or Title 32 status. Reserve soldiers are also forward deployed throughout the country, and Congress recently gave the President broader authority to mobilize these soldiers involuntarily in the event of a catastrophe. With this new authority, it will be easier for DoD to leverage the capabilities resident in the federal Reserves that could make a real difference in managing the consequences of a natural or man-made disaster.

Not only do the National Guard and Reserves offer substantial operational capabilities relevant to homeland defense and civil support missions, they also have the potential to form part of a more regional approach to homeland security. In recent years there has been a growing realization that more needs to be done at the regional level to properly prepare for future disasters. Recently, the government has taken steps toward strengthening the regionalization of homeland security policy, particularly in the White House Katrina after-action report, which called for greater regional cooperation, exercising, and training. The FY07 Homeland Security Appropriations Act also contained a provision

4. Wormuth, "The Future of the National Guard and Reserves..." p. 10.

aimed at strengthening regional structures inside the Department of Homeland Security (DHS).⁵

Establish Regional Civil Support Forces

The National Guard in particular offers a substantial capability that if used to maximum effect could both improve the nation's ability to respond rapidly and effectively to major catastrophes and build a more regional approach to homeland defense and civil support. Although in recent years the National Guard has taken a number of steps to focus more intensely on these mission areas, more can and should be done to ensure the nation is truly prepared to address the domestic security challenges it faces in the post-September 11 environment.

To ensure that governors have the resources they need to respond effectively to major catastrophes, the National Guard could be organized to form the backbone of Civil Support Forces (CSF) in each of the ten Federal Emergency Management Agency (FEMA) regions. These CSFs would be drawn from existing National Guard units and would have two primary functions. Each CSF would serve as a coordinator and facilitator for developing regional response plans for catastrophes. The regional CSFs also would serve as one of the initial military responders in the wake of a disaster or attack. They would have the ability to deploy rapidly in order to bridge the gap between when the local first responders arrive on scene and the arrival of federal assets more than 72 hours later.

A major focus of the CSF would be helping to facilitate better working relationships between the wide range of stakeholders in each FEMA region, including state and local governments; Northern Command (NORTHCOM) and Army North (ARNORTH); DHS/FEMA offices; Coast Guard elements in the region; and even key players in non-governmental organizations (NGOs) and the private sector who might play a part in a regional response. All of these organizations have important roles in responding to a terrorist attack or disaster. The best disaster response would be one in which all the organizations

5. The White House, "The Federal Response to Hurricane Katrina: Lessons Learned," (Washington, DC: February 2006), p.124, at www.whitehouse.gov/reports/katrina-lessons-learned/ (November 19, 2006).

work together, using their different areas of expertise to provide the most effective response, but all too often today the representatives of these diverse organizations are meeting each other for the first time in the middle of the crisis. The headquarters element of the CSF could play a major role in establishing working relationships among these stakeholders on a steady-state basis so that if and when a disaster occurs, key players already know how they will interact during a response.

Establishing CSFs in the National Guard would not require building new force structure. The DoD and National Guard could build on the new state Joint Force Headquarters (JFHQ), selecting one state in each region to serve as the CSF headquarters and designating it as a focal point for civil support planning, exercising, and training. That JFHQ-state would then work with other states in the region to identify the response capabilities needed for that particular region and determine which National Guard unit elements from each state could be drawn on virtually to serve as the CSF for the region.

Each CSF would be primarily comprised of combat support and combat service support units (e.g. security, engineer, transportation, CBRNE and medical assets) consistent with the capabilities that are most likely to be needed to respond to a disaster. The National Guard, under the leadership of Lieutenant General Steven Blum, has already established ten Chemical, Biological, Radiological, Nuclear, or High Yield Explosive Enhanced Response Force Packages (CERFP) that bring together these types of forces for use in consequence management. The CSF proposed in the CSIS report would be comprised of very similar types of forces, but unlike the CERFPs, they would be drawn from units throughout an entire region vice a single state, and they would be fenced from overseas deployment so that state governors would be guaranteed a ready and equipped response capability 365 days a year.

Using the National Guard more intensively for civil support is frequently presented as an either-or option: the Guard can be deployed overseas for warfighting or it can be used at home to respond to disasters. In fact, the DoD's new rotational model for the Army presents an opportunity to better use the National Guard for civil support without jeopardizing the critical role it now plays as part of the operational force. The Army Force Generation (ARFORGEN) model envisions deploying Guard

units overseas once every six years. When not deployed overseas, Guard units will spend five years gradually ramping up their training and exercising to prepare for the next deployment. During the early years of the rotational cycle, Guard units will be largely focused on individual training and will not yet be engaged in the higher end field exercises that are necessary to be fully combat ready to go overseas. Guard units in the third year of the ARFORGEN cycle will have sufficient equipment and personnel to function effectively as CSFs but would still be early enough in the cycle so that service as part of a CSF would not significantly disrupt preparation for more intense overseas missions. Fencing certain support units (both personnel and equipment) in the National Guard from overseas deployment during the third year of the ARFORGEN cycle to serve as regional CSFs would give the nation a dedicated and capable response capacity without undermining the ability of the National Guard to serve as part of the operational force.

Units serving as part of the regional CSFs during any given year would focus their annual training exercises on civil support missions, build relationships with the full range of other organizations that would be part of a regional response operation, and be on alert to respond to an actual disaster for the year in which they are “in the box” as part of the CSF. Units making up the CSF would report to their respective governors on a steady-state basis, but could be chopped to the command of the headquarters state adjutant general through Emergency Management Assistance Compacts (EMACs) for annual exercises.

Command and control arrangements for the CSFs reflect the inherent flexibility the National Guard offers in the area of homeland defense and civil support. In the event of an actual catastrophe, governors throughout the region could decide whether they would be willing to release control of component units to the governor of the state most in need of aid. Troops released to the command of another state governor could serve in either state active duty or Title 32 status. If the circumstances of an attack resulted in a presidential decision to federally mobilize Guard troops, the CSF would fall under the command of NORTHCOM and the Secretary of Defense. To ensure that CSFs are able to function effectively under the full range of command and

control scenarios, CSFs would conduct two exercises each year; one in which the CSF reports to a state governor, the other in which they report to NORTHCOM.

In order for the CSFs to respond rapidly to a disaster and bridge the gap between local first responders and the arrival of federal response assets, the CSFs would need reliable access to prompt airlift. The CSIS study on the National Guard and Reserves recommended that the Air Force recognize the requirement for civil support-related airlift and put air crews and planes on soft alert to ensure that CSFs could be deployed quickly and efficiently.⁶ One way to do this would be to associate the ten FEMA regions with the ten different Air Expeditionary Forces (AEFs). This would allow the alert requirement to be rotated, so that at any given time, active, Guard and Reserve airlift assets from only two AEFs would be on alert. Although this would constitute a new requirement for the Air Force, and is one that the Air Force to date has argued is not necessary, if the nation is truly facing a real threat to the homeland, the time has come to develop a consequence management capability that is reliable and can actually respond fast enough to make a real difference.

Regional CSFs would focus National Guard units more intensely on homeland missions, and provide a set of dedicated, trained and practiced response forces to assist in managing the consequences of a major catastrophe. These forces would advance regional planning efforts and build working relationships among states and a wide range of federal agencies. By drawing on units in the third year of the ARFORGEN cycle to man the CSFs, DoD could provide a more robust civil support capability than it currently offers without undermining the important role the National Guard plays in overseas missions.

The Guard Role at NORTHCOM and the National Guard Bureau

There are several important areas where transformation is needed to strengthen the homeland defense and security capabilities of the Reserve Component. Although NORTHCOM is working hard to

6. Wormuth, "The Future of the National Guard and Reserves..." p. 98.

build bridges to the states, relations between the command and state governors continue to be strained. Given that the Guard is likely to play a major role in any response to a catastrophic event, it makes sense to appoint a National Guard general officer as the Deputy Commander of NORTHCOM, at least for immediate future. Placing a National Guard general officer in the actual chain of command would demonstrate NORTHCOM's recognition of the Guard's key role in homeland security, would help to build bridges to the states, and would bring the upper echelons of NORTHCOM an accurate understanding of the Guard's strengths and limitations. If NORTHCOM and the Guard are to work effectively with one another, they must understand each other's capabilities.

The Chief of the National Guard Bureau (NGB) and the Bureau itself also need a greater voice in homeland defense and civil support issues. In the specific area of the role of the National Guard in homeland defense and civil support, the Chief of the NGB should be empowered to directly advise the Secretary of Defense. When the National Guard is called to serve in state active duty status or under Title 32 for domestic missions, it is fulfilling its role as the nation's militia rather than serving as part of the federal Army and Air Force. For such missions, it is wholly appropriate for the Chief of the NGB to advise the Secretary of Defense directly, just as the Army Chief of Staff and Secretary of the Army would advise the Secretary on matters concerning the Army, for example. Any revision of Title 10 would need to be crafted carefully to make clear the roles and responsibilities of the Chief of the NGB in this area relative to the roles and responsibilities of the Assistant Secretary of Defense for Homeland Defense. Unlike the Assistant Secretary of Defense for Homeland Defense, the Chief of the NGB would not have the responsibility to represent the DoD as a whole on homeland matters, including military assistance to civil authorities. Representing the Department on homeland defense and civil support matters to the Executive Office of the President, DHS and other federal departments and agencies, as well as State and local authorities should continue to be the role of the Assistant Secretary of Defense for Homeland Defense. The Chief of the NGB would have a more limited role focused on advising the Secretary of Defense on how the National Guard can contribute to homeland defense and civil support,

and would execute this role in close coordination with the Assistant Secretary of Defense for Homeland Defense.

Similarly, Congress should consider revising the statute outlining the functions of the NGB so that the Bureau could play a more direct role in advising the Combatant Commands and working with the Office of the Secretary of Defense (OSD) to develop plans, policies, and programs with respect to the Guard's role in civil support missions. While the Army and Air Force should remain responsible for developing doctrine and training requirements for its personnel, if the NGB's charter were revised to include this new function, the NGB would be able to advise the Army and Air Force on development of doctrine and training requirements for National Guard forces participating in defense support to civilian authorities operations. As part of this new responsibility, the NGB would be the primary adviser to OSD and the combatant commands for developing joint requirements for civil support missions that would draw on Guard forces and for advising OSD and the combatant commanders as they translate those requirements and the associated military capabilities resident in the National Guard into operational plans for these missions.

Finally, while the Guard gets most of the attention when it comes to responding in a crisis, there are many capabilities in the federal Reserves that also could be put to good use in consequence management. Particularly now that members of the Reserves can be involuntarily mobilized by the President during a catastrophic disaster, NORTHCOM and the Reserve commands should work with Joint Forces Command to ensure that NORTHCOM has real visibility into the kinds of Reserve Component capabilities that are available in the homeland and where these assets are at any given time. Such visibility would make it easier for NORTHCOM to plan for civil support missions using the full range of active and reserve capabilities.

Conclusion

The U.S. Reserve Component has numerous capabilities that will be needed to respond effectively to future catastrophes, whether a natural disaster or a terrorist attack. While Guard and Reserve forces have already played key roles in responding to disasters such as Hurricane

Katrina, they are not being used to their maximum potential. If organized more systematically to focus on homeland defense and civil support missions, National Guard troops in particular could be part of a major step forward in improving the nation's emergency preparedness.

The Hart-Rudman Commission argued years ago that civil support should be a primary mission of the National Guard. Although their recommendations in this area were not embraced by the DoD, they were right then and they are right today. Organizing National Guard elements into virtual, regional Civil Support Forces during the third year of the Army's new rotational cycle and focusing those forces on planning, exercising and training at the regional level can be done without jeopardizing the critical role of the National Guard as part of the operational military used overseas. Such forces would provide governors with a rapidly deployable, trained and guaranteed disaster response capability—something the nation does not have today.

No matter how the nation, the governors and the DoD ultimately choose to organize the National Guard and Reserves for homeland defense and civil support missions, the Reserve Component must be given the funding and equipment it needs to execute its full range of responsibilities. In order to perform missions at home and abroad effectively in the future, the Reserve Component will need the funding required to serve as part of the operational force and DoD will need to take steps to mobilize Guard and Reserve forces in a manner that is consistent with their new role and the constraints they face as citizen-soldiers.



Transformation of the Reserve Component

PETER VERGA

Principal Deputy Assistant Secretary of Defense (Homeland Defense),
United States Department of Defense

The “Transformation of the Reserve Component,” the title of our panel, is interesting but should not necessarily be examined in a vacuum, as the transformation of the reserve component cannot be generally separated from the transformation of the Department of Defense (DoD).

When President Bush was first elected, he articulated his goal for DoD transformation. Since that time, efforts have continued to reach that goal, even in the midst of on-going combat operations in Afghanistan and Iraq. Some have questioned whether these efforts—transformation and combat operations—should be conducted simultaneously, but I would argue that it is the only approach we can take in today’s world.

I have heard Ms. Mackenzie Eaglen, a Senior Policy National Security Analyst at the Heritage Foundation, suggest the Army National Guard employ a Stryker Brigade Combat Team in their efforts to reorganize, modernize and equip in lieu of heavy brigades or heavy battalions. Those of us who currently serve or who have served in the Army know that the size and shape of the forces used in combat operations, war, are made up of the forces you currently have. Although Secretary of Defense Donald Rumsfeld was criticized when he stated, “you go to war with the army you have, not the army you want,” he was speaking the truth. In hindsight, it’s easy to say ‘shoulda, coulda, woulda,’ in how we approached, conducted and continue to conduct our operations abroad, but we are where we are. Being from the ‘we are where we are’ school of management, I believe we cannot go back, but must instead move on from where we are now.

The DoD has adopted and now lives by the “total force concept,” which means having the right forces for the right capabilities for the right operations at any given time. What many may not understand is that the National Guard and the Reserve Components which include the Army and the Air Force National Guard, as well as the Service Title 10 Reserve Components are, in fact, fully integrated into that total force concept. Therefore, the Reserve Component is part of those right forces and are employed for their right capabilities to be used for the right operations at any given time.

The National Guard bore a significant burden of the early deployments into Afghanistan and to Iraq. This was done on purpose, as at that time we went with the ready forces we had to deploy—and the National Guard forces were ready. Since that time, while continuing to be integrally involved, they been scaled back considerably in terms of the numbers and percentages of the deployed forces. But that is not to say that, at some point in the future, the National Guard might again be deployed as a considerable percent of the forces deployed in Iraq and Afghanistan.

During the same time frame of involvement in Afghanistan and Iraq, we were also responding to the 9/11 attacks on the United States and concentrating on the development of Homeland Defense and Homeland Security operations inside the United States. Some question the difference between these two concepts: Homeland Security and Homeland Defense, so I will try to explain, rather than simply define the two and I’ll do so in terms of how I explained it to the 9/11 Commission.

One of the commissioners asked me to explain, in plain english, the difference. Here is how I attempted to explain using the attacks of 9/11 but within the current organization of our government: Preventing somebody, one of the hijackers, from getting into the country, preventing them from overstaying their visa, preventing them from getting through the airport security, preventing them from getting through the cockpit door and preventing them from hijacking the aircraft in order to take it over—these functions handled principally by the Department of Homeland Security (DHS). They constitute

“homeland security,” principally and functionally law enforcement functions.

“Homeland Defense,” on the other hand, is the military defense of the United States against external threats and aggression, such as guided missiles which have been captured by some hijackers who turn commercial aircraft into guided weapons aimed at the people of the United States. This is the mission of the DoD—to defend against these type threats. Performing this function is also a test of means, i.e. who has the means to perform the function. Homeland Defense is a mission of the DoD because we’re the only department with the training, personnel and equipment to deal such threats or situations. Now, there is a sort of sliding scale where there are air marshals onboard aircraft who might be able to retake control and capture the hijackers, but ultimately, if military force is required to defend the United States, it falls under the purview of Homeland Defense, and that resides within the DoD.

The United States Northern Command (USNORTHCOM) was established for the purpose of commanding the active duty military forces should they be employed inside the territorial limits of the United States or inside the rest of their area of operations. USNORTHCOM must plan for scenarios, identify gaps in our ability to defend the nation, and close those gaps. I believe in this planning, USNORTHCOM, or more specifically our government, should have 50% of our total force available at any time.

We also developed a Strategy for Homeland Defense and Civil Support. We recognized that part of Homeland Defense is the required support to civil authorities—the traditional role of the United States military in domestic affairs. Within that support, we have a focused reliance on the Reserve Component, in particular the National Guard, because the National Guard is comprised of the forces that, on a day to day basis, are deployed by and in the United States.

The Guard will tell you that they are in every town and every city—and I believe this is a fair statement. My in-laws reside in the small town of Chester, Vermont; a town with a population of 300. There is an

Air National Guard armory right there in Chester, Vermont. So yes, I believe they may be everywhere.

Over the years, the Guard has served well the interests of the United States and the interests of the American people. Governor James Gilmore and I are in virulent agreement as to the role of the National Guard and the role of the military domestically. We recognize that the founding fathers purposely set the system up so that domestic law and order, domestic security, and the security of the civilian population inside the United States are vested in the hands of civilian authorities. To do that, we rely on civilian law enforcement agencies and also the National Guard. Traditionally, the National Guard is the militia of each of the states or territories called into service by their governor if needed, by the President for deployment within the United States under certain circumstances, and called into service as part of the strategic reserve in the armed forces deployed overseas. The decision to call up or use the National Guard is not done lightly, nor without due consideration—the governors and the President will weigh various options and paths before determining the need for the Guard.

I'm a veteran of the Vietnam War. Those of you who remember that time know that our government made a conscious decision at the end of the Vietnam War to move certain military capacities and capabilities into the Reserve Component. This was a conscious decision to help ensure that the United States should not engage in future wars unless it was prepared to use all its national resources, including the reserves. So we purposefully moved the Army Reserve, Air Force Reserve, all the Reserve Components, and certain capabilities needed to go to war into the National Guard. In retrospect, was this the right way to do it? I don't know, but it's something that will be considered as we continue to transform the DoD, including the Reserve Component.

As previously stated, there is now a Strategy for Homeland Defense and Civil Support. One of the components or tenets of this strategy is our three concept-approach of: Lead, Support and Enable. The DoD and the federal and active military forces will always take the 'lead' in the military defense of the United States. One notable exception is how we depend on the Reserve Component, particularly the Air National Guard, to fulfill the air defense mission of the United States.

Since 9/11, 90-some percent of the air defense, about 32,000 sorties, have been flown by the Air National Guard. That's in addition to the deployment of Air National Guard forces overseas into Iraq and Afghanistan. Much of our air power is, in fact, in the Reserve and the National Guard.

The other part of that strategic construct is to 'support.' We recognize that the DoD can be called upon and will be called upon, under certain circumstances, to provide support to civilian authorities particularly during times often described as, 'when civilian capability is overwhelmed,' or 'when it is exhausted,' or 'when it is expended.' Whatever term is used, the active duty military forces will be available to be called upon when and if civilian authorities deem it necessary. Those civilian authorities are principally the state governors of the United States, as their sovereign authority rests under our constitutional framework. It is also worth noting, our military personnel, including all those within the reserve component, swear their oaths to the Constitution of the United States—not to any individual person or governing body. So there's never a question as to why we're doing something or how we're doing it.

The last part of our strategy is what we call 'enable.' Through this concept, DoD tried to enable our partners, both our overseas partners and domestic partners to be prepared to prevent, respond to, mitigate and recover from emergency situations. Their abilities to do what needs to be done impacts how and when the DoD is called upon; and to be candid, we in the DoD prefer not to be called upon, especially when we might otherwise be engaged. In other words, we want our partners to be able to do what needs to be done. And we have many specific programs designed for that.

Governor Gilmore and I agree on the necessity of building up the capabilities of state and local first responders. Just as all politics are local, all emergencies and all domestic activities are really local, as they are the first people on the line. Governor Gilmore has also discussed the idea of specialized military units deployed to support civilian authorities, in particular when responding to incidents involving Weapons of Mass Destruction (WMD). Congress, in its wisdom, has directed the DoD to provide 55 WMD Civil Support Teams around

the country—one for each state and territory and two for California. While these are small units of the National Guard, they are active-duty, full-time and paid for by the federal government. They can assist state and local governments in assessing the consequences of a WMD attack. If you have to go up a tier on those emergency responses, in particular with WMD, you get into Joint Task Force Civil Support with a component command in USNORTHCOM. Together, these form a ‘tiered-response’ to include federal, state and local authorities.

The main message that I would give is that reserve components are going to be transformed just as the active components will be transformed. People tend to concentrate on an organization, equipment and ‘things.’ In reality transformation is about thinking how we do business, how we do planning, how we respond and then about making sure that we respond with no more force than is ever necessary for the circumstance.

Chapter Four



Finding the Enemy Within



Finding the Enemy Within: Towards a Framework for Domestic Intelligence

DAVID HEYMAN

Director, Homeland Security Program
Center for Strategic and International Studies

Military Expands Intelligence Role in US¹

Pentagon, CIA Get Financial Data²

Bush Warned About Mail-Opening Authority³

FBI Finds It Frequently Overstepped in Collecting Data⁴

These headlines are some of a steady stream of stories cropping up about government collection of information on Americans in the fight against terrorism. In each case, the story sparks controversy and the Administration defends the actions as legal, necessary, and not unduly intrusive. But these assurances do not relieve public unease about a growing domestic role for national security agencies that traditionally have focused their attentions outward.

Of all the issues that we have wrestled with since 9/11, perhaps none has received more consideration or attention in discussions on homeland security than the acknowledged shortcomings of intelligence—in collection, analysis, and sharing—prior to the September 2001 attacks. In the United States, intelligence collection is split between agencies that look outside of our borders (e.g., the military, the Central Intelligence Agency [CIA]) and those that look inward (the Federal Bureau of Investigation [FBI]). And while there has been significant attention paid to the reorganization, revitalization and resourcing of

1. *The New York Times*, Sunday, January 14, 2007, Eric Lichtblau and Mark Mazzetti, p. A1.
2. *The New York Times*, Sunday, January 14, 2007, Eric Lichtblau and Mark Mazzetti, p. A17.
3. *The Washington Post*, Friday, January 5, 2007, Dan Eggen, p. A3.
4. *The Washington Post*, Thursday, June 14, 2007, John Solomon, p. A1.

our foreign intelligence services, far less attention has been paid to the domestic side of the equation.

There is, however, a clear new need and many new activities emerging to bolster intelligence capabilities to support post-9/11 homeland security/defense missions. And yet the increase in domestic intelligence (DI)⁵ collection has moved forward with little public discussion, no apparent framework, and little oversight. This raises the prospect of an emerging domestic intelligence ‘system’ where all the pieces don’t fit together, pieces are missing or redundant, and there is no framework for protecting individual liberties. To address DI responsibly requires answering fundamental questions about what agencies should be responsible for collecting intelligence within the United States; what types of domestic information the government should collect, and how it should be used; and how the government needs to coordinate and oversee the process to assure effectiveness and protection of civil liberties.

The Need for Domestic Intelligence

Increased focus on DI is a necessary response to the threat posed by international terrorism. Terrorists live, work, plan, and act all over the world, including within our borders. They move and communicate with relative ease between foreign capitals and U.S. cities. The 9/11 attacks represent a failure of intelligence agencies—foreign and domestic—to communicate and coordinate as the planners and perpetrators lived within and traveled in and out of the United States for months prior to the attack, with little notice.

Despite our success in Afghanistan, eliminating a regime that had provided safe haven for terrorists to train and launch operations to attack us, terrorism has neither been quelled nor conquered. To the contrary, terrorist recruitment and terrorist attacks continue to expand. Homegrown terrorism is on the rise in Europe, Australia, and North America, and the spread of radical Islamist ideology has

5. The term “domestic intelligence” used in this article is shorthand for intelligence – relating to threats of grievous harm to U.S. national security, including from foreign powers, persons, or from international or ‘home grown’ terrorism – collected on individuals located within the United States.

hastened, gaining traction in fragile democratic states from Lebanon to Indonesia.

Countering threats abroad cannot substitute for strengthening protection at home. We must be able to anticipate, prepare for, and interdict attacks at home. Because the threat at home is greater now than during the Cold War, when we worried more about attacks from nation-states abroad than from non-state attackers on American soil, confronting this threat requires greater understanding of domestic information and more flexibility in sharing analysis, and the use of that information.

Emerging Elements of Domestic Intelligence

To address the much-recognized need for intelligence reform following the 9/11 attacks, the U.S. government instituted a series of some of the most sweeping reforms of the nation's intelligence apparatus since the end of World War II. Among the changes following the 2001 attacks are the creation of new organizations, new missions, and new positions. They include:

- Establishment of the Homeland Security Council (HSC) at the White House to coordinate all homeland security-related activities among executive departments (including related-intelligence); and specifically, setting-up a Homeland Security Policy Coordination Committee (HSC/PCC) for the expressed purpose of coordinating interagency policy on detection, surveillance, and intelligence.⁶
- Establishment of a new homeland defense mission for the U.S. military, a new Northern Command (USNORTHCOM) responsible for providing command and control of Department of Defense (DoD) homeland defense and civil support efforts, and a new Assistant Secretary of Defense for Homeland Defense (ASD/HLD) to provide homeland defense related guidance for USNORTHCOM.⁷ Both ASD/HLD and USNORTHCOM will

6. The White House, *Homeland Security Presidential Directive-1 (HSPD-1)*, October 29, 2001. <http://www.fas.org/irp/offdocs/nspd/hspd-1.htm>.

7. Department of Defense. *Special Briefing on the Unified Command Plan*. Washington: Wednesday, April 17, 2002. <http://www.fas.org/irp/news/2002/04/dod041702b.html>.

require intelligence to perform their duties to protect America at home.

- Formation of a new National Security Branch (NSB) at the FBI to protect the United States against weapons of mass destruction, terrorist attacks, foreign intelligence operations, and espionage.⁸
- Creation of an Undersecretary for Intelligence at DoD charged with integrating defense intelligence, surveillance, and reconnaissance capabilities to better provide warnings, actionable intelligence and counter-intelligence support necessary for national and homeland.⁹
- Establishment of a new assistant secretary for Information Assurance and Infrastructure Protection at the Department of Homeland Security (DHS) (transformed today to Assistant Secretary for Intelligence and Analysis) to identify and assess current and future threats to the homeland, map those threats against our current vulnerabilities, inform the President, issue timely warnings, and immediately take or effect appropriate preventive and protective action.¹⁰
- Induction of the U.S. Coast Guard—responsible for protecting U.S. economic and security interests in any maritime region including America’s coasts, ports, and inland waterways—into the U.S. intelligence community and establishment of the Coast Guard Intelligence Coordination Center as it’s primary interface with the collection, production, and dissemination elements of the national intelligence and law enforcement communities.¹¹
- Creation of the National Terrorist Threat Integration Center (now the National Counterterrorism Center or NCTC), an interagency

8. Federal Bureau of Investigation. *National Security Branch Overview*. ONLINE. Washington: Department of Justice, September 2006. <http://www.fbi.gov/filelink.html?file=/hq/nsb/whitepaper12-06/whitepaper.pdf>.

9. Department of Defense. *Directive Number 5143.01*, November, 2005. http://www.fas.org/irp/doddir/dod/d5143_01.pdf.

10. United States Congress. *Homeland Security Act of 2002*. <http://news.findlaw.com/hdocs/docs/terrorism/hsa2002.pdf>.

11. United States Congress. *Intelligence Authorization Act for Fiscal Year 2002*. <http://thomas.loc.gov/cgi-bin/query/D?c107:6:./temp/~c107wuVNfa>.

body intended “to provide a comprehensive, all-source-based picture of potential terrorist threats to U.S. interests.”¹²

- Consolidation of all U.S. intelligence functions and activities to be coordinated under a newly created Director for National Intelligence (DNI).¹³

The approach to initiating and implementing DI reforms, however, has been ad hoc, fragmented and has emerged without a strategic vision to follow. In October 2005, the new Office of the Director of National Intelligence (ODNI) issued its blueprint for building “an integrated intelligence capability to address threats to the homeland, consistent with U.S. laws and the protection of privacy and civil liberties.”¹⁴ Despite this effort, the document failed to develop specific roles and missions, clear rules for collection, or how information should be shared among intelligence partners and other associated homeland security stakeholders.

In a world where non-state actors can gain asymmetric advantage by operating within the gaps of a dysfunctional or inefficient bureaucracy, one of our goal’s must be to deny terrorists safe harbors in the seams of society—seams between foreign and domestic, civil and military, federal and state, public and private, and even agency to agency—but to do so while also ensuring that we uphold the pillars that are at the heart of America’s constitutional identity—federalism, liberty, and justice. This requirement raises complex legal and policy issues because by its nature, DI collection affects the privacy and civil liberties of U.S. citizens and residents.

Problems in the Absence of a Domestic Intelligence Framework

If there is no framework for DI, no clarity about roles and responsibilities in its collection, each agency will set out on its own to get what it needs. Such activities can have negative consequences not only for

12. United States Congress. *Intelligence Reform and Terrorism Prevention Act of 2004*. http://www.nctc.gov/docs/pl108_458.pdf.

13. Ibid.

14. Office of the Director of National Intelligence, *The National Intelligence Strategy of the United States of America: Transformation Through Integration and Innovation*, October 2005: 11. <http://www.odni.gov/publications/NISOctober2005.pdf>.

civil liberties, but also for effectiveness. On the civil liberties side, an undefined, potentially unlimited program of covert surveillance of the American public raises huge privacy concerns, both in perception and in practice. In terms of effectiveness, when collection roles overlap or are not clearly defined, there is great risk that players will trip over each other by pursuing the same leads or sources, or will miss something because they believe others will pursue it. These or other mishaps could compromise important and sensitive activities.

The world of intelligence is largely closed. As a consequence, public debate is often limited between those who are un-informed or poorly informed. Those who have the facts are constrained by secrecy requirements from discussing the details, or, in some cases, even the broad outlines of the activities. Those who 'know' can stymie public discourse with arguments that any discussion would telegraph the nature or details of government collection to our enemies. Those that 'don't know' can inspire public fear and diminish public confidence by imagining the worst.

The Bush Administration and its national security officials have generally shied away from any broad discussion of how they will address the increased need for domestic intelligence. In his confirmation hearings, the new DNI, Michael McConnell, stated that the Intelligence Community has been "trained for years to think external, foreign," but stressed that with the terrorist threat it is important to "think domestically."¹⁵ The ODNI, however, has so far been reluctant to take responsibility for setting a policy framework for collection and use of domestic intelligence. This leaves each agency to make its own judgments about what information it needs and how to get it.

When it comes to discussing this issue, outside of the government, experts have tended to focus primarily on an organizational question: should the FBI remain the country's DI agency or should we separate the intelligence and law enforcement functions and create the U.S. equivalent of MI-5, the United Kingdom's domestic intelligence service.

15. Senate Select Committee on Intelligence. *The Nomination of Mike McConnell to Be Director of National Intelligence*. Hearing. February 1, 2007. Washington: Office of the Director of National Intelligence, 2007. <http://intelligence.senate.gov/hearings.cfm?hearingId=2482>.

This is an important question, but it is not the only question, and it should not be the first. What is most important is for the government to create a consistent and clear framework for its collection and use of DI. To do that it must answer three questions:

- Who can collect domestic intelligence, and why?
- What domestic intelligence can the government collect, and how?
- How must the government coordinate and oversee the process?

Who Can Collect Domestic Intelligence and Why?

To be clear, there are three primary roles that intelligence agencies perform: they collect intelligence, carry out clandestine operations, and engage in analysis. Collection might involve clandestine electronic or physical surveillance, use of human sources (including by means of interviews or interrogations), imagery or photo-surveillance, or seizure of records or other physical materials. Operations or actions—which to date has been less common in the DI context—might include undercover operations or disruption activities.¹⁶ Analysis necessarily involves access to all these sources of information, including in some cases private information, for the purposes of providing policy advice or threat information.

The source of information—of ‘domestic intelligence’—whether related to operations or analysis, is collection. Collection and operations are the functions that involve the greatest potential intrusions on individual privacy or liberty. Many concerns of the public regarding collection stem from a fear that a government unchecked and without proper limitations of law or oversight, as has been experienced at times in America and throughout history, will lead to unconstitutional abuses of government authority. In particular, some point to the danger inherent in the government collecting vast amounts of personal data on any and all persons, and that such information would be made available to any government agency for any future use, particularly in ways that the affected individuals may have no knowledge or ability to seek redress. Unlimited collection would not only be an invasion of privacy, it would be counter to the common expectation of Americans

16. Overt actions such as screening or denial of a benefit might also be based on intelligence, although they are not typically regarded as intelligence functions.

to be free to be left alone. Even the perception of unchecked intelligence diminishes greatly the public's trust in government. Further, when the public learns through news leaks of unwarranted, potentially unlawful collection, it leaves many asking what else is going on?

In the late 1970s the Senate Committee known as the "Church Committee" uncovered government abuse in the collection and use of DI.¹⁷ One of the reforms implemented after those revelations was to limit significantly the roles of national security agencies for collecting intelligence within the United States. By Executive Order and internal regulation, the policy since that time generally gave the FBI responsibility for domestic collection—both law enforcement and intelligence. Other national security agencies were to refrain from domestic intelligence collection or operations.

Since September 11, 2001, with the recognition of a greater need for Domestic Intelligence, the policy of FBI's lead and other agencies' restraint has become less clear. As noted above, no fewer than four agencies now play some role in DI today. For reasons of efficiency and of privacy, it is vitally important to define clearly the roles and missions of the various national security agencies in the collection of DI, and take care to avoid duplication of those roles or overstepping and abuse. Having too many agencies responsible for the collection of domestic information is a recipe for harmful errors, controversy, and diminished oversight. To enhance clarity and efficiency, as a general rule, one agency (the FBI, under the existing structure) should be responsible for intelligence collection and operations within the United States. Other national security agencies should be limited to collecting intelligence

17. The Church Committee – the 1976 Senate Select Committee to Study Government Operations with Respect to Intelligence Activities, chaired by Senator Frank Church – recommended numerous reforms after uncovering serious abuses when it examined the history of domestic intelligence activities in the United States. The Church Committee found that from the late 1930's through the early 1970's, "intelligence agencies collected vast amounts of information about the intimate details of citizens' lives and about their participation in legal and peaceful activities" and used that information to abuse the privacy and liberties of U.S. citizens and residents. Select Committee to Study Governmental Operations with Respect to Intelligence Activities, United States Senate, *Intelligence Activities and the Rights of Americans* ("Church Committee Report"), bk.2 (Washington D.C.; 1976) p.7. <http://www.aarclibrary.org/publib/church/reports/contents.htm>

within the United States when it is uniquely within their mission or capability, and when they can demonstrate why the FBI cannot serve their needs. And all agencies must have clear and direct paths for information sharing.

Some considerations for developing clear agency DI roles and responsibilities include the following.

The Federal Bureau of Investigation

The FBI is the primary domestic intelligence agency responsible for collecting intelligence within the territory of the United States. Many commentators have discussed the challenges for the FBI in its intelligence role. The FBI's background as a law enforcement agency means that it has primarily emphasized reaction—capturing and prosecuting criminals after the fact—more than prevention. In cases where the FBI has, for example, infiltrated groups to prevent a crime, the focus again is on law enforcement and prosecution. A law enforcement agency is not accustomed to the jobs of providing warning, assessing vulnerabilities, or informing policy-makers. Rewards and incentives in the FBI have tended to be for law enforcement successes, and movement to an emphasis on intelligence successes has been halting. On the other hand, there are important synergies between the law enforcement and intelligence roles. The basic mechanisms of collection—surveillance, use of human sources, undercover operations, and review of records—are similar between the two disciplines, so many skills transfer from one to the other. But there are also differences, primarily that law enforcement conducts cases on activities one is generally already aware of; intelligence, by contrast, attempts to uncover things one was not aware of.

It is a monumental task to take on a new mission and change the culture of an organization. The FBI has a long way to go to build up an experienced, capable cadre of domestic intelligence officers and a functional process for collecting and sharing DI at the headquarters and field levels. Some argue that the answer is to create a separate agency to focus exclusively on domestic intelligence. The challenges of building this capacity from scratch, however, would be extraordinary, including

establishing a new agency culture and a place in the notoriously turf-conscious national security community.

Whatever the ultimate answer to this question, what is clear is that we need one agency to have primary responsibility for intelligence collection and operations within the United States. Right now, that is the FBI and it must reinvigorate its move toward becoming effective in this area. Responsibilities of other agencies should be limited to situations in which, because of a unique capability or mission, they are better suited than the FBI to engage in the collection.

The Department of Defense

The role of the DoD in DI collection has been the greatest recent source of confusion and controversy. With its new domestic military mission—the homeland defense mission of USNORTHCOM—there has been a legitimate need for intelligence to support that mission, but also real concerns that DoD is seeking a much larger role in collection of intelligence within the United States and against U.S. persons.¹⁸

In 2002, for example, Deputy Secretary of Defense Paul Wolfowitz launched the Counterintelligence Field Activity (CIFA) program. The mission of the program is:

*to develop and manage DoD Counterintelligence (CI) programs and functions that support the protection of the Department, including CI support to protect DoD personnel, resources, critical information, research and development programs, technology, critical infrastructure, economic security, and U.S. interests, against foreign influence and manipulation, as well as to detect and neutralize espionage against the Department.*¹⁹

18. US Code Title 50 § 1801 (i) states that a “United States person” means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101 (a)(20) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power. http://www.law.cornell.edu/uscode/uscode50/usc_sec_50_00001801----000-.html.

19. United States Department of Defense, Directive Number 5105.67. Department of Defense Counterintelligence Field Activity (DoD CIFA), February 19, 2002.

What is noteworthy is the extraordinary broad scope of this mission that could extend beyond bases, and military facilities and into communities. In fact, under CIFA, the DoD established TALON (Threat and Local Observation Notice), a controversial program to gather raw, non-validated information about threats to the community surrounding DoD facilities to assist in early detection of threats to prevent attacks.²⁰ TALON is similar to and grew out of a program called Eagle Eyes, an Air Force anti-terrorist community watch program that “enlists the eyes and ears of Air Force members and citizens in the war on terror.”²¹

Following a 2006 Defense Department Freedom of Information Act release to the ACLU, the ACLU discovered that the TALON database included data on peaceful, law-abiding protesters as potential threats to the U.S. military, as well as 2,821 reports containing information on U.S. persons.²² Further, the ACLU found that other government agencies had been granted authority to access and use data from TALON, leaving the possibility that even if data were deleted from one source, it might still be maintained indefinitely in files of other government agencies, thus raising serious privacy concerns.²³ The DoD recently announced its decision to end the TALON program.²⁴ In doing so, James Clapper, the new Undersecretary of Defense for Intelligence, said it is “important that the proper balance be struck between the counterintelligence mission, on one hand, and the protection of civil liberties, on the other.”

In general, the DoD’s mission and supporting policies currently do not clearly delimit its role in DI; rather, in some cases they expand

20. See also CQ Homeland, January 31, 2006.

21. See: <http://www.osi.andrews.af.mil/eagleeyes/index.asp>. The Air Force inspector general newsletter in 2003 said program informants include ‘Air Force family members, contractors, off-base merchants, community organizations and neighborhoods.’” (see, “Defense Facilities Pass Along Reports of Suspicious Activity,” Walter Pincus, December 11, 2005, Washington Post. http://www.washingtonpost.com/wp-dyn/content/article/2005/12/10/AR2005121000893.html?nav=rss_nation/nationalsecurity)

22. ACLU, *No Real Threat: The Pentagon’s Secret Database on Peaceful Protest*. January, 2007: 31.

23. *Ibid.*, 5.

24. “Pentagon to End Talon Data-Gathering Program,” Walter Pincus, April 25, 2007, Washington Post. <http://www.washingtonpost.com/wp-dyn/content/article/2007/04/24/AR2007042402540.html>

it. This is perhaps an expected consequence of promulgating a new homeland defense mission to the agency in the absence of a framework for intelligence gathering and use. The Department's current responsibility is to conduct counterintelligence activities in support of DoD components worldwide, including within the United States, and to protect the security of DoD personnel and facilities. The 2003 National Military Strategy defines the overall role of intelligence as follows:

*Intelligence systems must allow commanders to understand enemy intent, predict threat actions, and detect adversary movements, providing them the time necessary to take preventive measures. Long before conflict occurs these intelligence systems must help provide a more thorough understanding of adversaries' motivations, goals and organizations to determine effective deterrent courses of action.*²⁵

More specifically, however, intelligence required for the homeland defense mission may extend beyond military facilities and deeper into civil society:

*The Armed Forces will protect critical infrastructure that supports our ability to project military power.*²⁶

The challenge for policy-makers is to determine the lanes of responsibility and lines of permissibility: what is the appropriate domestic intelligence domain of the DoD and what are the limits of collection? The Department currently has, and should have, authority to collect information on its personnel and its facilities within the United States to support these missions, and more recently in particular, homeland defense, but that authority must be defined clearly and limited so that it does not morph into a general collection authority that duplicates or supplants that of the FBI. Even when collecting information consistent with an appropriate mission, DoD entities should coordinate closely with the FBI, leaving to the FBI the task of carrying out any civilian aspects of the collection.

25. U.S. Defense Department. *National Military Strategy*, 2004: 10.

26. Ibid.

The National Security Agency

The National Security Agency (NSA) has the authority to collect signals and communications intelligence on foreign intelligence targets. Since the Church Committee reforms and before 9/11, general NSA policy has been to refrain from intentionally collecting communications to, from, or about persons or entities within the United States.²⁷ The NSA, however, has powerful and unique collection capabilities that could be critical in fighting terrorism. There will be circumstances under which NSA capabilities should be used to intercept communications from or to someone within the United States, but extraordinary care and clarity are necessary for any such role. The NSA's capabilities have great potential for intruding on individual privacy and constitutional rights. In addition, any use of the NSA to collect DI must be coordinated with the FBI and subject to the procedures and requirements of the Foreign Intelligence Surveillance Act (FISA).

The limitations adopted in the 1970s on agencies permitted to collect DI continue to be wise and the foreign intelligence agencies should not share the mission with the FBI. However, the NSA has collection capabilities that the FBI does not have that could be critical in the fight against terrorism. Therefore, the two agencies must cooperate in their efforts.

The Central Intelligence Agency

The CIA, like the NSA, is a foreign intelligence agency that should have no general domestic mission. Unlike the NSA, the CIA does not

27. See, United States Signals Intelligence Directive (USSID) 18, Section 3, July 27, 1993. Exceptions to this policy for interceptions involving individuals located within the U.S. were made only with approval of the Foreign Intelligence Surveillance Court (FISC) and subject to FISA. The reforms of the late 1970s were, in part, a reaction to NSA activities that targeted anti-war and other political activists within the United States. Since September 11, 2001, the NSA has departed from this policy for targeting related to terrorism, at least with respect to some communications between people located within the United States and others overseas (see Hayden testimony). We discuss here only the policy issues, not the legality of this surveillance involving persons located within the United States. There are significant legal issues related to the failure to comply with FISA in conducting this domestic surveillance, which are not discussed here.

have significant unique technical capabilities that are required for DI. To have the CIA running clandestine operations or collecting human intelligence within the United States outside the legal framework governing the FBI's ability to do so, vitiates any guidance, protection, or oversight attached to such sensitive activities, besides being unnecessarily duplicative, inefficient, and dangerous both to privacy and security. The CIA does have two missions that could require it to operate domestically to a limited extent. First, like the DoD, it has missions to conduct counterintelligence activities related to the protection and security of its facilities and personnel, including within the United States.²⁸ Second, its mission to collect human intelligence overseas can have some domestic aspects, such as debriefing people returning from overseas or recruiting non-U.S. persons who are visiting the United States. As with DoD, exactly when and how these domestic responsibilities will be carried out should be spelled out clearly, and they must not be permitted to expand beyond what is necessary to carry out the specific mission.

The Department of Homeland Security

The Department of Homeland Security is the new kid on the block. On December 2003, DHS became the 15th and newest cabinet agency. According to its mission statement, a primary function of the DHS is to "identify and understand threats, assess vulnerabilities, determine potential impacts and disseminate timely information to our homeland security partners and the American public." To do this, a principle activity of the department is to "gather and fuse all terrorism related intelligence; analyze, and coordinate access to information related to potential terrorist or other threats."²⁹

With the integration of the U.S. Coast Guard's new intelligence section into the Intelligence Community, and with the establishment of the Directorate for Information Analysis and Infrastructure Protection (now, "Intelligence and Analysis"), the DHS not only has a significant resource element responsible for collection, but also a functional arm that is responsible for fusion, analysis and dissemination as well.

28. Executive Order 12333, sections 1.8 (c) and (h).

29. U.S. Department of Homeland Security, *Securing Our Homeland: U.S. Department of Homeland Security Strategic Plan*, (2004): 10-12.

What remains to be clearly defined is what intelligence DHS is expected to obtain for itself and what it should receive from others. The U.S. Coast Guard, for example, and the borders, customs, and immigration arms of the department all collect information within the U.S. that is relevant to national security.³⁰ The DHS private sector coordinating councils and newly established links to state and local government fusion centers also provide links to a wide network of key industries responsible for protecting critical infrastructure and other governments where potentially relevant threat information may be found. What is important is that collection, fusion, analysis and dissemination responsibilities be defined clearly and limited to the areas of unique DHS responsibility. For collection beyond these responsibilities, DHS should look to the FBI.

Non-Federal Partners—Local Law Enforcement and the Private Sector

One of the dramatic changes since 9/11 is the expansion of the “national security community.” The front lines of war no longer coincide with political boundaries; they are instead in the streets and buildings of our cities and states, at curbside check-ins at airports, turn-styles at stadiums, and in hospital emergency rooms. As a consequence, the battles we must fight are no longer solely the purview of airmen, soldiers, sailors and marines; they now must also be fought by epidemiologists, cryptologists, firefighters, citizens, businesses and local police. As we expand the domain of national security, we expand the domain of those who may require intelligence. Similarly, as we look to these non-traditional, non-federal national security partners for bolstering security, we need to recognize that they too can help provide information from their activities that may contribute to a better understanding of the threat.

To elaborate this concept, DHS defined in its *Intelligence Enterprise Strategic Plan*, a newly identified “homeland security intelligence community” (HSIC). According to the plan, the HSIC “includes the

30. See for example discussion on role of intelligence in achieving maximum maritime domain awareness in U.S. Coast Guard, *National Plan to Achieve Maritime Domain Awareness* and U.S. Coast Guard *Strategy for Maritime Safety, Security, and Stewardship*, January 2007, as well as in U.S. Department of Homeland Security, *National Strategy for Maritime Security*, (2005): 16.

organizations of the [homeland security] stakeholder community that have intelligence elements.” It goes on further to define the stakeholder community as “all levels of government, the Intelligence, Defense, and Law Enforcement Communities, private sector critical infrastructure operators, and those responsible for securing the borders, protecting transportation, and maritime systems, and guarding the security of the homeland.”³¹

An example of one of the more significant stakeholders and newer member of the national security community is the over 13,000 state, local, and tribal law enforcement agencies. As eyes and ears of their local communities, and so-called boots-on-the-ground, these resources represent a potentially substantial force multiplier to federal agents. Local police generally have better relationships within their communities—communities where terrorist plans are often developed. They are more likely to come in contact with those running operations. And they are more likely to assess what constitutes ‘normal’ activities or not. Two of the 9/11 terrorists, for instance, came in contact with local law enforcement. Muhammad Atta, on April 26, 2001, presented his driver’s license during a traffic stop.³² And on September 9, 2001 Ziad Jarrah received speeding ticket in Maryland while driving on I-95.³³

Similarly, terrorist encounters with the private sector could help provide clues to potential threats. Zacharias Moussaoui’s flight instructor became suspicious of him due to the fact that he was so eager to learn how to fly large planes and yet had no desire to obtain a pilots license.³⁴ More recently, a Circuit City employee reported to New Jersey authorities that two men had recently brought him a tape of themselves and eight other men firing automatic weapons while chanting “Allah Akbar” (god is great). The two men had requested that he transfer the tape from VHS to DVD format. This incident sparked a 15 month long investigation ending in the arrest on May 7, 2007, of six men who

31. See U.S. Department of Homeland Security, *DHS Intelligence Enterprise Strategic Plan*, January 2006.

32. *Final Report of the National Commission on Terrorist Attacks Upon the United States*, July 22, 2004: 231.

33. *Ibid.*, 253.

34. *Ibid.*, 247.

were plotting attacks on soldiers training at Fort Dix who were bound for Iraq.³⁵

The changes in the national security environment have increased the need to develop and share information and intelligence across all levels of government and the private sector. As a result, new partnerships between non-federal actors and the historic national security community must be and have been established. These new relationships, in turn, however, raise important questions regarding what information is needed in order for each party to perform its respective security functions, and then ultimately what information can and should be collected, by whom, and shared with whom.

What Domestic Intelligence Can the Government Collect, and How?

The Fourth Amendment of the United States Constitution protects all U.S. persons from unreasonable search and seizure by the government. When it comes to collection, particularly within the United States, ensuring requirements of security and civil liberty is a difficult balancing act, posing the legitimate need for government to seek out and interdict potential terrorist threats within the United States on the one hand, while, on the other hand, preserving the rights and protections afforded to Americans under the Fourth Amendment.

The questions for policy-makers today are, given new and emerging DI requirements, as well as new and emerging roles of government and non-governmental agencies, and a dramatically different environment where threat information may reside, then:

- What may government collect, and how?
- Is all information valid, necessary, and useful?
- Should all means of collection be available and utilized?
- How, if at all, should the government be limited in what it may or may not collect?

35. Geoff Mulvihill, "Tipster in Fort Dix Plot Comes Forward," in the *Associated Press*, May 30, 2007. <http://www.washingtonpost.com/wp-dyn/content/article/2007/05/30/AR2007053000168.html>.

To answer these questions, we need to first consider two aspects of collection: the target of collection and the source of information. The *target* of collection is the person or persons involved in a possible plot or who may know of a possible plot (e.g., a plot to commit a terrorist act or espionage). The *source* of information is where relevant information related to a possible plot resides (e.g., on a computer, on a pad of paper, in someone's mind). The *source* of information is a predicate to the *how*; it also plays an important role in shaping what the government may or may not collect.

Collection is source-specific. It can be acquired by technical means (e.g., signals intelligence or SIGINT, measurement and signatures intelligence or MASINT, and imagery intelligence or IMINT), or non-technical means (e.g., human intelligence or HUMINT, or open source intelligence or OSINT). In a world that is now dependent on information technology for communications and for operations, targets use computer networks to convey, store, or share their secrets. In other words the source of information is increasingly found electronically. That is not to say that person-to-person communications are not still relevant; they are. And direct surveillance, remote observation, and interrogation remain critical elements of collection. But, as a result of the revolution in information technology, there is now a vast store of digital information found in communications over the Internet, through wireless or satellite transmissions, and on computers or personal data assistants (PDAs).

Therefore, in addition to classic techniques of physical surveillance, use of human sources, imagery, interviews, examination of records or other physical materials, collection must also rely on electronic or digital surveillance.

The explosion in digital technology, however, poses a number of challenges. First, there is the challenge of volume. What are the limits of collection? The new challenge today is what are the limits of collection for *unknown* targets—that is how do we find the enemy within, when there is no predicate for suspicion of an individual or individuals. Most of the nineteen hijackers who attacked America on 9/11 were unknown to intelligence or law enforcement officials, and

there was little if any remarkable characteristics or information about them that stood out when they came to the United States.

In an increasingly paperless society, however, where nearly every transaction can be captured and stored digitally, individuals leave behind digital fingerprints in nearly every thing they do, every day. Consequently, when we seek to find the proverbial ‘needle in a haystack’—the enemy within—the supply of potentially useful information is almost limitless. There are perhaps as many databases today to search containing so-called ‘dots’ to connect, as there are types of services available to people—financial profiles, spending habits, phone usage, travel patterns, web-surfing interests, video surveillance files, library borrowing or book/magazine past purchases, among others. Through the use of analytic or data-mining tools³⁶ analysts can find links and patterns that may point to suspicious behavior, or even terrorist links or activities.

But too much information may be almost as bad as not enough. We don’t want to add more hay to the haystack when the needle is already too small to find. For the analyst who must discern critical information from volumes of useless or meaningless information, more data may make the task harder. Further, without clear guidance, the world of data mining can become much like a fishing expedition attempting to catch a guppy with a drift net. In the process other information, perhaps interesting but unrelated, may get caught up in the net. For example, if we are looking for terrorists or terrorist connections, other bad actors (e.g., criminals, tax cheats, or dead-beat dads) or simply embarrassing information (e.g., perversions, obsessions, or illicit affairs) may also materialize. Is that information then useable? For what purpose? Can and should individuals be prosecuted for these other offenses? What becomes of the information? Is it FOIAble (i.e. available to the public)?³⁷ Without clear rules-of-the-road, massive collection may also yield to massive invasion of privacy.

36. Data mining has been defined as “the science of extracting useful information from large data sets or databases.” *Principles of Data Mining* by David J. Hand, Heikki Mannila, and Padhraic Smyth.

37. FOIA – Freedom of Information Act. See 5 U.S.C. § 552. U.S. Government Law (2002). Department of Justice. <http://www.usdoj.gov/oip/foiastat.htm>.

One particular concern with new threats of radical Islamic terrorism is the rise of so-called “homegrown terrorism.” Homegrown terrorism refers to terrorism by individuals born, raised, or based and operating primarily in the United States. In the context of DI, this threat requires some form of collection to help security officials identify, uncover and prevent potential terrorist acts. Current (publicly accessible) limitations on DI, however, restrict government agencies from spying on U.S. citizens unless pre-approved by a Foreign Intelligence Surveillance Court,³⁸ the U.S. Attorney General, or the Director of the National Security Agency, under certain circumstances.³⁹ These restrictions must be carefully reviewed.

What is important is to approach collection of DI in a rigorous and thoughtful way. Data mining is a new and potentially useful tool that can bring non-obvious relationships to analysts’ attention that might otherwise have been overlooked. It is also a tool that may bring unrelated, irrelevant, or even false relations to light. There are clear limitations today against collecting against U.S. persons, yet also rising concerns regarding homegrown terrorism. Clear guidelines must be developed and implemented. Constitutional rights protect American citizens against illegal search and seizure or invasion of privacy. Before collection is to be undertaken, specific questions must be answered, to include:

- What is to be accomplished by collecting the information?
- What type of information should be collected?
- How much information should be collected?
- Where and how long should the information be stored?
- Who should have access to this information and for what purposes?

38. The FISA Court (FISC) is a U.S. federal court authorized under 50 U.S.C. § 1803. Established by the Foreign Intelligence Surveillance Act of 1978 (FISA), the FISC oversees requests for surveillance warrants against suspected foreign intelligence agents inside the United States by federal law enforcement agencies. http://www.law.cornell.edu/uscode/html/uscode50/usc_sec_50_00001803----000-.html.

39. See for example, National Security Agency, *United States Signals Intelligence Directive 18 (USSID 18)* “Legal Compliance and Minimization Procedures,” July 27, 1993. Section 4, “Collection”: 2-6.

- How will unexpected derogatory or potentially damaging information be handled?
- What oversight systems are in place to ensure civil liberties are properly considered and appropriately protected?

Like other types of searches in society that take place without a warrant and that are permissible by law, under some circumstances there may be times when all of these questions cannot be adequately answered, but those times should be few, rare and the exception.

How Must We Oversee the Process?

A significant issue highlighted by the recent revelation that the NSA was carrying on a program of warrantless wire-tapping of Americans is the lack of sufficient oversight over unknown or new programs. It's one thing to have new covert missions, new collection programs, and new intelligence activities to improve situational awareness for homeland security, but without proper oversight poorly designed programs may be left underperforming, agencies that overstep their bounds may go unchecked, and a skeptical public may lose confidence in their government. In each of these circumstances, it does little to improve DI or homeland security.

Oversight for DI currently exists in each of the three branches of government. At the Executive branch level, agencies have independent inspector generals with the power to review intelligence programs (among others) either in part or in whole.⁴⁰ In addition, the Justice Department, which serves as the country's law enforcement agency, may have additional oversight responsibilities in certain circumstances.⁴¹

40. Dan Eggen, "Concord Monitor," in *The Washington Post*, January 11, 2006. <http://www.concordmonitor.com/apps/pbcs.dll/article?AID=/20060111/REPOSITORY/601110368/1001/NEWS01>. And in some instances, more than one inspector general may have jurisdiction over the given issue.

41. DOJ oversight programs. See, for example, Department of Defense, *Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons*, DoD 4240.1-R, December 1982. See also, Department of Justice, *Attorney General Guidelines on General Crimes, Racketeering, and Terrorism ("Guidelines")*, May 30, 2002.

The Executive branch has statutory obligations to ensure that Congressional Intelligence Committees are kept “fully and currently informed” on intelligence activities.⁴² These obligations extend to the newly created Director of National Intelligence and intelligence agency heads. It requires them to furnish material concerning any and all intelligence activities in a timely manner. The judiciary branch, too, has an oversight function. A court may strike down unconstitutional statutes or improper actions by the Executive branch.

Both the Judiciary and Legislative branches are limited in their oversight by what the Executive branch reveals to them. On certain sensitive matters, where the Executive branch has chosen to limit congressional notification to the so-called Gang of Eight⁴³ (such as the NSA wire-tapping controversy), members of Congress are only made aware of these activities if the Executive branch chooses to inform them, and even then, members generally are not permitted to consult with their staff or any other members, or anyone for that matter, leaving them at some disadvantage in terms of their normal course of review and oversight. Similarly, the Judiciary branch can only adjudicate matters that have been brought to its attention by the Executive branch, if the information is not publicly available elsewhere.

With new DI roles and emerging missions, congressional oversight must be re-examined, particularly for ensuring that government activities that did not previously exist, nor were envisioned under current authorities or previous jurisdictions, are afforded adequate guidance and outside evaluation. Specifically, three over-arching questions must be addressed:

1. Who is responsible for developing the overall DI framework?

Domestic intelligence collection must begin with a domestic

42. See National Security Act of 1947, Secs. 501-503 [50 U.S.C. 413 - 413(b)]. For further discussion on the statutory obligations of the Executive Branch on intelligence matters, see also: Alfred Cumming, Congressional Research Service, *Statutory Procedures Under Which Congress Is To Be Informed of U.S. Intelligence Activities, Including Covert Actions*, January 18, 2006.

43. The “Gang of Eight” is understood to include the Speaker of the House, the Minority Leader of the House, the Majority and the Minority Leaders of the Senate, and the Chairs and Vice Chairs of the intelligence oversight committees of both houses.

intelligence framework. Should this be developed by Congress? By the White House? By the DNI? Or DHS? All of these parties must be at the table. What is the overall architecture for developing a DI capability that utilizes all elements of information collection and analysis? On the supply of intelligence, who are the key actors? What are their roles? What information/intelligence could each actor supply regarding threat and vulnerability assessments? Are there duplications of effort? Are there existing shortcomings in the overall U.S. effort? Are efforts currently being undertaken by one actor that could be, should be or may be better undertaken by another actor? Similar questions should be asked on the demand side: Who are the primary recipients of intelligence products? What information/intelligence do stakeholders require to perform their security functions? Are there gaps between stakeholder demands and intelligence supply?

2. How does the DI ‘system’ run? Who can task collection requirements? How are multiple streams of information and intelligence to be fused and integrated? Who is responsible for analysis? Given the increased need to “connect dots”, how is information shared from one entity to another? Are there clear policies for how intelligence/information can be used? How long can agencies retain information?

3. What oversight is in place to maximize performance while also minimizing abuse, misuse, and mistrust? Looking across each branch of government, what checks are in place for preventing abuse and ensuring redress for oversteps and/or errors? Are existing authorities sufficient?

Conclusion

The attacks on 9/11 exposed shortcomings within the U.S. intelligence community in the gathering, processing and sharing of intelligence about foreign terrorists on American soil. Unfortunately, despite military, intelligence, financial, and diplomatic actions abroad, radical Islam continues to spread and terrorist plots continue to be discovered. Several plots have targeted U.S. sites on American soil. These plots have been found to be planned both by foreign terrorists as well as by

U.S. persons either on their own or in collaboration with other foreign terrorists. As a result, we must continue to develop the capacity to find the enemy within—to identify threats, uncover plots, track suspects, uncover networks, and interdict them before they can do harm. We must be able to do this against both foreign and U.S. persons, as the threat is no longer distinguishable by simple divisions between foreign and domestic, at home and abroad. This requirement poses direct challenges to American civil liberties. We must therefore ensure that any domestic intelligence system that may emerge be developed deliberately, with consideration for all elements and stakeholders involved. We must put in place a framework that clearly delimits roles and missions, determines what to collect and how, and elaborates a robust oversight capability to ensure that the privacy and constitutional rights of Americans continue to be protected and preserved.

Chapter Five



The Role of Information and Communication in Disaster Response



Foreword

DENNIS M. MURPHY

Professor of Information Operations and Information in Warfare
Center for Strategic Leadership

The title of this section, “The Role of Information and Communication in Disaster Response” admittedly may not resonate as well as “The Role of the Military in the Next Catastrophe” or “Goldwater-Nichols Equivalent for the Homeland”...or some of the other topics and titles found in this work. In fact, certainly some “warfighters” put up their defenses at the mention of public affairs, public information, media relations and strategic communication. But arguably the United States Government may get the role of the military right (very possibly) and may even get the interagency piece right (perhaps less likely), but if the government doesn’t communicate what they are doing effectively they will lose in the eyes of their audiences, whoever they may be. Perception is reality to the perceiver. Historical examples abound. Expectations that are overblown, or for that matter, not communicated contribute to the problem. The inability to respond to emotive mis- and dis-information exacerbates it even more. To be sure, the government response at all levels to Hurricane Katrina was, to be kind, inadequate. However, the government’s lack of situational awareness compounded by a woefully weak, uncoordinated intergovernmental communication plan created an information vacuum filled by others who then shaped perceptions. And so Hurricane Katrina provides an interesting and important case study in consideration of the strategic value and impact of information in today’s environment. This section addresses these issues and provides recommendations and cautions in consideration of the next catastrophe which, unfortunately but inevitably, will certainly occur.

Dennis Murphy, Professor of Information Operations and Information in Warfare at the U.S. Army War College opens the section by

considering the communications gap that occurred between August 29, 2005 and September 2, 2005...a gap filled by “new” and mainstream media to the detriment of the government. His analysis is anchored in an overview of today’s information environment and how it conflicts with the paradigm of government bureaucracy and current ways of doing business.

Dr. Bob Miller, Senior Research Professor in the Information Management Resources College at the National Defense University, follows with an insightful look at the significant breakdown of critical communication infrastructure and how it contributed to a lack of situational awareness unlike any other previous disaster. Dr. Miller speaks to, among other important factors, the importance of “second responders” as a critical element of immediate infrastructure repair. Among a number of critical national security postings, he is a past Deputy Director of the Critical Infrastructure Assurance Office.

Mr. Mike Perini is the Director of Public Affairs for the North American Aerospace Defense Command and United States Northern Command at Peterson Air Force Base, Colorado. He is a retired Air Force Colonel and has held public affairs positions at all levels of the Air Force. He will pick up where Professor Murphy’s piece leaves off, on September 3rd, when General Honoré **and the military began to receive significant** positive coverage. Mike was responsible for the military public affairs effort in New Orleans during the Katrina response and so provides first hand lessons learned on how effective strategic communication can be planned, coordinated and executed.

The Role of Information and Communication in Disaster Response: An Overview

DENNIS M. MURPHY

Professor of Information Operations and Information in Warfare
Center for Strategic Leadership

Well, I think first of all there was a failure to have real, clear information at our disposal. There was a real lack of situational awareness. We didn't have the capabilities on the ground to give us real-time, accurate assessments of the physical condition of the city.

—Michael Chertoff

Only recently has emphasis (at least in words if not deeds) on the information element of power surfaced as a key contributor to strategic success. In fact the United States is just getting around to coming up with an acceptable term to describe the way the nation wields information as power: Strategic Communication. The government is still arguing about the pure definition of this term, but, in order to establish a baseline, consider the definition from the Department of Defense's Quadrennial Defense Review. Strategic Communication is defined as:

Focused United States Government (USG) processes and efforts to understand and engage key audiences in order to create, strengthen, or preserve conditions favorable to advance national interests and objectives through the use of coordinated information, themes, plans, programs, and actions synchronized with other elements of national power.¹

In its simplest form, strategic communication in disasters and catastrophes serves several purposes: first, prior to the event, it can

1. Department of Defense, QDR Execution Roadmap for Strategic Communication, (Washington, DC: U.S. Department of Defense, 25 September 2006), 3.

serve to manage the expectations of the public regarding the capabilities and potential assistance provided at all levels of government; second it provides public information prior to and during the event to facilitate the safety and security of U.S. citizens; and finally, it can, if proactively and effectively used in conjunction with visible ongoing relief efforts, serve to increase the credibility of government and serve as a calming influence to the citizenry. Strategic communication during domestic disasters also serves a foreign policy role. Effective USG strategic communication can portray the United States as a capable, efficient and effective responder to the needs of its people and so send a message to emerging democracies regarding the role of government toward the needs of its citizens. On the other hand, poor USG strategic communication can contribute to the opposite perception world-wide.

Katrina: A Strategic Communications Timeline

Hurricane Katrina provides an excellent example of the impact of strategic communication on the perceptions of victims, the U.S. domestic population and foreign audiences. Consider the communicated reports and images as reflected in the following timeline:

- Hurricane Katrina made landfall on August 29, 2005 as a Category 4 hurricane.
- AP (The Associated Press) reported mass looting in the French Quarter on August 30th.
- August 31st: The Los Angeles Times reported that tens of thousands were trapped in the Superdome. "A 2-year-old girl slept in a pool of urine. Crack vials littered a restroom. Blood stained the walls next to vending machines smashed by teenagers."
- September 1st: The AP reported: "Storm victims were raped and beaten, fights and fires broke out, corpses lay out in the open, and rescue helicopters and law enforcement officers were shot at as flooded-out New Orleans descended into anarchy Thursday."
- September 1st at 2 p.m. Michael Brown said on CNN: "I've had no reports of unrest, if the connotation of the word unrest means that people are beginning to riot, or you know, they're banging on walls and screaming and hollering or burning tires or whatever."

I've had no reports of that." The following day President Bush publicly praised Brown: "Brownie, you're doing a heck of a job."²

- September 3rd: CNN reported that New Orleans Mayor Ray Nagin called Lieutenant General Russell Honore a "John Wayne dude" who can "get some stuff done. He came off the doggone chopper, and he started cussing and people started moving," Nagin said in an interview.³
- Also on September 3rd the Superdome was fully evacuated. But by the 9th the damage was done. Michael Brown was removed as the lead federal officer and replaced by Coast Guard Admiral Thad Allen. By the 12th Brown had resigned as the head of FEMA.⁴

Were the reports accurate? Did Brown get it wrong? Why didn't he see what the major media reported? What is the role of the media vs. the role of the government in communicating to the various audiences described above? The answer to these questions must start with an examination of the information environment in which the government, media and public communicate today. This information environment provides the context to understand the strategic impact of the time gap described above: a gap where the government's voice was not heard thus creating a vacuum that was quickly filled by other voices.

The Information Environment

Information is the oxygen of the modern age. It seeps through the walls topped by barbed wire; it wafts across the electrified borders.

—Ronald Reagan

Traditionally power has been defined as the ability to influence. This can be done in many ways. Certainly military power influences through coercion. But, information as power co-opts by shaping the percep-

2. This timeline extracted from: Think Progress, "Katrina Timeline"; available from <http://thinkprogress.org/katrina-timeline>; Internet; accessed Nov. 28, 2006.

3. CNN, "The Latest on Katrina's Aftermath," September 17, 2005 [newswire service on-line]; available from <http://www.cnn.com/2005/US/09/16/news.update/index.html?eref=sitesearch>; Internet; accessed November 28, 2006.

4. Think Progress, "Katrina Timeline."

tions of others.⁵ One must consider the challenges of the current information environment on the U.S. government's ability to shape it. News comes from many sources, from mainstream broadcast and print journalists, to someone on the street with a camera cell phone and text messaging, or a blogger with a laptop and Internet service. Images and stories (both accurate and inaccurate, rumor and innuendo) can be transmitted inexpensively and in real-time. Where once nation-states freely wielded information as power, now any one individual, anywhere in the world can strategically impact a nation-state's policies. The role of this "new media" has become so important that it will become a separate portfolio in a proposed reorganization within the office of the Secretary of Defense.⁶ So Thomas Friedman was right: "The world is flat," and when discussing the information environment the world is not only flat, it is shrinking...and rapidly.

The U.S. government (and its military) speaks of information superiority in its doctrinal and policy documents, but this environment not only precludes that superiority, but arguably only allows a government to dominate it for a short, finite period of time. It should be reasonable to expect, however, that the nation as a minimum *manages* the information environment effectively and efficiently. To do so it must proactively tell its story using key influencers as spokespersons and respond to mis- and dis-information rapidly and credibly. It must be available and respond at the beginning of a story. Failure to manage the environment results in what can be referred to as the "genie in a bottle" syndrome. Once the genie is out it's difficult, if not impossible, to get her back in. Likewise, once a story is out in the information environment, especially accompanied by powerful images, it is difficult (but not impossible) to counter. The period of August 29th through September 2nd, 2005, was a critical period in which the government lost its ability to shape perception. To be sure the government's situational awareness based on the significant communication architecture breakdown severely hampered the effort but the bottom line is that the genie was out of the bottle...and, while things would get better, the attitudes of the

5. Joseph S. Nye, Jr., *Soft Power* (New York: Public Affairs, 2004), 2.

6. Based on a discussion with the Office of the Deputy Assistant Secretary of Defense (Joint Communication) on October 26, 2006.

American people and the world were already irrevocably impacted. The U.S. government review spoke to the problem in its lessons learned:

Without timely, accurate information or the ability to communicate, public affairs officers at all levels could not provide updates to the media and to the public...federal, state, and local officials gave contradictory messages to the public, creating confusion and feeding the perception that government sources lacked credibility.⁷

It is through the lens of this information environment, then, that the role of the government and its military in strategic communication during domestic disasters must be examined and that the specific lessons learned from Hurricane Katrina must be viewed.

The Mainstream Media: Filling the Gap

I learned that in addition to enjoying words for the way they could evoke emotion, I also loved them for their usefulness in conveying information.

—Pierre Salinger

It is important to discuss the actions of mainstream media during Katrina through that information environment lens, for it has significantly impacted the business of journalism today. Note that the role of the media as a conduit of public information was filled admirably on the local level by the New Orleans Times-Picayune for their reporting on Katrina. Their heroic coverage under the most difficult of conditions resulted in a Pulitzer Prize for meritorious public service. But, the role of the U.S. broadcast and print media in filling the gap described previously with news reports on the ground cannot be overemphasized. The focus here is on national broadcast outlets, major newspapers and news services for that's where many Americans and foreign news sources get their information. Reporters, no longer acting as objective observers, instead became emotionally immersed in their stories in the midst of the catastrophe. Many Americans will remember Anderson Cooper's coverage of Katrina. Recall Cooper, of CNN, interrupting

7. The White House, "The Federal Response to Hurricane Katrina: Lessons Learned," February 2006, available from <http://www.whitehouse.gov/reports/katrina-lessons-learned.pdf>; Internet; accessed November 28, 2006.

Senator Mary L. Landrieu, a Louisiana Democrat, who was thanking federal officials for their help: "Excuse me, senator," interjected Cooper, "I'm sorry for interrupting. I haven't heard that, because, for the last four days, I've been seeing dead bodies in the streets here in Mississippi. And to listen to politicians thanking each other and complimenting each other, you know, I've got to tell you, there are a lot of people who are very upset, and very angry, and very frustrated.... There was a body on the street in this town yesterday being eaten by rats because this woman had been lying in the street for 48 hours."⁸ Many other reporters followed suit. This is not to imply that Cooper's report was not true, or that it was not important. It is, however, reflective of emotive reporting in isolation that seems prevalent today in contrast to the more objective (yes, balanced) reporting that was a hallmark of journalism in an age past. Such reports had a huge impact on the perceptions of the American and overseas audiences regarding the state of the recovery and thus the capabilities of the government even though, in retrospect, many of these broadcasts were simply inaccurate, fueled by rumors of mythical proportions.⁹ The "genie in a bottle" construct was in play and to this day many believe the initial inflated rumors of rape, murder and other violence.

Broadcast journalism in today's information environment is more than ever before a business; typically a fairly effective self-policing business. But it is about advertising revenue driven by viewership and so "hard-hitting," breaking news sells. The information environment fundamentally drives this journalistic bent. In the old system of journalism reporters provided value added by gathering information in the form of relevant stories and delivering it. Today, in this current

-
8. Alvin Snyder, "Hurricane Katrina-Domestic and Foreign Newscasters View Things Differently," University of Southern California Center on Public Diplomacy, September 18, 2005 [newswire service online]; available from http://uscpublicdiplomacy.com/index.php/newsroom/worldcast_detail/050918_worldcasting/; Internet; accessed November 28, 2006.
 9. Susannah Rosenblatt and James Rainey, "Katrina Rumors," *Los Angeles Times*, September 27, 2005; available from <http://www.latimes.com/news/nationworld/nation/la-na-rumors27sep27,0,5492806,full.story?coll=la-home-headlines>; Internet; accessed December 1, 2007. This article discusses inaccurate reporting based on rumor and speculation and cites numerous cases from numerous media outlets, to include the Los Angeles Times...the newspaper where the article was posted.

environment, information is plentiful and journalists constantly look for ways to make their product more “sellable.” Philip Meyer, holder of the Knight Chair of Journalism at the University of Southern California notes: “Old media no longer have the luxury of producing good journalism out of family pride, civic duty or dedication to maintaining their institutional importance. They have to justify it to short term investors. They have to create a new culture for themselves and find new ways to add value to information.”¹⁰ This is the reality of journalism today. It won’t change. The U.S. government must understand this in order to manage it, but the real issue is that they provided no effective counter to those stories. The good news stories weren’t being told.

Interestingly, reporting of September 11, 2001, events is the exception based on its focus on successes. Saving lives was a value added story.¹¹ But to be fair, 9/11, as tragic and devastating as it was, did not reflect the near total communication infrastructure breakdown caused by Katrina. And so not only was government’s job of providing public information greatly diminished, its ability to establish situational awareness in order to effectively respond was also limited.

Good news stories did eventually begin to flow particularly when General Honore and Admiral Thad Hall became visible, credible spokespersons. But the “gap” in time created an information vacuum that was filled by the broadcast media competing for the “value added” story.

Strategic Communication and Foreign Policy: The Broader Perspective

We must engage more aggressively, explaining and advocating our policies in ways that are fast, accurate and authoritative.

—Karen Hughes

10. Phillip Meyer, “The Proper Role of the Media in a Democratic Society,” in *Media, Profit and Politics*, ed. Joseph Harper and Thom Yantek (Kent, OH: The Kent State University Press, 2003), 12.

11. Frances Edwards-Winslow, “Telling It Like It Is: The Role of the Media in Terrorism Response and Recovery,” *Perspectives on Preparedness*, Harvard University, No. 9 (August 2002), 2.

The lack of strategic communication during the “gap” period had significant impact beyond our shores. While many parts of the world sympathized with our plight and offered significant assistance, emotive and inaccurate media reporting without effective and timely U.S. government response played havoc on the image of the U.S. overseas. South Africa’s “The Star” newspaper reported: “Who would have thought that over a million American citizens would become ‘refugees’ in their own country and flay their government for its failure to come to their aid” quickly enough “or that in the most advanced society in the world...the badly injured would be left for dead because of a lack of assistance?”¹² Qatar’s *Ash Sharq* newspaper on September 5th said the Bush administration’s handling of Hurricane Katrina “made parts of the U.S. appear like Mogadishu and the Congo.”¹³ Similar writings could be read in the popular European press.

The initial overseas reaction of sympathy was quickly replaced by shock. Images and reports in the mainstream press reflected what many audiences saw as evidence of abject poverty and racism from a government that touted democracy and freedom as the ideals for the world writ large. The public diplomacy mechanisms could not react to the bow wave of criticism abroad. The U.S. could not communicate effectively domestically or overseas.¹⁴ Karen Hughes officially took her job (as Undersecretary of State for Public Diplomacy and Public Affairs) on September 9, 2005, a post chartered to tell the American story to foreign audiences. She noted: “We saw pictures on Thursday of people who were waiting to be rescued and didn’t feel that we had

12. Todd Pittman, “Katrina Evokes Questions in Africa,” *Associated Press* (Dakar, Senegal), September 10, 2005; available from http://eccentricstar.typepad.com/public_diplomacy_weblog_n/hurricane_katrina_and_us_image_overseas/index.html; Internet; accessed November 28, 2006.

13. “Review of Arab Editorials,” *The Middle East Times* (Cyprus), September 5, 2005; available from http://eccentricstar.typepad.com/public_diplomacy_weblog_n/hurricane_katrina_and_us_image_overseas/index.html; Internet: accessed November 28, 2006.

14. Based on remarks at a meeting at the State Department by public diplomacy officials that the author attended in September 2006.

arrived quickly enough,” she said, adding that President Bush “has acknowledged that we have to do better and we want to do better.”¹⁵

But once again, the genie was out of the bottle... The damage was done.

RECOMMENDATIONS AND CAUTIONS

In the end, you make your reputation and you have your success based upon credibility and being able to provide people who are really hungry for information what they want.

—Brit Hume

The information environment flattens and shrinks the world, empowering individuals. There is no going back. The asymptotic rise in the ability of the individual to strategically impact the geostrategic playing field through the use of information will continue unabated into the future. The reference to the United States as a “superpower” is a misnomer. It refers only to its prowess in wielding the military element of power. It is certainly not an information superpower. One could argue, in fact, that the government can’t dominate this environment except for short periods of time...and so it must be prepared to manage information to its ends as effectively and efficiently as possible. But even management of the information environment requires a new way of doing business.

Bureaucracies are, by design, cumbersome and slow. The U.S. government is the quintessential bureaucracy in that regard. That is not a bad thing for many aspects of running a nation. The messy business of collaboration and consensus building creates a necessary friction in a democracy. Strategic communication, however, requires a nimbleness that is the antithesis of bureaucratic plodding. Communicating messages that are both proactive and reactive must occur on the turn of a dime. Studies have shown that you have about 15 minutes in today’s information environment to respond to mis- and dis-information or it becomes the truth to the target audience. So, nimbleness must be built

15. “Bush aide: U.S. image tarnished by looting after the hurricane,” *Cox News Service* (Gainesville, FL), September 9, 2005; available from <http://www.publicdiplomacy.org/53.htm>; Internet; accessed November 30, 2006.

into processes, cultures and infrastructure. One must think about this from both a planning and execution perspective.

Centralized policy and contingency planning based on a national strategy is essential. Rapid, decentralized execution of those plans with the flexibility to react to unforeseen circumstances can allow the U.S. voice to be heard domestically and world-wide. If the mainstream media can be on the streets of New Orleans providing real time images and reports, then the government must develop and rapidly deploy communication infrastructure packages that allow its voice to be heard simultaneously. Current ongoing actions at the national level are cautiously encouraging.

Ambassador Hughes has taken positive steps in this regard in the year that she has been in her job. A National Strategy for Public Diplomacy and Strategic Communication has been drafted and is being coordinated within the beltway for potential implementation. She has provided specific guidance to Public Affairs officers at embassies throughout the world that shortcuts (and eliminates in many cases) the requirement for bureaucratic clearances to speak to the international press. She has established a rapid response unit within the State Department to monitor and respond to world and domestic events. And she has established processes to disseminate coordinated U.S. themes and messages laterally and horizontally within the government.¹⁶ The Defense Department recognizes the problem as well and is doing something about it.

The Quadrennial Defense Review (QDR) conducted a spin-off study on Strategic Communication that resulted in a roadmap addressing planning, resources and coordination. Perhaps the most important aspect of the roadmap is the stated objective of creating strategic communication plans in conjunction with policy development, thus fulfilling Edward R. Murrow's desire to be brought in on the takeoff, not the crash landing.¹⁷ However, it is important to point out some cautions.

16. Based on discussions with members of Ambassador Hughes' staff at various times in 2005 and 2006.

17. QDR Execution Roadmap for Strategic Communication: 3.

First, there is a need for culture change within the U.S. government regarding wielding information as power. Senior government officials must seek out opportunities to engage the press. This must be a strategic imperative. To have a voice you must engage vigorously both the press who share your views and those who don't. The U.S. must embrace contrarians such as Al Jazeera, otherwise the Arab world will hear only one side of the story. This also requires that the government develop a culture of engagement with the press. This will mean that it may have to accept some incidents of information fratricide or information collateral damage...however, if it doesn't it will always be behind in today's information environment. Second, processes and organizations must be built that endure beyond this administration. Ambassador Hughes has the ear of the President and therefore may be able to achieve many of her goals even while serving only at the Undersecretary level. But when she departs in two years, it is unlikely that her replacement will maintain that level of trust or power. The short and frustrating tenures of her two predecessors serve as a testament to that reality.¹⁸ Americans have a modern history of distrust of information used as power by the government that goes back to World War I and the Creel Commission, and that was solidified by the propaganda machine of the Germans in World War II. The demise (after four months) of the Office of Strategic Influence in the Pentagon is recent evidence.¹⁹ The United States will never have a Department (or Secretary) of Information so the current positive policy actions must be codified to be enduring. Finally, the government must have both presence and communication infrastructure during crises, both domestic and abroad. Presence does not necessarily mean an American voice, but we must co-opt "key influencers" willing to speak on behalf of America to a target audience who see them as credible. Public affairs organizations must have a rapidly deployable capability, both in people and equipment, which puts them in the street with the mainstream media during disasters and catastrophes. The military has made strides in this regard; the policy level interagency has not.

18. David E. Kaplan, "Hearts, Minds, and Dollars," U.S. News and World Report, April 25, 2005: 27-28.

19. *Ibid.*, 30.

Strategic Communication during disaster response directly supports the ability of the U.S. government to establish a safe and secure environment for its citizens. Accurate public information is critical. Managing expectations and positively influencing perceptions is equally important. Senior leaders must provide accurate messages in conjunction with actions and images that instill public confidence in an information environment that they can rarely dominate. In the end, Strategic Communication is leader's business and leaders must take steps to break bureaucratic paradigms so that they can compete and tell their story.

Hurricane Katrina: Communications & Infrastructure Impacts

DR. ROBERT MILLER

Senior Research Professor, National Defense University

In some respects, Hurricane Katrina was the equivalent of a weapons of mass destruction (WMD) attack on the Gulf Coast. The hurricane caused catastrophic damage over an area roughly the size of Great Britain.¹

However, while it is tempting to view a storm such as Katrina as a once-in-a-lifetime event, doing so would be an exercise in wishful thinking. Although Katrina was a very large hurricane, it was not “The Storm of the Century,” or even “The Big One” which forecasters have warned about for many years. The best estimates are that at landfall, Katrina was at Category 3 strength (winds of 111-130 miles per hour [MPH]).² Sustained wind strength at landfall was about 125 MPH. By contrast, 1969’s Hurricane Camille was a Category 5 storm with winds greater than 155 MPH. Much of the extensive damage caused by Katrina was due to storm surge, especially along the Gulf Coast, and by levee breaches and resulting flooding in the New Orleans area, rather than by the wind and rain from the storm itself.

In other words, it should be clear that Katrina-sized incidents are neither unprecedented nor unlikely to recur. We will see more, and we may well see worse, either from storms, earthquakes, or other natural or man-made causes. The fact that a replay of Katrina-sized events are all but certain makes it all the more urgent that we draw appropriate lessons from the 2005 experience.

-
1. The affected area was approximately 93,000 square miles. See *Hurricane Katrina, Lessons Learned* (GPO, February 2006): Forward.
 2. National Hurricane Center, *Tropical Cyclone Report: Hurricane Katrina, 23-30 August 2005* (20 December 2005): 3.

Katrina as a Critical Infrastructure Collapse

Katrina offers lessons in another sense as well. One way to think about Katrina is to see it as a comprehensive critical infrastructure collapse—perhaps the most widespread critical infrastructure collapse that any advanced country has experienced since World War II. Virtually all of the critical infrastructure sectors in the region were put out of commission at the same time. Failures in one sector had cascading effects on others. These simultaneous failures far exceeded the experience base and available resources of public officials, and led to a partial or complete breakdown in command and control and in public order. Widespread critical infrastructure collapse is one of the marker elements that helps differentiate “catastrophes” from “disasters.”³

The concept of critical infrastructures is one of those classic inside-the-beltway obsessions that often seem to have little resonance in saner parts of the country. That’s unfortunate, because I suspect that as the 21st century goes along we will all find ourselves paying more attention to the implications of vulnerabilities in our critical infrastructures. There’s reason for this concern, given the ways in which today’s globalized, just-in-time, interconnected world magnifies the consequences of regional catastrophes. Globalization and interconnections mean that events which once could have been handled locally will have widespread ripple effects, and that these effects can be unexpectedly disruptive.

As one government commission put matters:

“...the U.S. has developed more than most other nations as a modern society heavily dependent on electronics, telecommunications,

-
3. For planning purposes, the government distinguishes between “catastrophes” and what could be called more typical disasters. The Catastrophic Incident Supplement to the Dec. 2004 DHS *National Response Plan* defines a catastrophic incident as: “any natural or manmade incident, including terrorism, that results in extraordinary levels of mass casualties, damage, or disruption severely affecting the population, infrastructure, environment, economy, national morale, and/or government functions. A catastrophic incident could result in sustained national impacts over a prolonged period of time; almost immediately exceeds resources normally available to State, local, tribal, and private-sector authorities in the impacted area; and significantly interrupts governmental operations and emergency services to such an extent that national security could be threatened. All catastrophic incidents are Incidents of National Significance. These factors drive the urgency for coordinated national planning to ensure accelerated Federal/national assistance.”

*energy, information networks, and a rich set of financial and transportation systems that leverage modern technology. This asymmetry is a source of substantial economic, industrial and societal advantages, but it creates vulnerabilities and critical interdependencies that are potentially disastrous to the United States.”*⁴

These potential dangers are particularly acute in the “information infrastructure.” Our economy and indeed all of society now depend—to a far greater degree than, say, twenty years ago—on the continued operation of the Internet and other networks and systems. These are important in their own right. And increasingly they act as control systems for other infrastructure sectors.

Viewed in this light, Katrina is a possible harbinger of what we can expect if (or when) similar critical infrastructure collapses happen in our future. During Katrina, these infrastructure collapses occurred rapidly, almost simultaneously, and over a very wide area. The multi-state nature of the collapse inhibited effective response—as it is likely to do in any future incident.

Katrina’s Impact on the Communications Sector

Communications was one of the critical infrastructure sectors that were most severely affected by the hurricane and its aftermath. Paul McHale, the Assistant Secretary of Defense for Homeland Defense, stated that “the magnitude of the storm was such that the local communications system wasn’t simply degraded; it was, at least for a period of time, destroyed.”⁵ Over 180 central office locations were running on generators as commercial power sources failed. About

4. *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack*, (2004): 2.

5. Quoted in, *Hurricane Katrina, Lessons Learned*, p. 34. The statement can be found in Paul McHale, Assistant Secretary of Defense for Homeland Defense, testimony before a hearing on Hurricane Katrina: Preparedness and Response by the Department of Defense, the Coast Guard, and the National Guard of Louisiana, Mississippi, and Alabama, on October 27, 2005, House Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, 109th Congress, 1st session: 74.

100 commercial radio stations were forced off the air.⁶ Up to 2,000 cell towers were also knocked out and responder Land Mobile Radio communications were significantly degraded.⁷ Emergency 911 service was severely damaged, and surviving stations were soon overwhelmed by spiking call volumes as desperate people tried to get help or check on those at risk. According to the Federal Communication Commission's "Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks":

The destruction to communications companies' facilities in the region, and therefore to the services upon which citizens rely, was extraordinary. Hurricane Katrina knocked out more than three million customer phone lines in Alabama, Louisiana, and Mississippi. The wire line communications network sustained enormous damage—dozens of central offices and countless miles of outside plant were damaged or destroyed as a result of the hurricane or the subsequent flooding. Local wireless networks also sustained considerable damage—more than a thousand cell sites were knocked out of service by the hurricane. At the hurricane's height, more than thirty-five Public Service Answering Points (PSAPs) were out of service, and some parishes in Louisiana remained without 911 or enhanced 911 (E911) service for weeks.⁸

In addition to the immediate damage to communications, the storm had a variety of indirect, persistent effects. As the FCC panel noted, much of the backbone conduit for landline service was flooded out. So were many of the central switching centers. Wireless capabilities were degraded as cell towers were put out of commission. The sustained loss of electrical power meant that those facilities that survived the initial storm had to run on back-up generators or batteries. Some of these were flooded out and many of the others soon ran out of fuel. Widespread disruptions of transportation, roads and bridges—and, as we will see,

6. Testimony, Kenneth Moran, Director, Office of Homeland Security, Federal Communications Commission, before the House Committee on Homeland Security, Oct. 26, 2005.

7. Testimony, Dr. Peter Fonash, Deputy Manager, National Communications System, before the House Committee on Homeland Security, Oct. 26, 2005.

8. Report and Recommendations, Paragraph 2.

the collapse of command and control—hobbled repair crews and made local re-supply of such fuel difficult or impossible.

To be sure, not all communications facilities suffered equally. Some of the private networks maintained by utilities and others continued to function reasonably well. Satellite phones also worked once the immediate storm passed, although they were in very short supply and eventually many ran out of battery power. Satellite radio, such as XM and Sirius, continued to function. Other forms of radio, including amateur (ham) radio, also continued to operate as long as power was available.⁹ However, these systems brought only limited relief to the overall communications problem. Finally, the Federal Emergency Management Agency's (FEMA) Mobile Emergency Response Support (MERS) teams are designed to provide emergency communications, but apparently had little impact during the first few days after the hurricane landed.¹⁰ The White House *Katrina Report* described the results, "The complete devastation of the communications infrastructure left responders without a reliable network to use for coordinating emergency response operations."¹¹

The communications failure also severely damaged the control systems—known as Supervisory Control and Data Acquisition (SCADA) systems—that manage many other systems and infrastructures. These systems, many of which depend on the Internet, were often put out of business for prolonged periods.

Failures in maintaining working systems—what are called *operability* problems—were exacerbated by long-standing issues with *interoperability*. While it was not exactly news that many public entities have problems in communicating with each other, the impact of these

9. The NCS Shared Resources High Frequency Radio Program continued to work and provided important, though necessarily limited, services during the emergency. See Fonash testimony cited above.

10. *A Failure of Initiative* reports that the senior Federal official in Mississippi testified that despite deployment of a MERS unit, Mississippi's "communications capabilities were far short of what was needed to be effective." p. 165.

11. White House, *Katrina Lessons Learned Report*, p. 37. The report provides a vivid description of the consequences of the communications collapse.

interoperability failures was magnified when “normal” communications links blinked out.¹²

Operational Consequences for Government: “The Fog of Katrina”

The consequences of this massive communications failure were both swift and severe, especially in southern Louisiana. Modern governments—and for that matter modern societies—depend heavily on telecommunications. This is especially true in emergencies. The communications capabilities that most public agencies depend on for everyday operation were eroded, and in some places eliminated, for days and in some cases for weeks. In effect, when communications went out something like the “fog of war” descended upon the Gulf Coast. To quote just two examples, the New Orleans Police Department’s communications system was inoperative for three days after the hurricane, and only a few backup channels were available to first responders in the area.¹³ Mississippi’s National Guard responders were unable to establish effective communications links with the governor or the state’s emergency management agency for 48 hours after the hurricane hit.¹⁴

Law enforcement units who rushed in from other jurisdictions often had two-way radios that used different frequencies than local police, DoD military responders found it difficult or impossible to communicate with FEMA or other civilian authorities, some of the key data was locked away on classified systems, and situational awareness—knowing what was going on, who was where, who needed what, and who was going where and when—was significantly degraded. The federal government’s systems for setting call priorities

12. The two terms deal with different things. From a responder/ government point of view, “operability” exists when users have a basic level of communications. “Interoperability” means that responders and officials from different jurisdictions and agencies can communicate with each other and exchange data in real-time. You can’t have the latter without the former. See the Statement of Dr. David Boyd, Director, Office for Interoperability and Compatibility, Science & Technology Directorate, Department of Homeland Security, before the U.S. House Committee on Homeland Security, April 25, 2006.

13. House of Representatives, Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, *Final Report: A Failure of Initiative*, H. Rpt. 109-396, Feb. 15, 2006: 164.

14. *Ibid.*, 168.

seemed to work effectively, but the lack of basic operability limited their effectiveness.¹⁵

One persistent problem was the lack of basic coordinating information: “No knowledge management plan existed for incident response. There was no central list of information needs, or listing of potential information sources, to help prioritize reconstitution efforts. Joint task force phone numbers were not preassigned, and several numbers changed while the response was underway. In many cases, key messages were printed and handcarried around command centers to make sure incident managers had the right information.”¹⁶ In military terms, government lost its “C 4 ISR” (or Command, Control, Communications, Computers, Intelligence [in the sense of situational awareness], Surveillance, and Reconnaissance) capability.¹⁷ Without working communications, government at all levels was in effect deaf, dumb, and blind, blundering about and trying to make sense of an endlessly confusing and rapidly changing situation. This rapidly led to chaos.

All of these factors degraded the ability of public officials to keep up with events and try to direct recovery efforts. Also—and very importantly—the lack of authoritative and believable information from public officials created a climate rife with rumor, misinformation and speculation, significantly reduced the government’s ability to

15. The National Communications System, or NCS, is the primary Federal government agency responsible for emergency communications. NCS operates several emergency services, such as the Government Emergency Telecommunications Service (GETS), which gives critical users priority for landline calls, and the parallel Wireless Priority Service (WPS). For emergency situations NCS operates a high-frequency radio system (called SHARES), as well as the Telecommunications Service Priority (TSP) program for restoration purposes.

16. Lt. Col. Greg Gecowets, “Coordination, Command, Control and Communications,” Joint Center for Operational Analysis Quarterly Bulletin, Vol. VIII, Issue 2, June 2006, p. 20. Colonel Gecowets points out that responding DoD elements had trouble creating an unclassified situational awareness picture, since most of their resources are (for understandable reasons) classified. Accessing classified systems from the field and sharing information among emergency centers was often difficult, and in any case, classified systems are usually unavailable to civilians.

17. To use another military term, the many units and agencies in the area lost the ability to create and maintain a common operational picture. Trying to make sense of the situation absorbed a great deal of senior leaders’ time and energy.

maintain public order, and added to the sense of dislocation and loss of public confidence. As one analyst put it: "Numerous media reports described incidents of crime and murders at the refuges of last resort, snipers shooting at rescuers, and other significant degradation in civil order. Although re-examination of these events has shown that many of these reports were in error or exaggerated, they had an impact on the allocation of resources and actions of responders because government officials lacked a realistic understanding of the situation in New Orleans, as well as the capability to convey an accurate picture of what was going on to the public."¹⁸

This feeling of dislocation came as a shock and a surprise to both the government and the public. A House of Representatives report summarized the consequences and deserves extended quotation:

Poor situational awareness and its resulting effect on command and control contributed to the negative effects of inaccurate media reports because public officials lacked access to the facts to address media reports. Throughout the early days of the response, media reports from New Orleans featured rampant looting, gunfire, crime, and lawlessness, including murders and alleged sexual assaults at the Superdome and Convention Center. Few of these reports were substantiated, and those that were—such as the gunfire—were later understood to be actually coming from individuals trapped and trying to attract the attention of rescuers in helicopters. Officials on the ground in New Orleans interviewed by Select Committee staff stated the media greatly exaggerated reports of crime and lawlessness and that the reports from the Convention Center and Superdome were generally unsubstantiated...

The near total failure of regional communications degraded situational awareness and exacerbated problems with agency coordination, command and control, logistics, and search and rescue operations. Reliable communications are critical to the preparation for and response to a catastrophic event because of the effect they have on establishing command and control and maintaining situational awareness. Without functioning

18. James Henry, *Incomplete Evacuation*, Joint Center for Operational Analysis Quarterly Bulletin, Vol. VIII, Issue 2, June 2006: 7.

*communications systems, first responders and government officials cannot establish meaningful command and control, nor can they develop the situational awareness necessary to know how and where to direct their response and recovery efforts. Similarly, without the ability to call for help, citizens cannot seek emergency assistance, alert responders or others to their whereabouts and needs, or receive updates or instructions from officials.*¹⁹

This problem was not limited to Southern Louisiana. The communications blackout along the Gulf Coast was almost as bad, at least for a while. As historian Douglas Brinkley put it in talking about Hancock County, Mississippi:

*The cell phone towers had all been knocked out, and the landlines were down, so communication was as primitive as a rag waved frantically by a person in trouble.*²⁰

In many cases, the inability to communicate led to a sense of paralysis. Here's Brinkley again:

*In a city surrounded by water, the police had only a handful of operable boats. Their radio system, cellular communications, and landlines went down simultaneously. They were without satellite phones. Because of flooding they couldn't even send couriers from one part of the city to another. [Quoting New Orleans Deputy Police Chief Warren Riley] "As a commander, as a captain, you prepare for weapons of mass destruction, for a terrorist situation, for hostage situations, SWAT situations, things like that. We prepared for terrorists trying to take over the Superdome. We prepared for terrorists to come down on Bourbon Street during Mardi Gras. But this storm was the ultimate enemy. It cut off the food, the water, the transportation, the lights. It segregated your units and stranded them where they couldn't do their assignments... This storm was absolutely beyond plausibility. How do you prepare for this?"*²¹

19. House Select Bi-partisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, Final Report, *A Failure of Initiative*, House Report 109-396, Feb. 15, 2006: 165 & 169.

20. *Ibid.*, 163.

21. *Ibid.*, 202 & 208.

After a few days of this, the repair of some communications facilities and the deployment of backup systems helped dispel this confusion and allowed government at all levels to begin to get a grip on the many problems facing the region. But it was a long—a very long—week before this “fog of Katrina” began to dissipate.

Some Implications

It would be an exercise in wishful thinking to pretend that Katrina was a unique event and nothing like it will happen again. Although we pray that it doesn't, prayers are no substitutes for prudent policy.

The communications sector is a case in point. Although all parties agree on the fundamental need for a more robust and inter-operable network, and Federal, state and local governments have made efforts to improve both basic operability and interoperability, the process can perhaps best be characterized as “stately.” What is missing, it seems, is the kind of sense of urgency that is needed to overcome the many forces of inertia within our federal system of government.

There is a larger concern at work here as well. As a starting point, we should realize that there is a significant policy difference between a catastrophe such as Katrina and a more “typical” disaster. As noted, the former was a full-scale and widespread critical infrastructure collapse that rapidly outstripped the coping capability of local, state and national government. As a result, many of the things that most of us have come to expect in an advanced, 21st century civilization disappeared for a few days, and the result was that government was paralyzed and society in some cases slipped back into a state of nature. Of course we cannot know what or where the next catastrophic event will be, but we can be reasonably sure that many of the same problems—including the communications problem, with all the difficulties it brought in its train—will recur in the next catastrophe—whatever its causes—and in fact the next one may very well be worse than Katrina. After all, with Katrina we had plenty of warning and we knew there wasn't likely to be a second onslaught (although Hurricane Rita came close). As a result, response groups and the government had time to respond, suffered few if any direct losses, and could operate with little fear of

further incidents. We can easily imagine scenarios where none of these favorable circumstances will apply.

Mitigation and Restoration Efforts: The “Second Responder” Issue

In the immediate aftermath of a disaster, attention is properly focused on rescue operations and first-responder needs. But as Katrina shows, there is also a compelling need to attend to what could be called “second responders”—those who begin the often arduous process of restoring basic services. These second responders are the ones who help restore electric power and the communications nets, clear the roads and patch the holes in critical infrastructures. They can be thought of as the necessary reinforcing wave in any recovery operation.

Although we cannot realistically hope to prevent another event such as Katrina, we can certainly take a number of steps to mitigate its effects and improve “second responder” operations. This is particularly important in dealing with such essential infrastructures as communications.

Some of the policy options that may improve the speed and effectiveness of both first- and second-responder actions in the communications sector include:

- Taking further steps to make it easier for military assets in areas such as wireless communications to backstop local response and law enforcement resources. Military communications networks, often encrypted and with a heavy emphasis on security, have not been designed to carry out homeland defense missions that require interoperability with emergency responders and civilian agencies. Although this lack of interoperability may have made operational sense in the 20th century, it is worth re-examining in light of current realities.²²

22. Active duty DoD assets (often referred to as “Title 10” forces) are generally seen as “responders of last resort,” which will be called in only when other local, state and federal resources are inadequate. For a general discussion of the problems caused by interoperability difficulties between the military and civilian agencies, see Government Accountability Office, *Hurricane Katrina: Better Plans and Exercises Needed to Guide the Military’s Response to Catastrophic Natural Disasters*,” (GAO-06-643, May 2006).

- Embarking on a broader re-examination of the military's proper role in responding to catastrophic incidents. Under the National Response Plan, the general rule is that the military backs up but does not supplant other responders.²³ However, it is increasingly obvious that only the active duty military has the resources, mobility and deployability needed to respond to catastrophic events that affect large areas and cross state lines.
- Building more redundancy into the current telecommunications networks at critical nodes.
- Requiring public communications carriers to maintain adequate and tested back-up facilities.
- Devoting resources to improving our ability to collect and disseminate accurate, prompt public information in order to reduce the kinds of false rumors that were so widely disseminated by the media in the immediate aftermath of the hurricane.
- Taking steps to reduce the time and effort needed to restore critical services and infrastructures when things do go wrong, including intensified efforts to create more rapid-deployment resources within DHS and creating more rapid-deployment federal/state/local joint operations centers.²⁴
- In general, working more closely with non-governmental entities and the private sector to enable a coordinated, less spasmodic response effort.
- Trying to untangle the Gordian knots—almost all of them political and not technical—that have limited interoperability.

Summary

Katrina provided a foretaste of what we can expect if and when the country faces another truly catastrophic incident. Given our increased

23. There are partial exceptions, notably in the case of catastrophic events that call for immediate response on a major scale; however, activation of the so-called Immediate Response Clause requires requests from cognizant civil authorities (as of this writing the requirement for an initiating civilian request is now under review, in good part because of the Katrina experience, and may be modified).

24. FEMA's Mobile Emergency Response Support (MERS) units saw their staffing and resources steadily reduced in the years before Katrina.

dependency on critical infrastructures and the speed with which these can collapse, it makes sense to learn Katrina's lessons while we still have time. One of these lessons is the importance of getting communications capabilities up and running as quickly as possible. Doing so requires a mix of technical and policy changes that, together, will serve to mitigate damage and accelerate restoration.



Public Communications: Vital Link to Maintaining the Public's Trust During Crisis

MICHAEL B. PERINI

Director of Public Affairs

North American Aerospace Command and U.S. Northern Command

Scene Setter

Pick up a daily newspaper; turn to any national news broadcast; type in the web address for your favorite Internet search engine. What you find from these sources is a smorgasbord of crises du jour.

Several recent examples:

- *A website claims that seven National Football League gridiron stadiums will be attacked with radiological dirty bombs. NFL stadiums in New York, Miami, Atlanta, Seattle, Houston, Oakland and Cleveland.¹ Fortunately, only a hoax, the FBI states.²*
- *What was initially thought to be another 9/11 attack over New York City turned out to be a tragic aircraft accident taking the life of New York Yankee pitcher, Cory Lidle, who crashed into a 50-story apartment building on Manhattan's Upper East Side.³*
- *Within moments of the Space Shuttle Discovery, STS-121, taking off the pad in Florida, on July fourth⁴ North Korea was making their own holiday fireworks launching seven missiles, one a long-*

-
1. Lara Jakes Jordan, Government doubts threat on NFL stadiums, AP, www.chron.com, Washington D.C., Internet accessed October 19, 2006
 2. Milwaukee (AP), Football Stadium threat is a hoax, FBI says after interviewing Milwaukee man, STRATCOM FMA News Desk, October 19, 2006
 3. Chris Dolmetsch and Peter Young, Plane With Yankee's Lidle on Board Crashes in NYC (Update 3), www.bloomberg.com. Internet accessed October 19, 2006.
 4. Spaceflight Now, STS-121 Mission Archive Discovery is home, Available at www.spaceflightnow.com/shuttle/sts121/, Internet accessed October 20, 2006.

range type.⁵ For several frightening moments their final impact points were unknown. Was the United States a target?

Daily, at local, state and federal levels, there are situations that cause the public affairs (PA) community to rapidly decide to engage or to not engage in public communications. The instant information age in which we work and live with Internet access nearly everywhere from homes to offices, from airports and coffee shops to mobile devices now hanging from ears of driver—is jammed with components that bring news and information rapidly to our citizens. The potential downside for the PA practitioner is there is little time to execute crisis strategic communication plans and be responsive to an onslaught of public inquiry.

In the future, the speed and flow of information will continue to increase requiring organizations to use all the tools of a 21st century society when addressing, affecting and assessing public opinion.

The global war on terrorism adds another dimension in public communications for the Department of Defense (DoD) and federal agencies at large. We operate in a dangerous, changing and uncertain security environment. Today, threats are diverse, adaptive and real. Terrorists do not operate on conventional battlefields but thrive in the “gray area” where notions of crime and armed conflict overlap. These circumstances make the work of the PA professional more challenging than ever.

Furthermore, the terrorists have an interest in influencing public opinion. A document recently posted on extremist websites describes a plan to “invade the U.S. media.”⁶ The document, written by the Global Islamic Media Front, the communications arm of Al Qaeda, states its priorities as translating Al Qaeda speeches, interviews and other messages into English and disseminating them to American newspapers, forums, television channels, prominent opinion makers and research groups.⁷ “People of the Jihad have to create a media war that goes parallel to the military war.”⁸

5. AP, West Coast Missiles on Alert After Test, USSNORTHCOM & NORAD News Clips, Colorado Springs, July 6 2006.

6. OSD Writers Group Office of Public Affairs, The Nature of the Enemy, 17 October 2006, Pentagon, Vol 1, Issue 2.

7. Ibid.

8. Ibid.

The American government has failed to match the enemy's sophistication.⁹ "Our enemies have skillfully adapted to fighting wars in today's media age, but for the most part we—our country, our government—has not adapted," conceded Defense Secretary Donald Rumsfeld in February, 2006.¹⁰

The circumstances of a crisis, from a homeland defense mission to disaster response, may differ in particulars but there are common threads regardless of the incident. A crisis:

- Does not occur at a time or place of your choosing
- Has potential to threaten the future of your organization, CEO or domain
- Creates victims (self-identified)
- Allows little to no reaction time to research, plan, execute and evaluate
- Requires strong leadership by the senior public affairs counselor

Bridging the Gap: NORAD and USNORTHCOM

Some aspects of all three examples cited in the first section have touched the commands of North American Aerospace Defense Command (NORAD) and U.S. Northern Command (USNORTHCOM).

NORAD has been engaged in crisis management for nearly 50 years. NORAD was established in 1958, headquartered in Colorado Springs, Colorado. The organization was envisioned as a bi-national command, centralizing operational control of continental air defenses against the threat of long-range Soviet bombers and ICBMs. NORAD contributed to winning the Cold War by maintaining its deterrence posture.¹¹

The events of September 11, 2001, demonstrated NORAD's continued relevance to North American security with a new focus against threats within NORAD's area of operations. Some of NORAD's post 9/11

9. Douglas B. Sosnik, Matthew J. Dowd and Ron Fournier, *Applebee's America*, Simon & Schuster, New York, 2006, 142-143.

10. *Ibid.*

11. NORAD-USNORTHCOM Directorate of Public Affairs, NORAD 101 Brief version 6, NORAD-USNORTHCOM, Colorado Springs, August 15, 2006.

missions have included supporting National Special Security Events such as space shuttle launches, G-8 Summits, national political conventions, and the Reagan funeral. NORAD conducts irregular air patrols within the United States and Canada and is always prepared to scramble and divert aircraft in response to suspected air incidents.

The terrorist attacks of 9/11 made it very clear that the strategic environment we operate in has changed significantly since the fall of the Berlin Wall and the end of the Cold War.

USNORTHCOM, created in the wake of 9/11 is charged with conducting operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories, and interests.

USNORTHCOM partners and shares information with other agencies to protect our people, national power and freedom of action. The command also provides defense support of civil authorities (DSCA), including consequence management operations, as directed by the President and Secretary of Defense.

The importance of the unity of command provided by USNORTHCOM cannot be overstated. USNORTHCOM is a combatant command, with a headquarters staff of 1,200 located in Colorado Springs that includes active duty, reserve and National Guard members, from the Army, Navy, Air Force, Marine Corps and Coast Guard. It also includes civilian employees, contractors and some 60 liaisons from various federal agencies.

As a regional combatant command, within DoD, USNORTHCOM can work with federal agencies at a tactical and operational level, but policies are set at the DoD level.

USNORTHCOM operates in a specific Area of Responsibility (AOR) in accordance with the Unified Command Plan of May 2006. What makes USNORTHCOM's AOR unique is that our homeland falls within it.¹²

12. NORAD-USNORTHCOM Directorate of Public Affairs, USNORTHCOM 101 Brief version 6, NORAD-USNORTHCOM, Colorado Springs, August 15, 2006.

Examples of USNORTHCOM's missions:

- Missile Defense operations
- Supporting National Special Security Events such as the national political conventions, the G-8 Summit, and the United Nations General Assemblies
- Shuttle launch support
- Helping federal agencies when they ask for military assistance in the fight against wild land fires
- Hurricane aftermath assistance and other natural disaster support

We also conduct or participate in exercises. Some, like TOPOFF (Top Officials), a national-level, multi-jurisdictional, “real-time,” limited-notice response exercise are opportunities for several state and federal agencies, including the DoD, to practice working together.

Having one commander for two commands facilitates a top down direction for a public affairs policy that allows for the timely and accurate release of public information. The “Principles of Information,” signed in 2001, by Secretary of Defense Rumsfeld, outline the Department’s obligation to provide the public with information so that they “...may assess and understand the facts about national security and defense strategy.”¹³

The commander’s focus for public communication—accurate, available, and aggressive—drives activities, programs and events for the dual-hatted NORAD and USNORTHCOM Public Affairs Directorate, ensuring that public communications occur during both the homeland defense and disaster response missions.

Crafting a Public Affairs Strategy

“Our institutional reputation depends on our ability to create and foster a positive image...”

—Charting Our Future, Air Force PA Strategic Plan, March 1995 ¹⁴

13. Donald Rumsfeld, “Principles of Information,” OSD PA, November 2001.

14. U.S. Air Force Office of Public Affairs, Charting Our Future, U.S. Air Force, Washington, D.C., March 2005.

This may be a statement of the obvious, but when published more than a decade ago it was one of the first efforts to recognize the strong link between an institution's ability to retain and sustain faith with the public and with those within the U.S. military organization.

Having a positive image begins with a concept called "positioning."¹⁵ Positioning, first introduced in the '80's, can start with a product, a service and yes, an organization. "Positioning is not what you do to a product....Positioning is what you do to the mind of the prospect.... That is, you position the product in the mind of the prospect," say Al Ries and Jack Trout, marketing and advertising experts.

Positioning has had a difficult time in gaining traction in the U.S. military. However, positioning is essential as an integral part of the public communications strategy as organizations within the U.S. military come to grips with the difficult problem of getting heard in an over communicated society. Having a strong positive position with the public adds credibility when communicating to the public during a crisis or disaster response.

In order to position to maintain the link between an institution and the public, PAs must draft and obtain approval for contingency, action step strategies. Each strategy must be backed by a thorough strategic communication plan. Building a plan will drive successful outcome, during a "brush fire." Elements of the plan should include:

*Foreword, Contents, Executive Summary, Purpose, Vision, Overview, Situation, Objectives, Issues, Audiences, Themes, Messages, Strategies and Tactics, Responsibilities, Core Values, Communication Goals and Metrics, Execution Timelines, Communication Tools, Audiences and Stakeholders, Measurement and Assessment Tools, and Operating Principles.*¹⁶

One area often overlooked in crafting a PA strategy is the development of an exit plan. As the DoD response to Katrina was winding down,

15. Al Ries and Jack Trout, *Positioning: The battle for your mind*; Warner Books, Inc., New York, 1986: 2.

16. Gen Ed Eberhart and Michael Perini, *Public Affairs Roadmap 2003-2004* United States Northern Command, NORAD-USNORTHCOM, Colorado Springs, 2003.

we faced a new challenge: how to *tell the public the DoD mission was finished*. Fortunately, we had gathered a good deal of information from our previous efforts and were able to develop a transition strategy to match the departure of DoD personnel. Our transition strategy was:

- Adapt PA activities to help manage public expectation as DoD presence declines
- Work hard to replace “soldier” with “civil authority” in images
- Refocus the public on our “deter and defend” missions
- Remain engaged regarding examination of the DoD response effort

The Interagency piece: Katrina Lessons Learned

Let’s review the facts for Hurricane Katrina:

- Over 1 million people displaced; with 270,000 to emergency shelters
- 1,700 children separated from families
- Second deadliest storm in the nation’s history; over 1,200 dead
- Cost as much as \$200 billion
- Largest domestic humanitarian military operation in U.S. history
- 70,000 military personnel deployed for Katrina – 30,000 for Hurricane Andrew, the previous U.S. natural disaster benchmark
- During height of mission, more helicopters supported this operations than currently in Iraq and Afghanistan combined
- More than 18,000 flight sorties
- 49,773 people rescued
- 3,800 animals rescued
- 25,000 DoD personnel involved¹⁷

Every disaster is local. The state with their respective National Guard forces provides the initial backup to the local first-responders. The governor can always ask for federal assistance. That assistance first comes from a variety of federal agencies. If those agencies can’t provide the support, they can turn to DoD and USNORTHCOM.

17. Michael Perini, Hurricane Katrina a Department of Defense Perspective, NORAD-USNORTHCOM, Colorado Springs, 2005, v 1.0.

By any public affairs standard of measurement the devastating aftermath of Katrina made disaster response public communications a Herculean task at all levels. Local and state officials are responsible for directly communicating with the people in their jurisdictions. Public officials had to convey the scope and urgency of the emergency—and that included issuing evacuation orders. The hurricane destroyed much of the communications infrastructure, making public communications difficult. Only one radio station was left on the air. USNORTHCOM provided 10,000 radios for Katrina evacuees.

One of the capabilities DoD provided was loudspeaker-equipped trucks—a capability normally used only for psychological operations overseas. The Federal Emergency Management Agency (FEMA) provided the messages; DoD operated the equipment. Another capability, the Digital Video and Imagery Distribution System, or DVIDS, is a system that allows both military and civilian journalists to transmit media products via satellite from remote locations for use by civilian media outlets.¹⁸ The availability of a DVIDS type system at all levels would have helped alleviate the gap in public information.

Keeping the responders informed was a major challenge. Not everyone had access to FOX or CNN. For the military, we relied heavily on our “chain of command” communications, but for others the structure was less concrete.

Images are powerful. Playing over and over were Superdome scenes, buses in the water and desperate people on roof tops. The U.S. military released positive images, both photos and video, of personnel saving lives and restoring infrastructure. We had a specific strategy, but unfortunately it took a while to get resources positioned. By the end hundreds of photos and hours of video were available to the media and public.

Finger Pointing Unfortunate

The Federal Response to Katrina, Lessons Learned, Chapter 5,¹⁹ cites the Federal government’s dissemination of essential public information

18. DVIDS, Available at <http://www.dvidshub.net/index.php>, Internet accessed November 1, 2006.

19. Frances F. Townsend, The Federal Response to Katrina, Lessons Learned, White House, Washington D.C., February 2006, Chapter 5.

prior to landfall as one of the most positive lessons learned. “The many professionals at the National Oceanic and Atmospheric Administration (NOAA) and the National Hurricane Center worked with diligence and determination in disseminating weather reports and hurricane track predictions...”²⁰

However, the report states the federal public communications and public affairs response proved inadequate and ineffective. More could have been done by officials at all levels of government, the report stated. “Without timely, accurate information or the ability to communicate, public affairs officers at all levels could not provide updates to the media and to the public,” according to the report. It took several weeks before public affairs structures, such as the Joint Information Centers, were adequately resourced and operating at full capacity.²¹ Federal, state and local officials gave contradictory messages to the public, creating confusion and feeding the perception that government sources lacked credibility, according to the report.

DoD Response a Success

Despite all the discussion and finger pointing at the federal response to public communications, we consider the active duty DoD response one of the successes of Katrina.

Communications—clear, accurate, and often—is an invaluable weapon in the U.S. military’s efforts in homeland defense and disaster response. Only as a result of an informed work force and public can USNORTHCOM wage a war or manage the peace. This is not a new concept. Clausewitz cited public opinion as a center of gravity in warfighting.²² Abraham Lincoln said, “Public sentiment is everything. With it, nothing can fail. Without it nothing can succeed.”²³

The DoD’s active duty support was lead by USNORTHCOM, Directorate of Public Affairs. The office was recognized with the 2006

20. Ibid.

21. Ibid.

22. Carl von Clausewitz, *On War*, edited and translated by M. Howard and P. Paret, Princeton University, NJ, 1984: 88.

23. The Collected Works of Abraham Lincoln, Roy P. Basher, ed., Vol. III, Lincoln-Douglas Debate at Ottaway (Aug. 21, 1858): 27.

Public Relations Society of America (PRSA) Silver Anvil Award in the crisis communications category. USNORTHCOM coordinated the active duty public affairs efforts for the largest military deployment and humanitarian mission in the United States since the Civil War.²⁴ “We congratulate U.S. Northern Command for the public relations program that incorporated measurable and sound research, planning, execution and evaluation.... This program contributes to the best practices of our industry,” said David M. Imre, 2006 Silver Anvil Chair and president of Imre Communications, LLC.²⁵

With the largest DoD response ever to a domestic disaster, we had to quickly deploy a team of Public Affairs Officers (PAO). The collective effort of nearly 100 DoD public affairs specialists, many of whom deployed to more than a dozen locations in the region, affected an environment where public opinion and media coverage were already negative toward the initial failed federal response.

As with any military organization, we established clear lines of authority. Additionally, we provided officers to help staff the Federal Joint Information Centers.

Once DoD was engaged in the operation, our challenge became one of coordinating and communicating with other federal agencies and the National Guard Bureau who had state status PAOs on the ground. Although there was a daily conference call among all agencies, a physical Federal Joint Information Center was not established until 10 days after the hurricane hit.

We relied on that daily conference call and established our own conference calls with our deployed military PAOs. Additionally we relied on email to provide written guidance and background materials throughout the DoD.

People felt reassured once Lieutenant General Russ Honoré started to appear on TV. General Honoré understood that public communications was an important element to his job. He was brash, earthy and

24. U.S. Northern Command, “U.S. Northern Command wins PRSA Silver Anvil award,” news release, June 12, 2006.

25. *Ibid.*

frank—not normally traits you would look for in a media spokesman. He was also from Louisiana, a proven leader, and accessible. He fit the situation. A USA Poll of 1,200 Americans voted him the most effective leader of the relief operation.²⁶

The Katrina challenge and the challenge still today is that USNORTHCOM will not be the only organization attempting public communications in disaster response. Local, state and federal levels, plus the private sector, will have their spokespeople, press releases and news conferences. The airwaves will be crowded. A clear pathway must be built to sustain faith by the public in organizations involved. Integration, fusion and timely dissemination of information will be the greatest challenges faced by the federal government.

The National Response Plan

The National Response Plan (NRP) published in December 2004, clearly outlines the federal government's role and delineates the responsibilities of all federal agencies including DoD. The NRP places the Department of Homeland Security (DHS) as the lead for Emergency Support Function (ESF) 15 and the conduct of public communications.

Note that this is a "National" response plan, not a "Federal" response plan. This recognizes that the response to any disaster is a national effort, drawing together the collective efforts of local, state, federal, and private sector responders.

As specified in the NRP, ESF15 integrates at the national level public affairs, Congressional affairs, state, territorial, local and tribal affairs coordination, community relations, international affairs, and the private sector under the coordinating auspices of external affairs.²⁷

Upon activation of ESF15 by the DHS Assistant Secretary for Public Affairs, federal external affairs personnel are employed to conduct operations during an incident of national significance or incident requiring a coordinated federal response in order to provide accurate,

26. Ibid.

27. Department of Homeland Security, Emergency Support Function 15, Standard Operating Procedures (SOP 2006), DHS, Washington D.C., May 2006.

coordinated, and timely information to affected audiences, including governments, media, the private sector and the local populace.

Standard operating procedures, or SOP, for ESF15 were developed with the benefit of first-hand experience and lessons learned from Katrina. “The catastrophic incident was the first real-world employment of ESF-15, and it identified a range of issues that required more detailed guidance,” according to Brian Besanceney, Assistant Secretary for Public Affairs, Homeland Defense Agency.²⁸

USNORTHCOM provides Defense Support to Civil Authorities within the general framework of the NRP.²⁹

During the Katrina response a message flow plan for public communications was put into place within DoD. We were keenly aware that audiences—domestic, international and adversary—were watching developments. Staying on message helped focus the media on what was important. “National messages” were distributed to the public in a timely manner. Bear in mind that the basic message could be modified to reflect each agencies roles and responsibilities at each stem.

There were bumps in the road in that DoD was very early in message distribution compared to other agencies. Lanes intersected but DoD stayed the course and did not publicly criticize other agencies. As long as each agency “stayed in its own lane,” the system worked well. The old axiom “That’s my story and I’m stickin’ to it” applied.³⁰ Leading from the rear was a challenge for DoD, but it is likely the position we will find ourselves. So, developing relationships before we exchange business cards at the scene is key for partnering for success.

USNORTHCOM’s Key Messages:

- *Saving Lives*
- *Partner with other agencies*
- *Provide the right response*
- *Continue to Defend the Homeland*

28. Ibid.

29. Ibid.

30. Don Miles, interview by Author, Colorado Springs, Co, 22 October 2006.

Below are examples of USNORTHCOM messages getting to the public.

“Our commitment is unequivocal,” said Assistant Secretary of Defense Paul McHale at a Washington news conference with officials from the Department of Homeland Security and other federal agencies. “We stand in a supporting role, and we are not only willing, we are eager in a time of national crisis to provide whatever relief we can.”

—Knight-Ridder Newspapers, August 31, 2005

“NORTHCOM does not provide any military relief independently, but responds to requests by FEMA, which directs the nation’s disaster relief...”

—Rocky Mountain News, Sept. 1, 2005

“Officials said disaster relief work won’t affect NORTHCOM’s military preparedness.”

—The Associated Press, August 31, 2005

Less than 2% of the reports USNORTHCOM analyzed were negative giving an idea of the reach and tenor of the reporting.³¹

A great asset to USNORTHCOM’s success is that co-located at the headquarters are approximately 60 different agency representatives including the NSA, FBI, NASA, DIA, DISA, DTRA, NRO, FAA, NIMA, USGS, USA Corps of Engineers, and Joint Theater Air Missile Defense Organization. This critical factor gives us a head start in developing that clear pathway if we are to build the relationships *now* with fellow senior level and field activity public affairs practitioners rather than during a crisis or disaster response.

Even with all the public affairs success from Katrina, DoD did have lessons learned.³²

- PA support must be near instantaneous and cannot be encumbered by RFF (Request for Forces) or IA (Individual Augmentee) process. Service and Joint Public Affairs Support Element (JPASE) augmentees fill mission gaps. Flexibility is critical.

31. Ibid.

32. Ibid.

- Flyaway communications packages for forward-deployed PAs are vital. DVIDS and satellite phone availability are a “must.”
- Message alignment between DoD and interagencies are vital. Dissemination must be synchronized. Conference calls are critical.
- PA preparation during crisis communications is dramatically reduced. PA can’t wait to media train primary spokespeople.
- Informing the commander and senior staff about PA activities and results is critical for building confidence and managing expectations.
- There is a need within DoD for trained/experienced PAs for interagency work.

Probably the biggest DoD issue to come out of the Hurricane Katrina response was a comment by the President. Because of the leadership and logistical response provided by DoD, people are now looking at how DoD might play a role in the future.

“...I do think [the bipartisan commission set up by Congress] ought to seriously consider the fact that there are – a storm, for example, of a certain category, which will require an overwhelming response by government that can only be provided by, say, the United States military through USNORTHCOM, because of its ability to muster logistical -- logistics and supplies so quickly. And that's what I want Congress to consider. And I think it's very important that Congress consider this.”

—President George W. Bush, Sept 16, 2005

Balancing the Public’s Right to Know

DoD has defined four basic audiences with specific goals for public communications:

- American Public: To enhance morale and readiness and increase public trust and support. The goals are to disseminate information concerning U.S. military power and capabilities, preparations, and results; to gain and maintain public support for military operations; and communicate resolve in a manner that increases public awareness and understanding of the Armed Forces.

- International: To communicate U.S. resolve in a manner that enhances global influence and deterrence. Modern military operations are often conducted as part of a coalition force and DoD should keep host nations informed much as they do the American public.
- Internal: To communicate with military members and their families. Military members include active-duty and retired, officer and enlisted, Guard and Reserve.
- Adversary Forces: Credible information regarding U.S. intentions and conduct can undermine adversary propaganda, potentially causing dissent within adversary ranks.³³
- Joint Publication 3-61: “Public Affairs” does preface this description with a caution: *The ubiquitous nature of today’s environment makes it difficult, if not impossible, to specifically target any one of these audiences through the mass media.*³⁴

A major flashpoint between the military and the media is over the issue of information security, OPSEC—safeguarding operational information from enemies. The media wants as much information as possible on topics and events. On the other hand information security is an essential part of the military’s responsibilities. Advance knowledge by the enemy of an attack plan could be detrimental to a soldier’s safety.

The handling of information during peacetime disaster response, though not likely to be “classified” under the rules of the National Security Classification System,³⁵ can still be a point of contention between news organizations and the military. The tendency of some military commanders is to hand the media a complete package of information well into the crisis. This approach will not work in a 24/7/365 world of instant information that demands even the smallest detail be released in a timely manner. Deliberations with news organizations prior to a disaster can help chart a course.

33. Chairman of the Joint Chiefs of Staff, Joint Publication 3-61 Public Affairs, Pentagon, Washington D.C., May 9, 2005.

34. Ibid.

35. Frank Aukofer and William Lawrence, *America’s Team The Odd Couple*, The Freedom Forum First Amendment Center, 1995: 23.

The military has a long history of assisting civil authorities. We are very sensitive at USNORTHCOM about protecting civil liberties of our citizens. USNORTHCOM can accomplish its mission within the framework of existing laws.

Conducting exercises or table tops to work through the “gaps and seams” of likely security, safety and privacy issues is a prudent measure before a crisis occurs.

Keep Your People Informed

Often lost in an organization’s response is keeping employees informed. With the relentless pressure to respond to the media and other agency officials our own people can be forgotten. Internal communications must be a priority.

Many of the public communications tools can be “force multiplied.” For example, press updates, fact sheets, responses to queries can be posted on the organization’s intranet. Photos and videos of spokespeople and organizational activities can also be copied and disseminated via electronic means. Copies of public affairs guidance can be distributed via email and discussed at townhall meetings.

During Katrina we provided all USNORTHCOM personnel with “wallet cards” that contained key messages, facts, figures and tips for neighborhood discussions and unscheduled, random media interviews. Where possible, a crisis plan should be created and practiced by family members.

Checklist for Success

Developing excellent communication skills is absolutely essential to effective leadership. The leader must be able to share knowledge and ideas to transmit a sense of urgency and enthusiasm to others. If a leader can’t get a message across clearly and motivate others to act on it, then having a message doesn’t even matter.

—Gilbert Amelio, President and CEO of National Semiconductor³⁶

36. John C Maxwell, *The 21 Indispensable Qualities of a Leader*, p. 23, Thomas Nelson Publishers, Nashville, 1999.

There is a critical path to success when managing public communications during a disaster/crisis response. Here is my “keeper list”:

- *Early engagement.* If time permits begin public communication prior to the crisis using available public affairs tools, i.e. news releases, townhall meetings, discussions with public officials, and develop a short list of reporters to embed.
- *Develop and maintain relationships.* Established early relationships give you a voice to correct bad information/reporting. Also, it allows the flexibility to provide background information to trusted reporters that put stories in proper context. Relationships also ensure journalists have the complete picture of the operation and not just a “soda-straw” view based on one observation or experience.
- *Have a plan – synchronize messages within the organization, at all levels and throughout the interagency.* Know what you have. Identify what you may need. Understand the process. Don’t just react to media reports, look at the entire domain of public communication channels to review and evaluate results and make improvements as required.

Be involved in the decision cycle. As a public affairs practitioner you should assume the role of the “CRO”—Corporate Reputation Officer.³⁷

- *Surge resources at the beginning.* Crisis events are most newsworthy at the beginning. It is important to have information/communications resources at all critical nodes (federal, state and local). Employ resources ensuring the right things, at the right places and at the right time. DVIDS provides another level of access for media as well as global reach at the critical time and place.³⁸
- *Provide media access.* Provide access to activities and updates to facilitate understanding rather than waiting for “wrapped packages” of information. Understand the pressure to be first with a story and the ever present deadline.
- *Transparency provides a full picture.* In other words, instead of being criticized for doing something too slow, you will be applauded for accomplishing the task as fast as you did because of the obstacles

37. David J Shea and John F Gulick, *Media Isn't a four letter word*, Aerospace Industries Association of America, Washington D.C., 2002: vii.

38. Ibid.

overcome. During Katrina, we found that embedding media with our senior leaders, while invasive, was a highly productive process. We were able to provide the in-depth background information that helped the media get the story right.

- *Monitor the media.* Make it a priority. Use digital recorders for network newscasts to ease dissemination and analysis. Hit the web hard and review print coverage. Distribute daily news clips.
- *When false information gets out, correct it immediately.* It makes the difference between a story being a blip on the radar and a full-scale crisis. The Internet provides a venue where even a false story from an obscure source has global potential. Most journalists want to get it right. The written historical record will outlive the event; corrections are important when the event is judged later.
- *Communicate with victims, first responders, and the public-at-large using every available tool for communication.* The use of a public access website can be extremely crucial. Normally, the USNORTHCOM website (www.northcom.mil) gets about 180 thousand hits, mainly from North America, over a ten day period. During Katrina it got over 1.3 million hits from around the world.
- *Choose the audience/venue carefully.* During Katrina we engaged the African American media. Avoid politically charged talk shows. Make time for the historical and internal media.
- *Be consistent.* Develop your story and tell it over and over again. Repetition ensures message receipt and ensures you stay “on message.”³⁹
- *Do the right thing for the right reasons.* It might not be in the job description but lending a helping hand can mushroom into public communications opportunities. Having compassion for the victims will go a long way to balancing an adversarial relationship with the media. According to Mike McCurry, White House Press Secretary to President Bill Clinton, “Listening carefully to the questions, understanding and being polite to critics and naysayers, and avoiding snarls at the persistent interviewer all help make a difficult job easier to handle...”⁴⁰

39. Ibid.

40. Ibid.

Summary

Crises are with us.

Local, state and Federal organizations will likely be impacted and must craft a PA strategy that is synchronized between all. This effort should include an exit strategy (getting off the front pages) and include activities that address both domestic and international audiences.

The interagency piece is critical. Having built relationships and developed a public affairs infrastructure early will go a long way in ensuring synchronization of message.

A key element that can't be overlooked is keeping our own people informed. Employees can often be the best ambassadors during a crisis.

Balancing the public's right to know with security, safety and privacy issues should be sorted out during exercises and not during the crisis.

Seize opportunities to take lessons observed and make them into lessons learned. Various public relations organizations have case studies on file that are excellent resources for handling the next crisis.⁴¹

The Instant Information Age is having a huge impact on the nation's faith in government institutions. If we don't work the public communication challenges now, we will not retain and sustain the support of the nation's citizens during future conflicts or disaster response.

41. International Association of Communicators (IABC) and Public Relations Society of America (PRSA) websites. www.Prsa.org; www.iabc.com, Internet accessed October 21, 2006.

