

VOLUME I, ISSUE 2: FALL 2006

# HOMELAND SECURITY AFFAIRS

THE JOURNAL OF THE  
NAVAL POSTGRADUATE SCHOOL CENTER FOR HOMELAND DEFENSE AND SECURITY

## Notes from the Editor

**Potholes and Detours in the Road to Critical Infrastructure Protection Policy**  
- Ted Lewis and Rudy Darken

**Homeland Security Capabilities-Based Planning: Lessons from the Defense Community**  
- Sharon L. Caudle



**Maritime Critical Infrastructure Protection: Multi-Agency Command and Control in an Asymmetric Environment**  
- Robert B. Watts

## FEATURED THEME: HURRICANE KATRINA

---

**Using Organizations: The Case of FEMA**  
- Charles Perrow

**Changing Homeland Security: An Opportunity for Competence**  
- Christopher Bellavita

**Unified Command and the State-Federal Response to Hurricane Katrina in Mississippi**  
- William L. Carwile III

**Hurricane Katrina as a Predictable Surprise**  
- Larry Irons

# *Homeland Security Affairs*

---

*Volume I, Issue 2*

2005  
2005

*Article 1*

---

## Potholes and Detours in the Road to Critical Infrastructure Protection Policy

Ted G. Lewis\*

Rudy Darken†

\*Naval Postgraduate School, tlewis@nps.edu

†Naval Postgraduate School, darken@nps.edu

Copyright ©2005 by the authors. *Homeland Security Affairs* is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of *Homeland Security Affairs* or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in *Homeland Security Affairs* rests with the author(s) of the article. *Homeland Security Affairs* is the online journal of the Center for Homeland Defense and Security (CHDS). <http://www.hsaj.org/hsa>

# Potholes and Detours in the Road to Critical Infrastructure Protection Policy

Ted G. Lewis Ph.D. and Rudy Darken D.Sc.

## Abstract

The national strategy for the protection of critical infrastructure and key assets is not working due to a number of failed strategies, which this article examines in detail: federalism (separation of state and federal governmental controls) advocates that the first line of defense is local first responders; two years after the creation of the Department of Homeland security, and the consequent requirement that states perform vulnerability and risk analysis on their critical infrastructures, DHS has yet to define basic terminology needed for states to perform meaningful analysis (“vulnerability” “risk”), or precisely state the objectives of such analysis; private ownership of the majority of infrastructure assets has been used as an excuse to do nothing – a major myth that is not only wasteful of effort, but dangerous to the security of the nation; and finally, the notion that critical infrastructure sectors are so large and complex that only the highest-consequence, lowest-probability events can be prevented has led to further missteps in the road to critical infrastructure protection policy. This article ends with recommendations for policy changes that address these issues.

**AUTHOR BIOGRAPHY:** Ted G. Lewis, Ph.D. is Professor of Computer Science at the Naval Postgraduate School and Academic Associate of the Homeland Defense and Security Master Degree program. He has 40 years of experience in academic, industrial, and advisory capacities ranging from an academic career since 1971 at the University of Missouri-Rolla, University of Louisiana, and Oregon State University, to Senior Vice President of Eastman Kodak Company, CEO and President of DaimlerChrysler Research and Technology, North America. Lewis has published over 30 books and 100 research papers, and is the author of the forthcoming book, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*, to be published by John Wiley & Sons, 2006.

Rudy Darken is an Associate Professor of Computer Science and the Director of the Modeling, Virtual Environments, and Simulation (MOVES) Institute at the Naval Postgraduate School in Monterey, California. Darken also directs modeling and simulation efforts for the Center for Homeland Defense and Security and serves as a Senior Editor of PRESENCE Journal, the MIT Press journal of teleoperators and virtual environments. He holds Master and Doctorate degrees in Computer Science from George Washington University.

**KEYWORDS:** Critical Infrastructure Protection, risk analysis, public-private partnership, critical infrastructure policy

## INTRODUCTION

One can frame the policies of the current national strategy for critical infrastructure protection using a number of colorful analogs, but transportation seems the most fitting because transportation is one of the sectors identified by the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, published by the White House in 2003.<sup>1</sup> Beneath the title of this article is the reality that we have a long way to go to protect critical infrastructure assets – across all sectors – at even modest levels of security. Indeed, if a 1,000-mile journey begins with a single step along a well-defined road, then the national strategy road is badly in need of repairs.

This paper exposes only a handful of the many myths, fallacies, and roadblocks preventing the nation from protecting its second-most important assets: the water, power, energy, telecommunications, information, and transportation systems that make up critical infrastructure (CI).<sup>2</sup> We claim that the first step in this 1,000-mile journey is to fix the potholes and eliminate the detours promoted by the current strategy for protection of the country's CI. To do so, we must understand how the national strategy fails to address reality. We couch these realities in metaphorical terms – as potholes and detours on the road to protecting the nation's critical infrastructures. The term “pothole” is used to identify problems and barriers to making progress, and the term “detour” is used to expose wrong-headed myths, distractions, and bumps in the road to better infrastructure security.

This paper argues against a purely federalist approach to critical infrastructure protection and instead advocates that the federal government take greater responsibility (and control) over state and local decisions; it argues that the first step in this transformation is to set standards, beginning with concise and clear definitions of vulnerability and risk. We then turn to the arguments preventing action – specifically that government is helpless to correct security problems in critical infrastructure because most infrastructures are owned and operated by the private sector. Finally, we make four concrete recommendations on how to improve critical infrastructure protection through re-thinking and re-aligning current policies.

### **Think Globally, Act Locally**

The national strategy is based on the idea that the federal government should set goals and policies, while the states should assume primary responsibility for homeland security, because incidents happen at the local level. Specifically, the National Strategy defines the relationship between federal and state/local governments as follows:

In addition to securing federally owned and operated infrastructures and assets, the role of the federal lead departments and agencies is to assist state and local governments and private-sector partners in their efforts to:

- Organize and conduct protection and continuity of government and operations planning, and elevate awareness and understanding of threats and vulnerabilities to their critical facilities, systems, and functions;
- Identify and promote effective sector-specific protection practices and methodologies; and

- Expand voluntary security-related information sharing among private entities within the sector, as well as between government and private entities.<sup>3</sup>

Basically, the federal government is primed to assist state and local governments, but the state/local governments are responsible for implementation of “protection practices, and methodologies.” This strategy has a number of deficiencies as pointed out by the first pothole.

**Pothole 1:** CIP (Critical Infrastructure Protection) is a local problem and therefore the federal government should provide guidance and funding, but state and local jurisdictions must become the first line of defense against attacks on critical infrastructure assets.

This policy is not only dangerous – because local jurisdictions will never have the capability to protect their critical infrastructure assets – but an unfortunate waste of money. In fact, the Government Accounting Office recognized this problem soon after the Department of Homeland Security (DHS) was formed: “The challenges posed in strengthening homeland security exceed the capacity and authority of any one level of government.”<sup>4</sup>

Consider the case of the Alaskan telecommunications sector. Alaska’s telecommunication infrastructure supports local police, fire, and emergency management functions as well as consumer telephone and Internet access. Without it, Alaskans would be isolated from the rest of the United States. Naturally, it makes sense for the Federal government – through the Department of Homeland Security – to provide funding and training to Alaskans so they can strengthen their telecommunications infrastructure and harden it against potential terrorist attacks. However, this strategy is inadequate and dangerous, because Alaska’s telephone and most Internet services are dependent on a single building in Seattle! The Weston building in Seattle is the sixth largest telecom hotel in the nation, and it provides connectivity to the citizens of Alaska. Alaskan’s cannot protect this major asset no matter how much money the Federal Government provides, because it lies outside of their jurisdiction.

In addition to the problem of an asset in one state being critical to another state, there is the overarching problem of Interstate Commerce laws that regulate and shape infrastructures such as telecommunications, energy, power, and transportation. States have little power over the Federal regulators when it comes to passing laws that might affect an element of one of these infrastructures and weaken the same infrastructure at the national level. Examples of this can be found in cross-sector interdependencies. For example, the largest electrical power plant in Missouri (New Madrid) is totally dependent on the rail system that delivers coal from Wyoming. Rail transportation and electrical power sectors are regulated by federal agencies – not Wyoming and Missouri – and yet, a policy that may ensure reliable electric power generation in Missouri could conflict with energy policies affecting Wyoming. For example, should Interstate Commerce regulation of Wyoming rail shipments of coal be implemented to raise money to harden the rail transportation system across the USA, the rate payers in Missouri (and other states) would be negatively impacted. There is nothing that the state and local governments can do to offset federal regulation of infrastructure industries.

What should be done to circumvent this pothole? The current strategy is a detour headed in the wrong direction:

**Detour 1.1:** Allocation of funding for CIP needs to be decided at the state and local level, not the national level.

The problem with this detour is simply the fact that what is critical to a state may not be critical to the nation. Separate funding of State and local districts is a waste of money in most cases because the funding does not address the true need – typically because states and cities do not have the expertise to evaluate risk. Two years after receiving funding from the Department of Homeland Security, most local governments have not spent most of their allocation. It isn't that they can't spend the funds, but rather that there are many restrictions placed by the federal government on the spending of these funds and, most importantly, there is no coherent linkage of these restrictions to an infrastructure resiliency plan. Americans want to know how they are safer because of this funding. There is no answer, but there needs to be one.

Once again, we can use Alaska as an example. The largest nuclear power plant in the nation is located in Arizona, but most of the power consumed by Alaskans comes from a much smaller power plant in Beluga Bay, Alaska.<sup>5</sup> If we use size as a measure of criticality, then it makes more sense to harden the Palo Verde Power Plant in Arizona than the much smaller Beluga Power Plant in Alaska. The problem with this strategy from a national CIP perspective is that the Beluga plant is more important than the Palo Verde plant, because it supplies 60% of all Alaskan power, while the Arizona nuclear power plant supplies less than 3% of the power consumed by the Western Power Grid. If the nuclear plant shut down, it would not be missed, because the Western Grid obtains power from many sources. This is not the case with the Beluga plant. If it fails, most Alaskans will be left without power. Therefore, the Beluga plant is much more critical – to the Western Grid as well as to Alaska – than the much larger plant in Arizona. Size is not always the best measure of criticality.

**Detour 1.2:** Allocation of funding resources should be based on population, size of state, and other political factors as determined by the Department of Homeland Security.

According to Citizens Against Government Waste, “Funding ratios guarantee each state .75 percent of the funds available for homeland security. This formula initially distributes 40 percent of the funds among the states, with 60 percent for other allocations. Under this model, for example, California, a target-rich state containing 12 percent of the nation’s population, received only 7.95 percent of general grants. On the other hand, Wyoming, which received .85 percent of the funds, holds only .17 percent of the population. That means Congress provided \$5.03 per capita for California and \$37.94 per capita for Wyoming. Similarly, data from the Public Policy Institute of California revealed that Alaska received an astonishing \$58 per resident and New York got less than \$25.”<sup>6</sup>

Once again, allocation of funding based on arbitrary or political considerations will not solve the problem of enhancing security. Instead, it is wasteful and increases the probability of a successful terrorist attack. A national perspective is needed in this risk analysis process as demonstrated by both of these examples. This would reorient funding towards allocation on the basis of risk reduction – hopefully where it can reduce risk the most.

These examples illustrate why the National Strategy's pressure to push responsibility for the protection of critical infrastructures down to the local level is flawed. States and local governments are often not in control of the critical infrastructure assets they depend on. Further, local analysis of local assets results in wasted funding. Arizona is likely to be concerned for its Palo Verde Power Plant when, in fact, the Alaskan power plant at Beluga Bay is more important. But Arizona is unlikely to transfer funding from Arizona to Alaska! These are only the top-level challenges facing the nation – there are several other significant problems lurking at a deeper level.

### **A Failure to Communicate**

One of the most difficult challenges facing the field of critical infrastructure protection is the lack of shared terminology. There are too many people using too many ill-defined terms for the community of homeland security experts to communicate, properly. The lack of widely accepted definitions of terms used in homeland security leads to reinvention of the wheel, false starts, and more detours.

**Pothole 2:** There are as many definitions of “vulnerability” and “risk” as there are agencies in federal, state, and local governments, combined! Before we can take the first step in a 1,000-mile journey, we need a compass. Currently, there is no universally accepted definition of the most basic measures of criticality – *vulnerability* and *risk*.

For example, the intelligence community typically defines “risk” as  $R = T + V$  (Threat plus Vulnerability). The FBI says “risk” is  $R = I * T * V$  (probability of an incident times threat times vulnerability).<sup>7</sup> A number of other methodologies use arbitrary metrics to gauge risk. The most popular method of gauging criticality of an asset such as a port, telecommunications center, water treatment plant, or transportation terminal is to assign numbers to each asset and then add them together. In ranked ordering systems such as the U.S. Coast Guard's port security and risk assessment tool, risk is computed by summing assigned numbers to various properties such as damage, casualties, vulnerability, and threat. These numbers are provided by subject matter experts who, in turn, rely on their individual judgment when rating “vulnerability” and “risk.” The port asset with the highest total is declared the most critical.

The validity of this approach relies on subject matter experts, which does not address the problem of inconsistency across experts. This leads to uneven ranking, because every expert has a different idea of how to assign numbers. It also leads to meaningless totals, because of the different interpretations of what the numbers mean.

The intelligence community's risk equation is difficult to apply because it is not clear how one compares a low-threat, high-vulnerability asset with a high-threat, low-vulnerability asset. If we add threat and vulnerability together and get the same total, what is the difference? Clearly, a high-threat condition deserves closer scrutiny than a low-threat condition, regardless of the vulnerability, and yet  $R = T + V$  produces indistinguishable totals.

The FBI metric cannot deal with combination incidents such as the 9/11 attacks on the World Trade Center and the Pentagon. What does risk mean when the attackers target two or three assets at once? The U.S. Coast Guard metric has no equivalent in the real world, because the numbers are without units. For example, the USCG ranking does not

measure risk in dollars, casualties, or probability. Hence, it cannot be standardized, so how do we compare the results obtained by assessing two different ports?

We need a standard, scientifically exact method of assessing vulnerability and risk. Only then will we be able to define vulnerability and risk. A standard definition means that states and localities will be able to compare apples to oranges, and that the result of vulnerability analysis will mean something – across the 50 states. We can even go further: we can fund projects in a meaningful and productive manner.

**Detour 2.1:** Individual cities, states, and regions are in the best position to make their own definitions of “vulnerability” and “risk”, without the interference of the federal government.

This approach pretty much sums up the current state of affairs. While the DHS has provided general guidelines, each state is left to its own devices when it comes to defining what is critical, and how each defines “vulnerability” and “risk.” In 2003, the first year all states were required to perform a complete vulnerability analysis in order to receive federal funding for CIP, the results were meaningless, because every state used a different method, with a different outcome. It was impossible to compare the risk assigned to a bridge, say, in California, with a bridge in Wisconsin.

The definition and terminology problem can be easily solved by establishing simple, yet scientifically valid, definitions. Suppose for example, “vulnerability” is defined as the *probability that an attack will succeed* and “risk” is defined as the *expected value of the damage caused by a successful attack*. Vulnerability is a probability (a number from zero to 100%) and risk is a cost (a number that represents the impact of an attack on an asset or entire sector). Mathematically, risk is  $V * D$ , where  $V$  = vulnerability and  $D$  is typically in units of dollars, casualties, or some other loss.

These definitions are easily applied to all kinds of critical infrastructure assets and they have meaning in the real world; probability and dollars are real-world metrics. Vulnerability is equivalent to ‘likelihood’, and risk is equivalent to the real-world cost associated with an incident.<sup>8</sup>

Now we can standardize the results so that an assessment made by one expert is identical to an assessment made by another expert. We can compare apples to oranges, and then make progress towards hardening the most critical assets: the higher the risk, the higher the criticality of an asset.

Vulnerability is relative to the threat; e.g. the vulnerability of the Federal Reserve Bank in Manhattan might be 10% relative to a car bomb, and 60% relative to a cyber intrusion. This means there is a 10% likelihood that a car bomb will do enough damage to close the bank and a 60% chance that a cyber attack will halt banking business. Therefore, our definition incorporates the threat as well as the weakness of an asset to a specific threat. A bank may be vulnerable to a cyber attack, but not so vulnerable to a car bomb attack.

Vulnerability is not risk, and risk is not vulnerability. Instead, risk is the product of vulnerability times damage:  $R = V * D$ . Risk can be measured in casualties, loss of equipment, financial loss, etc. But you can’t mix metrics in one analysis. If you use dollars you can’t switch to casualties. The important distinction is that “vulnerability” is the probability of a successful attack, and “risk” is the expected value of damage due to the attack.

Suppose the estimated damage of a successful car bomb attack on the bank is ten million dollars and the cyber attack, one million. Since risk equals vulnerability times damage, the risk associated with a car bombing is one million dollars (10% of \$10 million), and the risk associated with a cyber attack is \$600 thousand (60% of \$1 million). In tabular form, we have the following:

Threat	Vulnerability	Damage	Risk
Bomb	10%	\$10 million	\$1 million
Cyber	60%	\$1 million	\$600 thousand

Notice that the bank is more vulnerable to a cyber attack (60%), but the risk of a bombing is higher (one million dollars vs. \$600,000)! Risk and vulnerability represent different measures of “criticality.” In this case, the cyber threat is “more critical” because the bank has greater vulnerability to a cyber attack, but the bomb is “more critical” because the bank has higher risk to a bombing. It is important to distinguish between vulnerability and risk, because they can produce different definitions of criticality depending on their relative size. Vulnerability is not the same as risk, which means we must decide which is more important – to minimize risk or vulnerability.

What is the most likely incident in the foregoing example? Is it more likely that the bank will suffer a bomb attack or a cyber attack? How do we decide? In most risk assessment methods there is no way to model all possible incidents or events. In this example, the most likely event is a cyber attack (54%), and the least likely incident is a car bomb attack (4%). In addition, there is a 6% probability that both attacks will occur! In other words, the assessment must consider all possibilities. Most risk assessments ignore the likelihood of multiple, simultaneous attacks. The attacks of 9/11 were multiple, simultaneous attacks overlooked by the intelligence analysts, perhaps because their methodology ignored combination events. In our simple car bomb versus cyber attack example, there are actually three threats as summarized below.

Threat	Vulnerability	Damage	Risk
Bomb	10%	\$10 million	\$1 million
Cyber	60%	\$1 million	\$600 thousand
Both	6%	\$11 million	\$1.6 million

Vulnerability and risk assessments must incorporate combination events such that they can be compared across sectors, jurisdictions, and agencies. One way to do this is to standardize the multiple-event model. For example, a rigorous and standard method used in reliability engineering is *fault tree analysis*. Unlike current techniques in use by critical infrastructure protection analysts, fault tree analysis reveals all possible combinations of events, and assigns each a likelihood and risk value. Fault tree analysis can then determine the best allocation of funds to minimize vulnerability or risk. Fault tree modeling is beyond the scope of this article, but it is an established technique, so why not adopt it?

Without a scientific definition of vulnerability and risk, there is no way to perform meaningful risk assessments. There is no way to compare the risk of losing the Palo Verde nuclear power plant with losing the Beluga power plant, and there is no way to decide how much money to spend on prevention of a car bomb attack versus prevention of a cyber attack against banks and government buildings. Existing risk assessment

techniques cannot compare apples to oranges, and when they derive a figure of merit, the numbers are meaningless because they are based on opinion, not scientific measurement.

### **The “Do-Nothing Policy”**

One of the myths circulating among policy-makers suggests that local government is helpless when it comes to CIP, because most critical infrastructure assets are owned and operated by private companies that make up the private sector. How can government protect assets they do not own? The problem with this myth is that it leads to a ‘do-nothing’ policy. This assumption that private-sector infrastructures are beyond the reach of government agencies is not only wrong, but also dangerous, because it leaves the most critical of assets unprotected.

**Pothole 3:** Private companies own and operate most critical infrastructure, hence government cannot intervene on behalf of public safety. These owners and operators must provide critical infrastructure protection – not the government. However, because prevention is costly, the owners are unlikely to spend the money needed to protect these assets on behalf of the public they serve.

For example, the Congressional Budget Office states, in an introductory comment to “Why the Private Sector Might Spend Too Little on Security,”

Businesses would be inclined to spend less on security than might be appropriate for the nation as a whole if they faced losses from an attack that would be less than the overall losses for society. A number of common circumstances can exist in private industry in which there is a gap between the private and public costs of a terrorism event.”<sup>9</sup>

This is one of the most prevalent misconceptions in critical infrastructure protection literature. It ignores the burdensome regulation that controls these industries. Most power, telecommunication, and energy companies have little control over their business because of inter-state commerce law and a long history of government regulation. The government still “runs” these sectors through extensive regulation. In nearly every case, these industries fall under inter-state commerce laws or regulation by various governmental agencies designated by the U.S. Congress as overlords. In the electrical power sector, for example, Congress exercises its control through the FERC (Federal Energy Regulatory Commission) and in the telecommunications sector, Congress exercises control through the FCC (Federal Communications Commission). In other words, most critical infrastructure is controlled by the federal government, which dictates how each sector operates.

Let us take the telecommunications sector as an illustrative example. The telecom industry was recently re-regulated by passage of the Telecommunications Act of 1996. This act reasserted detailed governmental control over this vast infrastructure. For example, telecommunications companies like AT&T, Verizon, and Nextel paid billions of dollars in license fees to the US Government for the right to “broadcast” cellular telephone signals through the air. Furthermore, state governments can set prices on telephone service, which leaves very little room for profit. The exercise of this federally and state-centered power suggests the opposite – that government does indeed exercise control over these sectors. In reality, government has the power to protect most critical

infrastructure sectors through existing regulatory agencies. For example, DOE (Department of Energy) sets standards of safety and security for all nuclear power plants; similar regulations control the safety and security of the nation's energy pipelines through the Department of Transportation's Office of Pipeline safety.

The current policy of the Department of Homeland Security appears to be "hands-off" when it comes to dictating security standards in the telecommunications industry. This does not make sense when, in fact, the telecommunications industry is already heavily regulated by federal and state governments. Because the telecommunications business is an inter-state commerce business, there is virtually nothing preventing the addition of security standards to inter-state commerce policy. Indeed, the security standards of sister industries such as the electrical power industry, are dictated by federally run agencies such as the Department of Energy, FERC, and NERC (North America Energy Reliability Council). What prevents implementation of security measures in the telecommunications industry? It is certainly not the case that the telecommunications sector is owned and operated by the private sector.

**Detour 3.1:** Critical Infrastructure Protection is too expensive to be provided by the companies that own and operate the CI, so we must increase taxes and provide financial incentives to the owners so they will harden their assets in the best interest of the country.

This myth is also widely believed by politicians and policy-makers, but once again, it defies logic and is dangerous because it distracts us from the task at hand – hardening the most critical assets in the various national infrastructure sectors. The first observation is this: most sectors bill consumers proportionally to services or products consumed. The electrical power companies bill by the kilowatt; the telecommunications industry bills by the minute; and the energy sector bills by the amount of energy consumed. In other words, these companies stop making money when services or consumables cease to flow. Continuity of operations already has its own built-in motive – the more reliable the operation, the more money received. Therefore, utility companies are motivated to increase continuity of operations. They do not need governmental incentives to reward them for doing what they do best: deliver services and consumables to the public.

The only thing more expensive than critical infrastructure protection is loss of continuity of operations. The notion that these industries will not protect the sources of their profit is a detour in the road to critical infrastructure protection. Instead of doing nothing, the national policy should be focused on solving the problem of continuity of operations and let the private sector pay for it, because they seek maximal profit. The profit motive works – it is maximized when the sector is operational 100% of the time.

And yet it cost something to harden critical infrastructure assets such as power plants, roads, and railways. Doesn't this cost reduce corporate profits? We only need to look at the immediate past to show how the profit motive works in favor of private sector investment in security. Hurricane Katrina not only damaged much of the infrastructure of New Orleans, it also forced Entergy (the regional power company) to the brink of bankruptcy. Entergy lost revenues because its electrical power distribution lines and gas-powered generators were flooded. The cost of stronger levees would have been much less than the loss of the company. But of course, Entergy has no control over levees – the Army Corps of Engineers does!

## The Big Bang Strategy

From the very outset, the strategy of the Department of Homeland Security has been to prepare the nation to respond to high-consequence (high damage), low-probability (low vulnerability) events. One of the early critics of the federal government's strategy identified three weaknesses:

1. Domestic preparedness is focused on *highest consequence, least-likely* attack, i.e., low-probability, high consequence WMD (Weapons of Mass Destruction) terrorism,
2. It is geared toward *consequences of chemical/biological WMD* attack, because WMD are becoming *more accessible to terrorists*,
3. It is geared toward federal investments at *the state and local level* due to Federalism and the belief that *attacks will be local*, not national; the *US is too large* to maintain a national operational capability at the local level; Federalism gives *states extensive rights and responsibilities*; and the *division of labor* across local, state, federal jurisdictions was compatible with the *Stafford Act*.<sup>10</sup>

The problem with this strategy is that state and local governments are woefully unprepared to meet such emergencies. Furthermore, they are unlikely ever to be capable of responding to big bangs such as a dirty bomb, pandemic, or mass transit emergency. The Hurricane Katrina disaster is the latest illustration of local governments being overwhelmed by a high-consequence, low-probability event.

**Pothole 4:** Critical Infrastructure assets are so vast and geographically dispersed that we can only protect against the highest-consequence, lowest-probability events.

Closer examination of this pothole shows how impractical it is. Consider the case of a smallpox attack launched in a major metropolitan area.<sup>11</sup> Suppose the eight million inhabitants of Manhattan are exposed to smallpox via a scenario similar to the anthrax contamination perpetrated through the U.S. mail in 2002.<sup>12</sup> Smallpox has a three day incubation period, which means vaccination is effective if given within three days of contraction of the virus. Vaccination is a non-trivial medical procedure that requires a trained person to carefully administer fifteen pinpricks to medically screened recipients. Working twenty-four hours per day, it is estimated that 4,000 health care workers would be needed to vaccinate one million people in a timely fashion. In other words, 32,000 workers would be needed to vaccinate all eight million people living and working in Manhattan!

Logistically, this is an impossible situation. The entire state of New York does not have 32,000 health care workers ready to vaccinate eight million people within three days. Where might these 32,000 workers come from? The NYPD (New York Police Department) employees 34,000 workers, so why not turn this problem over to law enforcement? This leads to another detour.

**Detour 4.1:** Terrorism is a criminal activity and hence its prevention should be left to local law enforcement, fire fighters, and emergency management services.

If terrorism is a criminal activity, then all our problems are solved! There are more than four million law enforcement, public safety, and medical emergency personnel in the

U.S., which makes the combined “EMS community” larger than the sum total of armed forces under the command of the Department of Defense. The problem is, they are dispersed throughout the country and lack the training, equipment, and intelligence information to leverage the entire community of four million “first preventers.” They would need to be coordinated at the national level in order to prepare them to respond to a high-consequence, low-probability event. If the strategy is to be prepared for the high-consequence, low-probability event, then preparations must be national, not local. National readiness requires national organization and coordination. The lessons of Hurricane Katrina remind us that state and local preparedness is insufficient when major events occur.

## RECOMMENDATIONS

Historically, most critical infrastructure failures have been caused by natural disasters, not terrorists, so why so much emphasis on the war on terrorism? Is terrorism, and critical infrastructure protection in particular, overrated? The answer must be ‘no’, because of 9/11. Prior to 9/11 the U.S. considered the homeland safe; non-governmental organizations lacked the capacity to reach across the barriers provided by the Atlantic and Pacific oceans. The asymmetric attacks of 9/11 changed our thinking from elimination of the improbable to careful consideration of unlikely high-consequence events. Second, the 9/11 attacks were – among other things – attacks on critical infrastructure. Manhattan, and the twin towers in particular, are the center of banking and finance for the entire country.

If we are to seriously consider critical infrastructure protection as one of the pillars of homeland security, then several policy adjustments will be required. As a start, the Department of Homeland Security must:

1. Establish itself as a security standards setter and enforcer and act quickly to define basic terminology such as ‘vulnerability’ and ‘risk’. In addition, these definitions must be applied uniformly across the nation so that true risk assessment can become a practical means of evaluation and allocation of funds.
2. The national strategy must leverage national assets to the advantage of high-risk areas of the country rather than distribute responsibility to state and local governments. The U.S. already does this in a number of other areas: the FBI is essentially a national police force; the Department of Interior’s forest fire fighters are essentially national fire departments; and the National Guard is essentially an interior army. While all of these must remain under civilian control, there is little reason to hold back; use these national resources to protect national assets.
3. The interface between government and private sector companies has long been established by inter-state commerce laws, regulatory agencies, and the utilities that own and operate most critical infrastructure sectors. There is no reason to do nothing. Legislation needs to be enacted to guarantee “target hardening” of the nation’s most critical infrastructure assets.
4. Terrorism is not only a criminal activity – it is a military assault on the entire population. Hence, we must disavow the notion that local law enforcement agencies are capable of preventing acts of violence against critical infrastructure assets. An attack on the Weston building telecom hotel located in Seattle is not a criminal

activity against Seattle, but a military action against the entire country. It must be dealt with as such.

It is time to re-evaluate the national strategy and replace state and local strategies with a national effort. This has been done within the Department of Interior and Forest Service: large forest fires are fought across regional boundaries, largely by a federal force. It has been done to some extent within the food and agriculture sector: FDA regulators work with the private sector to ensure the safety of the food supply. And whether or not we admit it, the FBI is a national police force that transcends state and local borders.

---

<sup>1</sup> *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Feb. 2003, Department of Homeland Security. <http://www.whitehouse.gov/pcipb/physical.html>

<sup>2</sup> The most important asset is people – our citizens rank the highest in priority.

<sup>3</sup> *The National Strategy*.

<sup>4</sup> “Homeland Security: Reforming Federal Grants to Better Meet Outstanding Needs,” GAO-03-1146T, September 03, 2003.

<sup>5</sup> Arizona’s lone nuclear power plant, Palo Verde, ranks second on the Energy Information Administration’s (EIA) [list](#) of 100 largest electric plants. It is the largest nuclear power plant in the United States. [www.eia.doe.gov](http://www.eia.doe.gov).

<sup>6</sup> Coulton, Andrew, “DHS Funding Reform Unfinished,” December 20, 2004, [www.cagw.org](http://www.cagw.org)

<sup>7</sup> Dean, W., “Risk Assessments and Future Challenges,” *FBI Law Enforcement Bulletin*, July 2005.

<sup>8</sup> Lewis, T.G., “Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation” (Wiley: 2006)

<sup>9</sup> Congressional Budget Office, “Homeland Security and the Private Sector,” December 2004, Section 3 of 7. [www.cbo.gov](http://www.cbo.gov)

<sup>10</sup> Falkenrath: Problems of Preparedness, (Paper 2000-28, Belfer Center, Harvard U.) Dec 2000.

<sup>11</sup> Public Health is one of the critical infrastructure sectors defined by the national strategy.

<sup>12</sup> U.S. Postal Service, “Issues Associated with Anthrax Testing at the Wallingford Facility,” GAO-03-787T.

# *Homeland Security Affairs*

---

*Volume I, Issue 2*

2005  
2005

*Article 2*

---

## Homeland Security Capabilities-Based Planning: Lessons from the Defense Community

Sharon L. Caudle\*

\*US Government Accountability Office, [caudles@gao.gov](mailto:caudles@gao.gov)

Copyright ©2005 by the authors. *Homeland Security Affairs* is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of *Homeland Security Affairs* or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in *Homeland Security Affairs* rests with the author(s) of the article. *Homeland Security Affairs* is the online journal of the Center for Homeland Defense and Security (CHDS). <http://www.hsaj.org/hsa>

# Homeland Security Capabilities-Based Planning: Lessons from the Defense Community\*

Sharon L. Caudle

## Abstract

Beginning in 2004, the Department of Homeland Security (DHS) began to define and implement a national domestic all-hazards preparedness goal, intended to improve the nation's preparedness for national catastrophes, including terrorist attacks. DHS's approach was capabilities-based planning (CBP), adopted from the Department of Defense (DoD). This article illustrates several components important for CBP implementation to contrast with DHS's approach. These components range from setting out the business case for CBP adoption to necessary organizational and cultural enablers. The article concludes with CBP implementation challenges because of differences between homeland security and the defense community.

**AUTHOR BIOGRAPHY:** Dr. Sharon Caudle is an assistant director with the U.S. Government Accountability Office's (GAO) Homeland Security and Justice Team. She specializes in homeland security and national preparedness strategic policies, programs, standards, and management. She currently serves on the American National Standards Institute's Homeland Security Standards Panel steering committee and the technical committee for the national standard for disaster management, emergency management, and business continuity. She is also a senior fellow with the George Washington University's Homeland Security Policy Institute and is an adjunct faculty for the Office of Personnel Management's Development Centers and The George Washington University. She earned her Master degree and doctorate in public management from The George Washington University in Washington, DC, and recently earned a Master degree in homeland security and homeland defense from the School of International Studies, Naval Postgraduate School, in Monterey, CA.

**KEYWORDS:** capabilities-based planning, performance management

---

\*This article represents the views of the author and not those of the Government Accountability Office.

## INTRODUCTION

In 2003, President Bush's Homeland Security Presidential Directive 8 (HSPD-8) required the Department of Homeland Security (DHS) Secretary to develop a national domestic all-hazards preparedness goal. The intent was to establish measurable readiness priorities and balance threats and consequences with resources required to prevent, respond to, and recover from them. The goal would include readiness measures, standards for preparedness assessments and strategies, and a system to assess the nation's overall preparedness to respond to major events, especially terrorist acts.

Paying attention to the goal and related readiness priorities, particularly at the state and local levels, is vital, for at least one simple reason—federal funding. Under the directive, state all-hazard preparedness strategies consistent with the national preparedness goal will determine federal preparedness assistance.<sup>1</sup> This direction was affirmed when Congress subsequently cited HSPD-8 for preparedness requirements and funding in the fiscal year 2005 DHS appropriations' language. The National Intelligence Reform Act of 2004 also required DHS to set national performance standards and ensure state homeland security plans' conformance with those standards.

Responding to the HSPD-8 mandates, DHS adopted a capabilities-based planning approach (CBP) from the United States Department of Defense (DoD). This article describes the approach, implementation practices from the DoD experience, and contrasts with the DHS strategies.

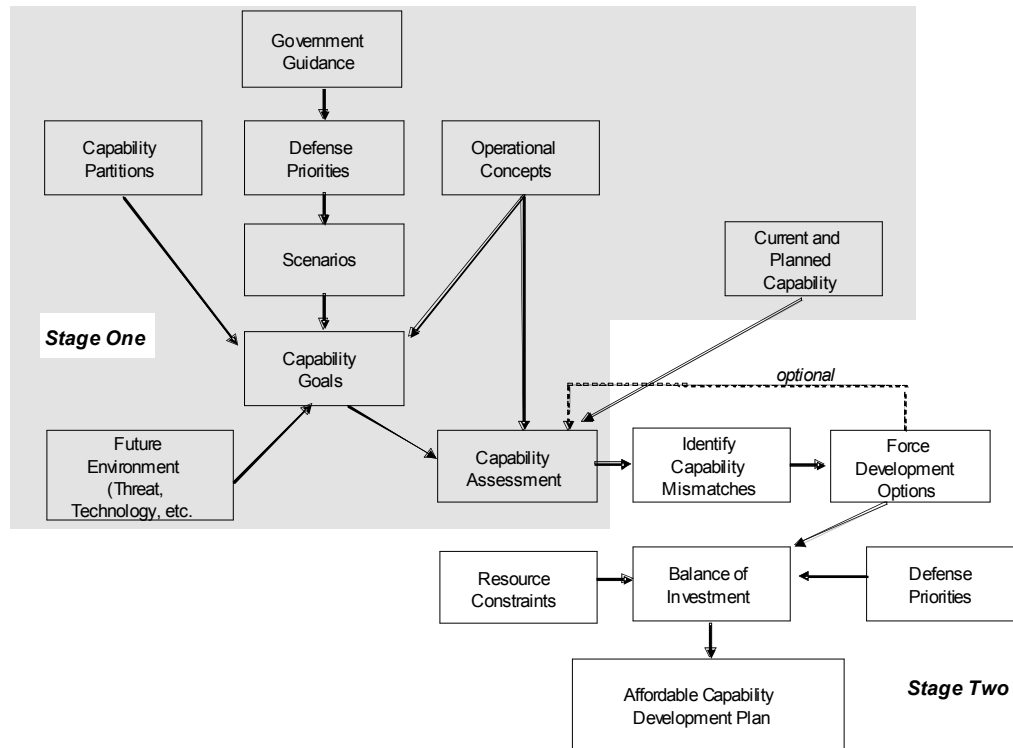
## CBP MODEL FOR HSPD 8 IMPLEMENTATION

Capabilities-based planning is one approach that is intended to manage risk, set specific preparedness goals and priorities, make investment choices, and evaluate preparedness results. Proponents describe CPB as developing the means—capabilities—to respond to a wide range of potential challenges and circumstances while mindful of costs and sustainability. CBP uses intelligence, strategic studies, and experiences to describe potential future threats and specific event or longer-term scenarios. The scenarios are used to define specific capabilities through an analytical framework starting with mission objectives and measures of strategic and operational success and ending with an assessment of options on factors such as risk. Choices consider capability tradeoffs and impacts at multiple levels within and across organizational components.<sup>2</sup>

All member nations of the defense community's Technical Cooperation Program (TCP)—Australia, Canada, New Zealand, United Kingdom, and United States—use capability concepts for long-term future defense force structure planning. The central audience for the defense community's CBP is the “combatant commander” who must achieve specific missions. The TCP's generic CBP process chart, shown in Figure 1,

starts with overarching guidance, identifies capability gaps, explores options, and ends with an affordable investment plan.<sup>3</sup>

Figure 1. Generic CBP Process Chart



## DEFENSE CBP COMPONENTS AND DHS IMPLEMENTATION

My review of the defense community's CBP experience represented by the TCP highlights several components important for CBP implementation to contrast with DHS's approach and provide "lessons learned" useful for future CBP implementation.<sup>4</sup> In the following sections, I describe these components and briefly contrast them with DHS's efforts to date. Table 1 highlights the defense components and DHS efforts.

Table 1. DHS Approach and the Defense Components

Components	DHS Progress
Business Case for CBP Adoption: <i>Justify organizational commitment and investment</i>	Business case stated in terms of national preparedness in HSPD-8 and now in legislation; clear business case still to be made for adopting CBP.
Strategic, Cascading Policy Goals: <i>Use top-level government guidance that cascades goals into strategic policy and operational documents and into CBP.</i>	Multiple sources of policy goals including national strategies, HSPD-8 and other presidential directives, the National Response Plan, and the National Incident Management System; integrated, single-source policy document for homeland security and national preparedness not yet available.
Stakeholder Ownership: <i>Ensure stakeholder involvement, collaboration, and perspective-sharing.</i>	Inconsistent attention paid to state and local entities as primary stakeholders; primarily federal approach used in consultation with, not collaboration with those entities. Private sector stakeholders yet to be closely involved.
Top Leader Ownership: <i>Ensure top leader support, involvement, and decision-making.</i>	Federal leadership within DHS appears supportive; top leadership from other stakeholders still evolving. Decision-making processes not transparent and apparently fragmented.
Specific Management Decision-Making Process: <i>Design and implement CBP decision process that captures mission tasks and capabilities, their priority, how they relate, solutions, and resource allocation.</i>	Process has evolved over time but is not formally structured with clear responsibilities, decision-making roles, and integration into stakeholders strategic planning, budgeting, program evaluation, and corrective action. Interim documents extend the process.
Risk Assessment Approach: <i>Use risk assessment in the CBP management process to determine investments.</i>	Risk assessment is not well-defined and presented as an integral part of DHS CBP decision-making similar to the defense communities.
Different Planning Horizons: <i>Incorporate different planning horizons into CBP to stage the development of capabilities.</i>	No expression of planning horizons to date; DHS has promised to evolve CBP and planning horizons may be part of the evolution.
Mission-Based, Phased Scenarios: <i>Have the right scenarios on which to base planning and/or exercises</i>	Selection of 15 scenarios for planning; concern the scenarios are much too focused on terrorism in contrast to a clearer all-hazards approach and do not include different timeframes, including very long term.
Capability Development and Standard Categories: <i>Provide guidelines to craft capabilities and develop standard capability categories that fully reflect what effects the capabilities should generate.</i>	Limited guidance on how to develop capabilities; capability categories still in process; no clear direction provided as to what is the best way to structure the capabilities for use by most entities.
Decision Rules for Lists: <i>Establish clear rules for the development of task lists and capability lists.</i>	Rules for development not explicit; changing categories and elements.
CBP Evolution: <i>Evolve CBP depending on planning applications and developing maturity.</i>	Policy timeframes have precluded a more evolutionary approach to CBP and addressing differing maturity in capability areas.
CBP Enablers: <i>Consider organizational and cultural enablers to support CBP adoption.</i>	Enablers may be recognized but have not been adequately addressed; process characterized by rapid spiral development with extremely limited timeframes for consideration.

### **Business Case for CBP Adoption**

First, CBP adoption requires a strong business case to justify the organizational commitment and investment. In the defense communities, the business case grew primarily out of the need to shift defense planning from a “threat-based” model to a “capabilities-based” model. Instead of planning for large conventional wars in a few distant theaters under the threat-based model, the 2001 Quadrennial Defense Review proposed identifying capabilities that relied on surprise, deception, and asymmetric warfare to deter and defeat adversaries.

DoD used threat-based planning since DoD instituted the Planning, Programming, and Budgeting System in 1962. However, threat-based planning meant strong response to a few situations while largely ignoring all other potential challenges. DoD’s threat-based approach and illustrative official planning scenarios for major theater wars served as specifications, defining necessary and sufficient characteristics of the force structure, thereby leading to consistent support of current programs. The approach only considered conventional-wisdom threats and point-in-time versions of detailed scenarios, as though the circumstances of future conflict could be predicted. In the foreword to the Joint Operations Concepts, Secretary Rumsfeld said a capabilities-based approach would focus more on how the United States would defeat an adversary’s broad array of capabilities instead of identifying who the adversaries were and where they might threaten joint forces or United States’ interest.

While addressing the limitations of threat-based planning was the primary business case for DoD’s adoption of CBP, there were other reasons too. CBP attempts to break down traditional single-service stovepipes allowing systems and concepts from multiple services to achieve capabilities. A joint focus encourages decisions with broad defense force goals in mind instead of considering their own service. CBP also compares options for achieving the same capability in an integrated fashion. Before CBP, acquisition requirements often were developed, validated, and approved as stand-alone solutions to counter specific threats or scenarios with systems integration forced at the end. The result was duplication, poor spiral acquisition practices, and problems in prioritizing joint warfighting needs. CBP links procurement decisions to strategic goals and provides an audit trail for accountability.

Thus, the defense community experience suggests the adoption of CBP requires a strong business case to justify the organizational commitment and investment, such as flexibility in addressing current and future adversaries and their strategies. For homeland security, DHS officials assumed there would be overwhelming state and local support of a national preparedness goal simply because it was mandated in HSPD-8. Beyond this almost “motherhood and apple pie” argument, very little attention was paid to significant benefits that might result, such as clearly defined levels of preparedness understandable across many organizations and useful for funding decisions. In addition, a clear business case was not made in support of an all-hazards approach under the national goal. The goal’s implementation clearly stressed counter-terrorism, with all-hazards a secondary emphasis.

### **Strategic, Cascading Policy Goals**

A second component is establishing specific strategic policy goals from top-level government guidance to derive high-level capability objectives. These policy goals support the use of top-level doctrine or some overarching operational concepts that consider the way a force will fight. Moreover, these goals cascade into strategic policy and operational documents, and then into the CBP process and its planning outputs. For example, the foundation for Canada's CBP was an early White Paper that defined governmental expectations, leading to a Strategy 2020 document that articulated the national defense vision. In turn, the Canadian Forces concept of force employment was crafted to describe how the national defense vision would be delivered. Force planning scenarios illustrated where and when the concept of employment would be applied, finally leading to Canada's capability goals matrix and Canada Joint Task List (CJTL) for CBP. In the United Kingdom, a defense white paper also set out the need to defend against future principal security challenges such as international terrorism, weapons of mass destruction (WMD) proliferation, and weak and failing states. The Australia Department of Defence also relied on a white paper on the future of Australia's defense force.

A similar process occurred in DoD in planning for joint processes and in individual services. DoD built its strategic framework to defend the nation and secure a viable peace around four defense policy goals—assuring allies and friends, dissuading future military competition, deterring threats and coercion against U.S. interests, and if deterrence failed, decisively defeating any adversary. These strategic policy goals are further defined in other documents. For example, within DoD joint force decision-making concepts – Joint Operations Concepts, Joint Operating Concepts, Joint Functional Concepts, and Joint Integrating Concepts – are translated into a capability level of detail, often using a time frame of 10 to 20 years into the future. Military judgment is applied to those concepts to validate what collection of attributes and measures are needed, and thus a standard for critical functional areas. Current programs are mapped against that standard to compare current capabilities against the standard, propose alternatives, choose a specific capability, and then move that decision into the investment strategy.

In summary, specific policy goals, derived from top-level government guidance, should cascade into strategic policy and operational documents, and then into the CBP process and its planning outputs. The National Strategy for Homeland Security provided the most central statement of homeland security intent, but was written largely in support of the formation of DHS. It was joined by other sources of national policy goals, including other national homeland security-related strategies, HSPD-8 and other presidential directives, federal agency strategic plans, regulations and policy guidance, the National Response Plan, and the National Incident Management System. In large part, these various documents are statements of federal perspectives because no clear mechanism exists to produce top-level “national” guidance that is accepted and applicable across all levels of government, non-governmental organizations, and the private sector. Unlike what appears to be the case in the defense communities, these various federally-developed national policy documents stand alone. They have not been systematically integrated into a cohesive policy whole. That may be the role envisioned for the national preparedness goal and related guidance, but its current construction will not meet that need. In some cases, there are conflicting objectives and requirements

across the policy documents. DHS could solve this problem with a single-source policy document for homeland security and national preparedness.

### **Stakeholder Ownership**

A third component is ensuring stakeholder ownership, especially important for joint planning and operations. The TCP says that one of the first requirements for successful implementation of CBP is stakeholder involvement, described in collaborative terms. Stakeholders generally control the information, resources, and authority required to support CBP, and their requirements must be considered from the outset. Key stakeholders—those responsible for identifying and deploying the capability envelopes—will eventually control the CBP process, and it is important that they have ownership of it. Each stakeholder should have an understanding of the perspectives of other stakeholders and an appreciation of different, if not competing, requirements. Defense planners should be engaged at all levels. As with other components, the decision-making process can help build in stakeholder ownership. For example, the U.S. Air Force (USAF) uses its decision process to secure “joint acceptance” of capability selections.

To summarize, the defense community experience shows that the stakeholders should own the process and take responsibility for its use and outputs. Stakeholders generally control the information, resources, and authority required to support CBP. For homeland security, DHS attempted to include stakeholders such as state and local government officials, national associations, and other federal agencies involved in homeland security. However, instead of taking a partnering, collaborative approach, DHS used consultants to develop voluminous draft material and then asked for stakeholder reaction. DHS justified consultation rather than partnership on the tight national goal implementation timeframes in HSPD-8 and its requirement for federal development in consultation with others. The end result has been “push back” from key state and local stakeholders, confusion about intent and requirements, and lack of understanding of CBP and what it is intended to do. In hindsight, of course, a better approach would have been to partner and take a less complex approach to implementation if the HSPD-8 implementation timeframes could not be changed.

### **Top Leader Ownership**

Another component is top leader support, involvement, and decision-making—ownership—for the CBP process. DoD’s Joint Integrating Concepts (Joint Concepts) are delivered with a detailed scenario, concept of operations (CONOPS), and a list of tasks with measures for a Functional Capabilities Board (Board) to perform a capabilities based assessment on each Joint Concept and perform a data call to services to match Joint Concept tasks to current, programmed, and planned systems. Each Board is a key decision-making body.

Only the high-level Joint Requirements Operation Council can charter a Board. The Boards ensure new capabilities are conceived and developed in a joint warfighting context and proposals are consistent with an integrated joint force. They also organize, analyze, and prioritize capabilities proposals, oversee the development and updating of functional concepts, and ensure integrated architectures reflect the functional areas. Each Board assesses the Joint Concept against the baseline scenario provided by the author, and then may run it against additional Defense planning scenarios to refine the conditions

and standards for each task and aggregate capability. The CBP output is a weighted list of capability needs, gaps, and excesses.

In 2000, the USAF began developing six CONOPs to support its contribution to the joint defense strategy. All USAF operations, programming, and budget decisions in turn are designed to support the capabilities defined by the CONOPs. Six new CONOPS divisions on the USAF Air Staff in the Operations Requirements Directorate were created to connect CBP around these CONOPS. Each of the USAF's six CONOPS has an assigned advocate called a Champion responsible for the capabilities the USAF has, or needs to develop. The CONOPS Champions play a key role in mitigating risk throughout CONOPS development. They are charged with overseeing the entire development process and for communicating issues to senior leadership. CONOPS assessment and analysis is conducted by subject matter experts under the critical jurisdiction of each Champion. CONOPS Champions will integrate priorities among capabilities for review by the USAF corporate structure and participate in the Joint Requirements Oversight Council via USAF challenges. Oversight action and challenges ensure all CONOPS capabilities are addressed at the Boards to help ensure all programs are jointly accepted.

Therefore, the defense community experience demonstrates that top leadership support, involvement, and decision-making are critical to CBP success. For defense, support has truly started at the top of cabinet departments and ministries and been sustained. Top military and civilian officials are responsible for CBP and are held accountable for its operation. In contrast, DHS never established similar top leadership authorities and decision-making processes for CBP. This could be corrected by establishing a formal board, similar to the DoD Functional Capabilities Board for top CBP leadership. Such a board would include federal, state, and local representation with national state and local associations tasked to name representatives.

### **Specific Management Decision-Making Process**

A fifth component is a well-designed and implemented decision process for CBP. This process should capture tasks and capabilities needed to carry out missions and their priority, how they relate, solutions to meet those needs, and allocation of resources. For example, the Joint Capabilities Integration and Development System (JCIDS), the Defense Acquisition System, and the Planning, Programming, Budgeting, and Execution process form DoD's three principle decision support processes to transform the military forces to support the National Military Strategy and the Defense Strategy. The JCIDS provides an enhanced methodology to identify and describe gaps and redundancies in capabilities, prioritize capability proposals, and improve collaboration with other departments and agencies. The goal is to ensure that the joint force has the capabilities necessary to perform across the range of military operations.

JCIDS analysis begins with a Functional Area Analysis that identifies the operational tasks, conditions, and standards needed to achieve military objectives. As input, it uses the national strategies, Joint Operating Concepts, Joint Functional Concepts, Joint Integrating Concepts, Integrated Architectures, the Universal Joint Task List, and the anticipated range of broad capabilities that adversaries might employ. Output consists of the tasks to be reviewed in the follow-on Functional Needs Analysis that assesses the ability of the current and programmed joint capabilities to accomplish the tasks that the functional area analysis identified, under the full range of operating conditions and in

compliance with designated standards. The needs analysis produces a list of capability gaps or shortcomings that require solutions and indicates the time frame in which those solutions are needed. A Functional Solution Analysis follows, which is an operationally-based assessment of potential approaches to solving (or mitigating) one or more of the capability gaps (needs) identified in the Functional Needs Analysis.

A capabilities review and risk assessment (CRRA) step following a functional needs analysis is the most important step for the Air Force. In the CRRA, capability measures are developed from a variety of analysis tools such as current intelligence estimates, modeling and simulation, and wargaming. Measures of effectiveness are assigned to all levels of required capabilities within a master capabilities list to score how well the USAF performs. Scenarios are selected to assess the USAF's ability to deliver effects needed. Scenarios from the Defense planning scenarios are used and further refined by guidelines in the National Security Strategy and the National Military Strategy. The scenarios also are modified by more demanding requirements known as stressors to craft broad spectrum capabilities. Analysis determines a definition of problems and capability shortfalls, presented to USAF senior leadership for decision-making and resource allocation.

Thus, the defense community experience indicates a well-designed and implemented decision process for CBP is an element for success. This process should capture tasks and capabilities needed to carry out missions and their priority, how they relate, and solutions for meeting those needs. Homeland security, however, does not yet have a process similar, for example, to DoD's Joint Capabilities Integration and Development System. The homeland security CBP process at this point is not formally structured with clear responsibilities, decision-making roles, defined steps and expected inputs and outputs, and melding into formal organizational planning, budgeting, and procurement decisions. It is not clear how CBP will be seamlessly integrated with existing management approaches for government agencies, non-governmental organizations, and private sector companies. The linkage from results expectations to budgeting is particularly problematic for funders such as boards of directors, city councils, state legislatures, and Congress must accept and act on CBP's analytical framework and its products for decision-making.

### **Risk Assessment Approach**

A sixth component is using risk assessment in the CBP management process. A key tenet of CBP is addressing affordability and sustainability, which means that not all capabilities can be deployed or maintained. Affordability and sustainability requires addressing risk tolerances and priorities for capability development and deployment, and assessing capabilities and their impacts over time. Balancing investments in CBP will require deletions and additions in elements such as force development as part of risk and priority setting.

For example, the DoD developed a broad approach to risk management intended to ensure the defense establishment is sized, shaped, postured, committed, and managed to accomplish defense policy goals. Managing risk means changes in operating practices and military and civilian personnel systems, business practices, and infrastructure. These dimensions reflect DoD's experiences over the last decade in attempting to balance strategy, force structure, and resources. The risk management framework gives DoD the

ability to consider capability tradeoffs among fundamental objectives and fundamental resources constraints.

The framework is made of four related dimensions: force management, operational, future challenges, and institutional. Force management is the ability to recruit, retain, train, and equip sufficient numbers of quality personnel and sustain the readiness of the force while accomplishing operational tasks. Operational is the ability to achieve military objectives in a near-term conflict or other contingency, with risk management considering not just additional force structure, but also assessing changes in capabilities, concepts of operations, and organizational designs to help reduce risk. A future challenge is the ability to invest in new capabilities and develop new operational concepts needed to dissuade or defeat mid- to long-term military challenges. The last dimension is institutional, the ability to develop management practices and controls that use resources efficiently and promote the effective operation of the defense establishment.

Periodic assessment of existing and planned capabilities is part of ongoing risk assessment. The TCP notes some nations that are practicing CBP will assess capabilities three or four times over an approximate fifteen year period. For example, the Canada Department of National Defence uses a capability goals matrix to rank capabilities. There are four levels in the Canadian matrix—military strategic, operational, and tactical, with the operational level divided to identify goals in the domestic and international context. The capability areas are rated as to importance (high, medium, and low) to the Department of National Defence and the Canadian Forces to achieve their overarching defense mission. To reach high capability, the Department of National Defence and the Canadian Forces must be capable of exerting effective, unilateral defense ability in the majority of the applicable Canadian Joint Task List sub-tasks associated with that capability area. The capability must be high and unilateral because it cannot be delegated to another nation or because experience and strategic circumstances dictate that high is the minimum acceptable level for overall success and risk management.

Medium level capability goals, less easily defined, are those where an effective capability in most of the applicable sub-tasks is considered important and may also result from a conscious decision to assume some risk in that capability area. For example, the Canadian Forces need to conduct joint and combined operations effectively and possess interoperability with major allies. Canada's risk assessment considers joint and combined operations as separate concepts. "Jointness" is the art of combining capabilities from different military services to create an effect that is greater than the sum of the parts. However, not all military functions or capabilities need to be joint: some will be combined. Canadian units more frequently will be combined (interoperate) with the units of another nation of similar capabilities, producing a larger formation and complementary capabilities coordinated in a specific situation. Units may also need to assume a significant leadership role for medium capability goals, although this will not normally be necessary.

A low capability goal indicates a minimum level of capability, depending on a specific strategic situation or an assessment of benefits in seeking a higher capability level for an assigned defense mission compared to costs. Under a low capability goal, Canadian units must be able to take part in joint or combined operations, but not assume a leadership role.

In sum, the defense community experience points out that risk assessment is part of the CBP management process. Risk assessment addresses affordability and sustainability, and thus risk tolerances and priorities for capability development and deployment and their impacts over time. Assessment of risk is built into scenarios, capabilities review, and a consideration of benefits and costs. Measurement systems are viewed as very important. Other than scenario development and directions for states and localities to consider what is appropriate for their jurisdictions, risk assessment is not well-defined and presented as an integral part of homeland security CBP decision-making. Measures and evaluation systems are still in development. Moreover, it will be difficult to develop and implement regional approaches where core capabilities can be supported and supplemented by other jurisdictions in the region. Political considerations may encourage jurisdictions to have a complete set of core preparedness activities rather than rely on other entities. As a result, many jurisdictions will be engaged in parallel activities within their own risk decisions, and there may be little opportunity to learn from one another or share resources as part of an overarching risk management approach.

### **Different Planning Horizons**

An additional component is incorporating different planning horizons into CBP to stage the development of capabilities. The timeframes should cover a sufficient span for action and changes to take effect, and then allow an assessment of risk over time. To illustrate, the Canada Department of National Defence envisions three planning horizons, each with a different focus for CBP. Horizon One is for a maximum of five years and seeks to deliver capability in already identified ways. Horizon Two is for five to fifteen years and focuses on delivering already identified capabilities in better ways. Horizon Three is for ten to thirty years and determines if capabilities are needed in the anticipated future, in addition to exploring radically new ways of delivering capabilities. The time period is deliberately overlapping for Horizons Two and Three.

Canada describes the first horizon as the most detailed because it executes an already developed plan and shapes near term program aspects. It requires detailed programming of resources, determining if plans are unfolding as required, and developing the appropriate level of capability. The second horizon optimizes how best to do what already is generally understood and ensure that introducing a more effective way of delivering a known capability transitions seamlessly into the more detailed plans from Horizon One. The third horizon is the most challenging as it deals with introducing fundamental changes in the way a capability will be delivered and determining what developments promise to deliver the future necessary capabilities.

Similarly, DoD describes the need for a two-pronged view of implementing CBP—maintaining a military advantage in key areas while developing new areas of military advantage and denying asymmetric advantages to adversaries. Thus, it entails adapting existing military capabilities to new circumstances, while experimenting with the development of new military capabilities. More specifically, force development planning solves future capabilities by asking what top-down investment guidance is needed to address future strategic challenges. Force development decisions also consider what DoD can provide in achievable technologies and methods of the future force. In contrast, force employment decisions involve planning for today's events, such as strategic

decisions as to how best to manage and posture DoD assets to support national interests and mitigate risks.

In sum, the defense community incorporates different planning horizons into CBP to stage the development of capabilities for the near, medium, and long term. The homeland security approach at this stage does not appear to have any similar expression of planning horizons. The fifteen homeland security planning scenarios address an event in the “here and now” (bombings and bioterrorism) with an emphasis on national priorities. DHS has promised to constantly assess and change CBP and thus the needed planning horizons may yet be addressed. However, lack of attention to capabilities for varying horizons may result in implementing capabilities that may be appropriate next year, but not five years from now. The result is poor investment portfolio planning and creating capabilities that may be obsolete or require extensive updating in a short time period. The focus on national priorities may obscure or delay an emphasis on more valued planning horizons that anticipate possible future scenarios.

### **Mission-Based, Phased Scenarios**

The eighth component is having the right scenarios on which to base planning and/or exercises. Defense capability should be assessed using plausible situations encapsulated in planning scenarios. These scenarios provide the context of CBP and should cover the full spectrum of military activities. The scenarios help develop realistic capability goals and the provision of a defense force meeting government requirements at a minimum cost. In addition, as mentioned earlier, scenarios should provide a series of time frames to facilitate capability assessment through time as part of risk assessment, rather than at a single arbitrary point in the future. Scenarios also should be used in combination to assess simultaneous operations.

Scenario types can be on a spectrum, ranging from real world planning scenarios to generic scenarios. Whichever type of scenarios are used, the scenarios should reflect the type of tasks that the government may want its defense force to undertake. In addition, scenarios used for CBP should be common across the defense force and detailed enough so that re-interpretation of the scenario does not occur.

Australia uses one or more strategic scenarios to identify a capability requirement and then operational scenarios determine the operational requirements for a proposed capability. Strategic scenarios represent strategically endorsed scenarios, high-level descriptions of situations with a brief history of preceding events and their context. Each scenario typically will describe a conflict situation, an opposing force, a military setting, a theatre of operations and the events leading up to the conflict situation. They specify the international setting and the attitudes of allies, allies of the enemy and neutrals. They also detail the political aims of the Australian government and its military strategic objectives. All strategic scenarios, taken together, in principle largely define overall defense requirements.

Australia’s strategically derived operational scenarios are reference scenarios that have been extended from strategic scenarios, to provide sufficient detail for rigorous evaluation and descriptions of defense requirements for and use of capabilities. One scenario example is evicting an enemy from an overseas territory with phases representing the buildup, the establishment of sea and air dominance, lodgement, the tactical battle, and the post-battle phase. The Australian operational scenarios are more

detailed extensions of the strategic scenarios, often detailing a force structure with equipped capabilities to be applied to achieve the particular mission. Strategic and operational scenarios form a link between strategic planning, futures analysis, experimentation, capability development, force development, contingency planning and preparedness.

The United Kingdom Ministry of Defence builds in what it calls “concurrency” in its use of scenarios for force structure development. The Ministry of Defense establishes what is needed for a particular operational scenario and then maps the conclusions against a number of operations that should be conducted at any one time. For example, the United Kingdom should be able to respond to a medium scale operation at the same time as an enduring small scale operation and a one time small scale intervention operation.

The Canada Department of National Defence uses operational research tools in a scenario operational capability risk assessment model to identify how often different types of capabilities are called upon in the scenarios. While there are arguments for using a broad range of scenarios in CBP to thoroughly test force structure for a wide range of situations, the Department of National Defence argues for a small number. The Department believes that while a more comprehensive list of scenarios may theoretically add more precision to the force planning process, they may not as there are so many uncertainties.

Thus, the defense community emphasizes that defense capability should be assessed by using plausible situations in planning scenarios to cover the full spectrum of military activities. In addition, scenarios used for CBP should be common across the defense force and detailed enough so that re-interpretation of the scenario does not occur. Many state and local officials are concerned that the national planning scenarios focus too much on terrorism and, as mentioned above, the scenarios do not include different timeframes, including very long term.

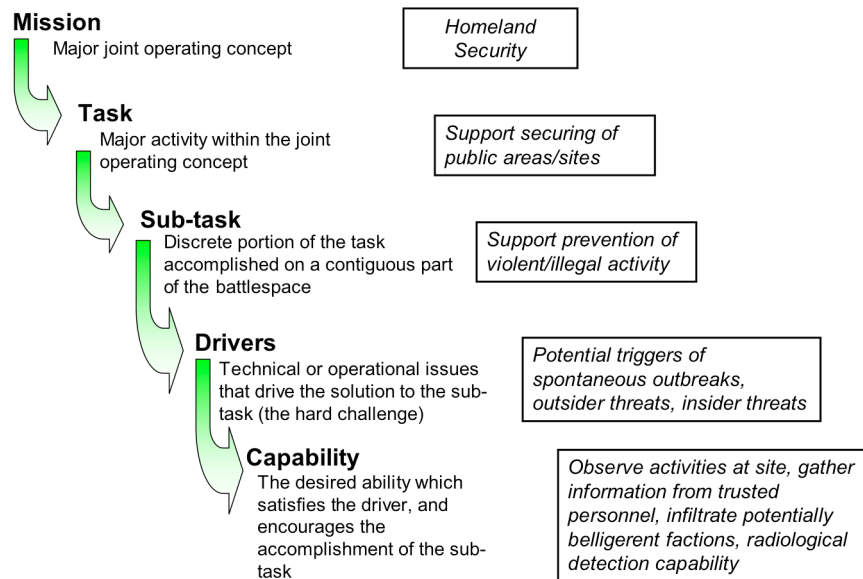
The homeland security CBP approach makes the assumption that preparing for terrorist events, representing the vast majority of the planning scenarios, will prepare jurisdictions for all-hazards events. Many would argue that it might make more sense to develop capabilities for more probable all-hazards that can be “ramped up” for large-scale terrorist events or large-scale natural or non-intentional human-caused disasters. As a result, capabilities would cover a full spectrum of homeland security activities. Capabilities then could be scaled to what is affordable and sustainable (and more likely to be used) at the state and local level, and then supplemented by regional and/or federal capabilities if an event overwhelms those capabilities. This approach anticipates that in most catastrophic situations, even a full complement of capabilities at the local or regional level will be quickly overcome.

### **Capability Development and Standard Categories**

A ninth component is providing guidelines to craft capabilities and develop standard capability categories that fully reflect what effects the capabilities should generate. For example, the DoD’s Battlespace Awareness Functional Capabilities Board provides guidelines to craft capability descriptions. The descriptions must indicate 1) what the capability is to do, such as “track” or “determine,” 2) identify a target or subject, such as a person on a battlefield, 3) the size or range of the subject, such as a large vessel, 4) the

domain of the target systems, such as air-breathing targets, 5) the area of action, and 6) the range to area, or the distance over which effects must be made or action taken. Capabilities are seen as the end of a “waterfall” of lower levels of mission used in functional area analysis, illustrated in Figure 2.

Figure 2. Battlespace Awareness Waterfall Example



Regarding categories, the TCP recommends standard groupings such as capability clusters or capability partitions to make the CBP process more manageable. There are many ways to define the boundaries between capability partitions. These partitions are based on the ability to perform tasks, or to deliver effects, such as the control and denial of underwater battle space. A key enabler for successful CBP is getting the partitions agreed to by the key stakeholders and account for synergies and dependencies across partitions. The capability partitions should not be aligned to inappropriate organizations. If they are aligned, then organizational stovepiping is encouraged.<sup>5</sup>

It is suggested at least two fundamental military capability categorization options can be used independently or in combination. One is functional or means-focused. These capabilities would include battlespace awareness, command and control, logistics, and force management. Another option is operational or ends-focused. Operational categories might include strategic deterrence, homeland defense, civil support, and land combat operations. Each category then would be further defined. To illustrate, force management would include force employment and force deployment. Homeland defense would include capabilities such as continuity of operations, securing domestic approaches and territory, and population protection.<sup>6</sup>

The defense communities have taken similar approaches to capability categorization. For example, as described by the United Kingdom Ministry of Defence, military tasks

provide a framework for detailed defense planning for the size, shape, and capabilities of the United Kingdom's Armed Forces. The military tasks reflect the broad types of tasks and operations in which the United Kingdom is likely to be involved and then provide an output-focused framework for developing force structure requirements. The eighteen military tasks are in the four areas of 1) standing strategic commitments, such as nuclear deterrent and strategic intelligence gathering, 2) standing home commitments, such as security at home in support of other government departments, 3) standing overseas commitments, such as commitments to international alliances and partners, and 4) contingent operations overseas, such as humanitarian assistance and peace support operations. Military capability is divided into six key capability elements, such as maritime, land, and logistics. The Canada Department of National Defence divides military tasks into eight capability areas, such as Command, Information and Intelligence, and Corporate Policy and Strategy.

The defense community experiences indicate that an important component is providing guidance on crafting capability descriptions and developing standard capability categories fully reflecting what effects the capabilities should generate. DHS policies and guidance do generically define a capability, but guidance is lacking as to how to craft a capability description. The homeland security capability categories should be agreed to by key stakeholders and account for interrelationships across the capability categories.

At present, there does not appear to be a clear sense and rationale as to the best way to partition the homeland security capabilities for use by most entities. The task list categories, still in draft, initially indicated capabilities will reflect primarily an indirect organizational categorization—federal, state, and local responsibilities, and then later on those for the private sector, nongovernmental organizations, and citizens. This may have created organizational stovepiping of capabilities, which the defense community cautioned against. The latest draft documents use “mission areas” for emphasis—prevention, protection, response, and recover. The IED prototype uses mission areas with critical tasks drawn from the organizational tasks lists, adding to the confusion of what categories are in play or may be the final form. The categorization across task lists and capability areas should be clarified, justified, and stabilized.

### **Decision Rules for Lists**

In another component, the defense communities establish clear rules for the development of task lists and capability lists. These rules include the source for compiling the lists, what criteria will be used in selecting candidates for the list, and how they should be arrayed. For example, the universal joint task list for DoD's CBP is the result of fourteen years of spiral development. Many sources of information from the task list to individual service sources to interagency information regarding tasks, conditions, and standards are being filtered for DoD's universal capability library. The library structure consists of a capability library—a master database of capabilities linked to current, planned, and roadmapped forces, units, and equipment—and a task library. The task library is the master database of all doctrinal and conceptual tasks.

The Australia Department of Defence has followed several principles for designing its Australian Joint Essential Tasks: joint, enduring, essential, and containing relevant and current content. Joint tasks are those that require the contribution of two or more forces working together to achieve the desired outcome. Enduring tasks capture how the

Australian Defence Force operates currently and might undertake joint operations in the future. Essential tasks capture what are required for the conduct of an operation.

In addition to the design principles, Australia Department of Defence has set two further design goals for future Joint Task development—uniqueness and hierarchical. For any given level of command, a task only appears once in the task hierarchy. No tasks should be duplicated, although some related tasks might appear in more than one place. The requirement for uniqueness is analogous to the United States' UJTL requirement that tasks be mutually exclusive, that is, that any task performed by any joint organization or service unit will fit into only one place in the task structure. Thus common tasks were abstracted out of their natural parent task and were grouped together.

In addition, the Joint Tasks, similar to other defense agencies, are intended to maintain a hierarchical structure. For a high level task, its subordinate tasks, taken together, comprehensively define all of the activities in the higher-level task. For example, the Australian Joint Tasks and Canada's joint task list have three levels of joint tasks—strategic, operational, and tactical. The tasks within each level are further disaggregated into two additional layers of sub-tasks with each layer more detailed and specific.

However, opinions differ about hierarchical and uniqueness design for the lists. Some recommend that hierarchies should not be imposed because these require preconceived notions about what criteria are more valuable or useful for segregating data. Hierarchies require frequent changes or alternate versions of lists. Mutual exclusivity also may not be required, at least at the operational level as no real force, unit, equipment, or system falls entirely within any one category.

To summarize, the defense communities establish clear rules for the development of task lists and capability lists, such as uniqueness and hierarchy. For homeland security, publicly available documents indicate a lack of explicit rules for decision-making. As part of CBP implementation, DHS could easily formulate such rules. Explicit decision rules should help the further development and revision of the detailed and lengthy lists over time. For example, a rule regarding uniqueness would ensure developers would independently assess each task and whether its description is similar to or actually part of another task.

### **CBP Evolution**

Another component is evolving CBP depending on planning applications and maturity. Each defense organization is in various stages of implementing CBP, both on a national joint and individual service level. However, each organization has tailored CBP and taken a staged approach to implementation. For example, as described by the Australia Department of Defence, allied CBP approaches are similar, but emphasize different outcomes over time:

- The United Kingdom has primarily focused on immediate operations and long term planning. The United Kingdom has used a list of essential joint tasks as an analysis tool for exercises with more recent efforts to integrate the tasks into mission analysis and operational planning.
- Canada's tasks are closely linked into force planning scenarios and future planning and are used in joint department structuring so each department uses the same criteria for operations and to translate tasks into capability. Canada uses its joint task list

for force employment and capability development and has developed eleven force planning scenarios to link their capability development and planning.

- The United States joint task list has aided in the development of planning requirements for joint exercises since 1993. The joint task list was developed specifically for training but is now linked into readiness and preparedness reporting and capability development.

CBP also will progress at a different pace in the organization, creating different levels of maturity overall. Thus, some capabilities needed for the defense community of a nation may be delayed compared to others. The Canada Department of National Defence points out that over time CBP improves commonality among defense planners by introducing a common way of describing and discussing capability elements. As the different national defense organizations in Canada adopt the common terminology, it becomes easier to link different plans providing various capability components. In the beginning, certain plans will be more mature or more vital for integrated planning. Canada's long-term plan for major equipment is the most mature in employing CBP. The development of long-term plans for personnel resources, research, concepts, information technology, and infrastructure is likely necessary before more encompassing capability planning can be done in Canada.

Thus, the defense community experience includes evolving CBP to reflect planning applications. CBP will progress at a different pace in different parts of the organization, creating different levels of maturity. For homeland security, current policy timeframes have precluded a more evolutionary approach to CBP and imposed extremely limited turnaround time for stakeholder comments on various draft products. DHS does plan on enhancing the approach, but it will be very hard to dismantle earlier structures once the homeland security grant process "institutionalizes" around capability categories and tiered requirements. A comprehensive CBP system is expected to be up and running in a timeframe of months. While adoption initially will be based on one scenario—explosive devices—for initial planning, federal funding guidance indicates that in less than two years, all scenarios will be part of state and local planning. In addition, the CBP as currently being adopted does not directly address differing maturity in capability areas that may impede overall progress in homeland security preparedness. DHS would be well-served to consider such maturity considerations in its CBP implementation decisions.

### **CBP Enablers**

The last component is additional organizational and cultural enablers for effective CBP adoption. These are other necessary and sufficient factors, which along with components already mentioned, such as stakeholder ownership, create and sustain the environment for implementation. Many practitioners and students of CBP have highlighted considerations for CBP design and deployment that cover a wide range of factors, from mindset changes to the practicalities of resourcing CBP planning and execution.

Davis and Jenkins write that CBP's complexity requires a passion for adaptiveness and substantial analysis leading to a combination of incentives, standards, and policies for CBP.<sup>7</sup> They cite the need for major studies on how to modify economic and other incentives to encourage more adaptive and recoverable systems. Feaga recommends developing new languages in risk management and effects once it is known what

capability proficiency and sufficiency levels are needed.<sup>8</sup> The Australian experience indicates attention is needed to address conflicting processes, the lack of suitable analytical tools, excessively prescriptive requirements, and the recognition of functional linkages and dependencies between related capabilities.

Similarly, DoD recommends a broad and long-term strategic perspective, a greater appreciation of the operational and strategic environmental factors, and a rigorous analysis of the capabilities needed to achieve defense policy goals. The Technical Cooperation Program lists the need for consistent cost estimates and resource provision for both the development and execution of the CBP process. Moreover, joint force personnel will require a joint and expeditionary “mindset” reflecting a greater level of deployability and versatility to avoid organizational stovepiping. Canada’s Department of National Defence identifies the challenge of developing and maintaining capabilities to conduct operations independently in domestic situations and alongside alliance and coalition partners for international obligations. Canada believes the focus must remain on combat-capable units because these units can be employed in other security activities, such as peacekeeping, while those with non-combat capabilities cannot meet combat needs.

Therefore, additional organizational and cultural enablers are needed for effective CBP adoption. The defense experience indicates many facilitative factors come into play for effective CBP, many analytical and skill-based, but others such as incentives, the rationality of processes, and a deliberative approach. For homeland security, enablers such as these may be recognized but have not been adequately addressed, perhaps because they are the difficult “softer” issues or the assumption is that they will be dealt with by stakeholders individually. In addition, the rapid spiral development process has forestalled more careful consideration of CBP and what is needed to support its successful implementation.

## **CHALLENGES IN ADOPTING THE DOD APPROACH**

While this article has highlighted many components important to CBP implementation if the DoD experience is the model, DHS will face further challenges in implementing CBP. My analysis indicates that four key factors differentiate homeland security and the national defense mission that will pose challenges for DHS adoption.

### **Mission Scope and Coverage**

A first challenge is mission related. In defense, the **mission scope** is more clearly defined for national defense, most often military action and civil support. While many rightly argue that the national defense mission has broadened considerably in recent years, for homeland security, the mission is arguably broader for prevention, vulnerability reduction, and response and recovery responsibilities. Actions are required at home and abroad, from dealings with individual citizens to negotiations with nation-states as border protection is extended overseas. Homeland security also stresses all-hazards preparedness, requiring attention to a wide range of events, from small-scale earthquakes to catastrophic terrorist events. CBP should allow Homeland Security to consider these multiple and diverse missions, the common and unique capabilities they require, and what tradeoffs in priorities and resourcing might be necessary.

In addition, the defense experiences emphasize **full mission coverage**. At present, it is not clear if the homeland security CBP approach is emphasizing prevention and deterrence. While draft DHS task lists have included prevention efforts such as intelligence development and providing strategic and threat intelligence, the task lists focus much more attention on vulnerability reduction and response and recovery. Emergency response—after an event—appears to take the lion’s share of analysis and preparation with clear emphasis on first responder roles and responsibilities.

The constrained homeland security mission scope and coverage may be the result of several factors. Gilman observed that there has been a major DHS focus on weapons of mass destruction and terrorism, and not on all hazards and events that happen all that time, such as explosions.<sup>9</sup> Prevention has been “under the radar screen” for DHS as it might be considered the purview of other agencies, such as the Department of Justice or the Central Intelligence Agency, or state and local law enforcement officials. In addition, DHS’ Office for Domestic Preparedness has had a mission of emergency management, not other aspects of homeland security, and it would be normal to see this office maximize its area of strength or understanding. Perhaps more importantly, since September 11, first responders have been front and center, their needs expounded, and the results in terms of new equipment and capabilities much more visible.

### **Organizational Perspectives**

A second challenge involves organizational perspectives. One perspective is a **federal department versus a national view**. The defense community normally contains decisions within a cabinet department and White House sphere, with input from other federal agencies and to a lesser extent, international partners. In contrast, homeland security is presented as national in scope, not a federal responsibility of primarily just one executive department or agency. A national perspective requires a much more collaborative approach, particularly in a federalist system, and a fairly clear distinction between public and private spheres.

Moreover, even within the federal homeland security establishment there is fragmentation. Federal agencies other than DHS can act autonomously, buoyed by their own sources of support and direction. Even when collaborative decisions are made, the vehicles for enforcement are very limited or unwanted. The homeland security organizations represent different disciplines and perspectives, levels of public, private, and nongovernmental organizations, and even horizontal relationships such as the involvement of different federal, state, or local cabinet agencies. Defense has a central core of military services that perform its activities that share a common culture and perspective to support and deploy the warfighter. CBP should allow Homeland Security to change its unit of analysis from organizations and requirements to capabilities and their delivery.

In addition, **chain of command and exercise of authority** are different. Defense normally has a top-down command and control structure with a highly disciplined attention to authority. The homeland security CBP approach at present does not adequately guide analysis when assets and capabilities to accomplish a mission are not under one jurisdiction, may be unknown, or may ebb and flow over time. The draft national preparedness rating scheme indicates that a group of organizations can be rated

collaboratively under a mutual aide or an assistance compact to perform prevention, response, or recovery tasks for a specific scenario.

For CBP, it is crucial that relationships are driven by strategic alliances among equal partners where all stakeholders—strategic partners—are identified, their needs clearly represented in collaborative decision-making, and incentives provided for decisions not to unravel. Capability planning is always tied to sustainability analyses and funding support favors multiple-use capabilities and multiple sources of capabilities to reduce the funding burden on any one organization. Additional work is needed to better understand how to apply the framework where there are networks of organizations that work homeland security issues or are discrete sets of organizations that handle specific homeland security functions. Contingency planning is necessary in the event individual organizations or sectors will not meet their capability obligations. This will be even more important when the CBP framework is expanded to address private sector and nongovernmental organizations who are critical players in prevention, vulnerability reduction, and response and recovery strategies and actions.

### **Resource Development and Leveraging**

A third challenge is the resources that can be brought to bear for homeland security in contrast to the defense community. To start, resource leveraging requires the **understanding of assets** that compose capabilities and in general what they can accomplish. Capabilities include a diverse selection of elements, such as plans, procedures, personnel, equipment, and activities. Defense organizations have paid considerable attention to the assets that can be combined for capabilities, where they are deployed, what their maintenance or skill condition is, and when they will become obsolete or require renewal. This is not yet the case in homeland security, where asset identification and control is dispersed to thousands of organizations who may or may not have a complete and accurate inventory. Many homeland security contingency plans draw on mutual aid or regional agreements, often without full identification of assets and how they will work together. CBP provides a mechanism for asset identification, but initially CBP will be hampered as Homeland Security officials gather and assess this information and their contribution to capability planning.

In addition, resources include **planning resources, skills, tools, and experiences**. Defense communities normally have decades, if not centuries, of planning experience for concrete events and contingencies. These communities bring to bear a wide range of tools such as wargaming, exercises, and simulations, and a small army of skilled and experienced planners devoted to such work. Exercises and actual field experience are rapidly fed back to planners. In contrast, homeland security is in the early stages of planning and is often not well-resourced with dedicated staff, particularly in smaller jurisdictions. Tools and skills are still in development in government organizations. While emergency exercises have been the norm for a number of years, a systematic collection, evaluation, and dissemination of lessons learned and better practices has only recently picked up speed. The private sector in some critical infrastructure areas and for some companies, may have the requisite resources, skills, tools, and experiences, or can draw on combined sector practices, but not all. Non-governmental organizations, with limited resources, may also have difficulty in adopting CBP. It can be expected there

will be a slower identification of current and required capabilities and under what scenarios they are effective.

A tiered CBP approach in homeland security may not adequately address the very wide variety of structures, skills, and processes for homeland security activities across the nation. For example, Gilman noted that DHS does not understand, or chooses not to understand, that there is a major difference in homeland security or emergency preparedness operations and capacities between the rural and urban areas in a state or region.<sup>10</sup> He said that many homeland security and emergency management contacts are in rural areas, and many are volunteers or handle homeland security along with many other tasks. These officials often have limited infrastructure support, such as access to good communication services. Rural areas also have more difficulty forming mutual aid compacts and, if they do, may get limited help because of geography or limited regional assets and liabilities. Rural areas may have to wait many hours for mutual aid help to arrive because of the distances involved.

### **Target Audience**

A final challenge is the differences in the target audiences for CBP. For the defense community, the clear customer for CBP outputs is the combatant commander who must carry out the defense missions and relies on mission capability packages. For homeland security, the target audience at present is broadly described by DHS as the “homeland security community,” which can cover federal, state, local, private, and nongovernmental organizations, and even to the level of the individual citizen. Thus, there is not a discrete set of homeland security “combatant commanders” under the current DHS CBP approach. This has added to the complexity and confusion surrounding CBP that will require further attention.

Federal national policy is primarily directed at state and local jurisdictions at this time, with some attention paid to limited regional compacts. It may be that CBP development over time will clarify that the combatant commander should be those state and local government officials responsible for direct prevention, vulnerability reduction, and response and recovery activities. While private sector and non-governmental officials have direct homeland security responsibilities as well, the CBP process may need to stop at the governmental level. Governmental CBP outputs can be planning inputs to these other jurisdictions for their own planning processes.

Instead of supporting the combatant commander, the capabilities-based approach might get bogged-down in a checklist mentality of responding to lists of many tasks represented by the UTL (Universal Task List) and a targeted list for critical capabilities. “Checking off” the tasks forces attention to discrete activities, and not to capabilities and homeland security results for an organization and its homeland security partners. State and local officials at the October 2004 capabilities workshop noted that the task lists and defined capabilities can easily become a standard of care to which they will become individually accountable. A defensive posture might be to manage to the lists, and not to the overall results that must be achieved within a risk assessment decision-making process. As a result, developing envelopes of capability for specific operational challenges for the combatant commander will be lost.

---

<sup>1</sup> The White House, *Homeland security presidential directive/HSPD-8* (Washington, DC: The White House, December 17, 2003).

<sup>2</sup> C. Kelley, P. Davis, B. Bennett, E. Harris, R. Hundley, E. Larson, R. Mesic, and M. Miller, *Metrics for the quadrennial defense review's operational goals* (Santa Monica, CA: RAND National Defense Research Institute, 2003); P. Davis, *Analytical architecture for capabilities-based planning, mission-system analysis, and transformation* (Santa Monica, CA: RAND, 2002).

<sup>3</sup> The Technical Cooperation Program, *TTCP technical report: Guide to capability-based planning* (2004) [http://www.mors.org/meetings/cbp/cbp\\_presentations.htm](http://www.mors.org/meetings/cbp/cbp_presentations.htm) (accessed October 19, 2004).

<sup>4</sup> The defense community sources drew on material from the Australia Department of Defence, the Canada Department of National Defence, the United Kingdom Ministry of Defence, the United States Department of Defense, The Technical Cooperation Program, and individual papers and presentations.

<sup>5</sup> B. Taylor, *Guide to capabilities-based planning*. Presentation to the Military Operations Research Capabilities-Based Planning Conference, Alexandria, VA (October 18-21, 2004).

<sup>6</sup> T. Kiefer, *Capabilities based planning framework*. Presentation to the Military Operations Research Capabilities-Based Planning Conference, Alexandria, VA (October 18-21, 2004).

<sup>7</sup> P. Davis and B. Jenkins, *Deterrence and influence in counterterrorism: a component in the war on al Qaeda* (Santa Monica, CA: RAND National Defense Research Institute, 2002).

<sup>8</sup> K. Feaga, "The USAF capabilities based CONOPS construct," Academic research paper, U.S. Army War College (2004).

<sup>9</sup> J. Gilman, "Using a performance management system for homeland security funds to demonstrate accountability and improve organizational effectiveness," Presentation to the Advanced Learning Institute's Performance Measurement for Homeland Security conference, Arlington, VA (December 1, 2004).

<sup>10</sup> Ibid.

# *Homeland Security Affairs*

---

*Volume I, Issue 2*

2005  
2005

*Article 3*

---

## Maritime Critical Infrastructure Protection: Multi-Agency Command and Control in an Asymmetric Environment

Robert B. Watts\*

\*NPS monterey, rbwatts27@hotmail.com

Copyright ©2005 by the authors. *Homeland Security Affairs* is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of *Homeland Security Affairs* or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in *Homeland Security Affairs* rests with the author(s) of the article. *Homeland Security Affairs* is the online journal of the Center for Homeland Defense and Security (CHDS). <http://www.hsaj.org/hsa>

# Maritime Critical Infrastructure Protection: Multi-Agency Command and Control in an Asymmetric Environment

Robert B. Watts

## **Abstract**

As a maritime nation, the United States is economically and strategically reliant on its ports, a fact well known to our potential enemies in the Global War on Terror. A successful attack against maritime critical infrastructure in our ports has the potential to cause major economic disruption and create mass casualties and conflagration. The United States has faced military threats in its littoral before, and lessons from the past offer value in determining how to defend ports in the modern era. But these lessons must be considered in light of the new asymmetric terrorist threat. By examining lessons from the past and considering current maritime multi-agency capabilities, a logical command and control solution can be devised to effectively fuse agency efforts in tactical defense of maritime critical infrastructure.

**AUTHOR BIOGRAPHY:** A 1985 graduate of the U.S. Coast Guard Academy, CDR Bob Watts has served six tours at sea, most recently commanding USCGC STEADFAST (WMEC 623) on homeland security duty. A qualified Surface Warfare Officer, he holds post graduate degrees from the Naval War College (CCE), Old Dominion University (History), and American Military University (International Naval Studies). He has been published numerous times in USNI PROCEEDINGS on Coast Guard-Navy strategic issues, including winning the 1998 USNI Colin Powell Joint Essay Contest. He is currently assigned as Coast Guard Liaison Officer to office of the CNO (N5), and is a student in the Naval Post Graduate School's HLS/HLD program.

Throughout its history, the United States has been a global maritime nation, dependent upon the oceans for economy, welfare, and defense. In the modern era emphasis on globalization and the world economy has increased this dependence considerably. There are some 95,000 miles of United States' coastline and 3.4 million square miles of territorial seas and exclusive economic zones in the U.S. maritime domain.<sup>1</sup> Connecting the continental United States to this zone are over 1,000 harbors and ports, 361 of which are cargo capable. Through these ports enter approximately 21,000 containers daily, representing ninety-five percent of the nation's overseas cargo, including 100 percent of U.S. petroleum imports.<sup>2</sup> In addition to commerce, there are seventy-six million recreational boaters in the United States. Six million cruise ship passengers visit U.S. ports annually. In the strategic/military sense, a substantial portion of U.S. national power relies on the sea, both in the form of traditional Navy Carrier Strike groups that deploy from ports in the continental United States and the subsequent ability to reinforce deployed forces overseas. Without unimpeded access to the sea, the ability of the United States to project national power is extremely limited.

Maritime infrastructure is crucial in maintaining this link to the sea. From naval bases to commercial ports, maritime infrastructure is well developed nationwide and is crucial to both the economic sector and military strategy. Maritime infrastructure is critical to the employment of national maritime power and as such is a logical (if not desirable) target for acts of terrorism by our enemies. A successful attack against a port could incur serious economic and military damage, present an enemy with the opportunity to inflict mass casualties, and have serious long-term detrimental effects on our national economy.

Maritime Critical Infrastructure Protection (MCIP) presents many challenges in an asymmetric environment. Previous models of maritime defense have focused on protecting ships from traditional naval attack; even when ports and supporting infrastructure have been considered targets, emphasis was on defense against a military threat. The Global War On Terror (GWOT) has created a number of heretofore unconsidered vulnerabilities in this traditional outlook. Many targets that would not be considered legitimate (economic, symbolic, etc.) in a conventional war must now be considered in strategic defensive planning. In conducting these attacks the unimpeded use of the sea is a force multiplier for an enemy dedicated to striking a wide range of potential targets. Possible threats from the sea are wide-ranging and diverse, relying on a combination of asymmetric offensive tactics while exploiting the variety of the littoral.

This asymmetric nature of GWOT requires a multi-agency approach to devise effective command and control for modern port defense. The Coast Guard and Navy have made important strides in this area by devising experimental Joint Harbor Operations Centers (JHOCs) as a component of maritime anti-terrorist force protection. The expansion of this concept into multi-agency maritime homeland security is a logical next step in the evolving problem of port security and defense. This is made evident by

examining likely terrorist threats to ports and studying the lessons of the past that apply in this environment which can be used to expand the current command and control system to meet the new threat

### **New Threat Matrix: Ports as Targets**

The GWOT threat to ports is a relatively new element in the spectrum of naval warfare. This is largely due to the evolving nature of the shipping industry and the nation's growing reliance on sea power. Historically, a nation's maritime strength has been measured by the size and capability of its merchant fleet and Navy; attacks against a nation's sea power meant the physical destruction of these ships. Ports, until quite recently, were composed of infrastructure that was relatively easy to replace or replicate, making them relatively low priority targets for an enemy dedicated to striking at maritime strength.

This has changed in the modern era of containerization and the increased size and technical nature of ships. In modern times ports have become centers of highly technical, well-integrated infrastructure designed for the rapid loading and unloading of cargo, an evolution that has become highly complex in the era of containerization. Commercially efficient, port cargo operations are also highly dependent on networked operations, making the disruption of the process far simpler for a potential attacker. Additionally, the complexity of this evolution, combined with the increasing size of seagoing merchant vessels (and warships), has greatly reduced the number of commercial ports available for use by global shipping. This has the dual effect of making major ports more important economically and strategically while simultaneously making them more attractive targets for offensive action.

The attractiveness of ports as targets for terrorists can be summarized as follows:

**A. Economic Impact:** An unprecedented amount of trade – both imports and exports – relies on shipment by sea. A successful attack on maritime infrastructure would affect this trade in far greater proportion than the actual damage. It is likely that an attack on one port would have a cascade effect on others as increased security measures are applied nationwide. The recent impact of the London bombings can be seen as illustrative of this effect; although there was no indication of additional terrorist activity, security measures were increased at transportation hubs worldwide. Increasing security alerts at a train station is one thing; closing a huge economic entity such as a port is quite another. Delay of shipping in loading and offloading cargo is one of the most costly elements of the shipping process. We must also consider the impact to the shipping industry itself. During the Persian Gulf re-flagging operations of the late 1980s, for example, analysis showed the greatest impact to the shipping of oil was not the damage to tankers inflicted by the warring Iraqis and Iranians (which was, in fact, minimal), but the increased insurance costs of operating in that area.<sup>3</sup> An attack on a U.S. port could have a similar, if not larger, effect.

**B. High visibility/High Casualties:** Ports are not isolated areas, but rather major centers of commerce, usually surrounded by large cities and economic centers. An attack on a port could be highly visible and potentially the scene of mass conflagration. As a result of urban development, most major ports are no longer confined to strictly industrial areas,

but rather have become well-developed centers of commerce and entertainment, surrounded by built up waterside areas dedicated to tourism and recreation. Many of these facilities are located next to volatile maritime infrastructure (fuel tanks, docks, etc.) that could create mass conflagration if attacked through large explosive force. Sympathetic detonation, fires, and other catastrophic effects would certainly create mass casualties.

**C. Ease of attack:** Commercial ports are not fortresses. The ocean itself presents a number of distinct advantages to a dedicated attacker, especially when employing maritime suicide terrorism or means to rapidly deliver large explosive force. Water is not only a tremendously efficient transport medium (allowing for rapid transit), but the large amount of legitimate commercial and recreational traffic in ports allows for an enemy to mask movements prior to an attack, making effective defense difficult.

Given the importance of ports to our economy and military power, the potential for creating mass casualties, and the ease by which an enemy can attack, a strong case can be made that ports will become a target for future terrorist attacks. If this is the case, we can apply the military planning process to meeting this threat. The first step in this process is looking for lessons learned that could be used in the current scenario: have we faced this threat before, and if so, what can we learn from the experience?

### **Cold War Model**

Port defense is not a new concept, but during the later stages of the Cold War port defense theory underwent considerable revision. In the mid-1980s the “long war,” or prolonged NATO/Warsaw Pact conventional war scenario came into vogue with NATO planners. In such a conflict re-supply of Europe would become a top priority. If Europe was to be re-supplied from the United States it was assumed that, given the noted strength of the Soviet submarine fleet, the historical “Battle of the Atlantic” scenario would repeat itself using modern technology. If this were the case it was assumed the coastline of the United States would be a logical target for attack; historically, the Nazi U-boat offensive against the coast during the Second World War was particularly effective, destroying over 400 ships in an almost completely undefended littoral, a lesson that would not be lost on Soviet planners.<sup>4</sup> But unlike the historic scenario where ships were subject to conventional torpedo attack, it was argued that the targets of Soviet offensive power would likely be ports due to the large array of unconventional weaponry that could effectively target port infrastructure (mines, special operations teams, etc.) and the impact that such an attack would have on the overseas war effort.<sup>5</sup>

Accordingly, an entirely new Coast Guard-Navy command structure was designed to meet the anticipated threat.<sup>6</sup> In 1984 the Coast Guard and Navy stood up the Maritime Defense Zone (MDZ), a combined USCG-USN command tasked with the maritime defense of the United States 200nm seaward. Ports, especially strategic out load ports, were given a high priority in defensive planning in recognition of the high tech infrastructure that was necessary to load-out mass military supplies. This was arguably the first time since the Second World War that the defense of ports became a significant part of the national maritime strategy. Reflecting this priority, a new command and control system was designed and implemented for tactical defense. Ports and outload

operations were placed under Navy-Coast Guard “Sub-Sector” constructs that effectively combined defensive operations between the Services by co-locating Coast Guard and Navy personnel in operations centers that would oversee all military operations (including load out operations and critical infrastructure protection) within the port during time of national emergency.

Since we once again face a threat from the sea, it would be tempting to simply implement a defensive structure similar to that used in the past. But there are key differences between then and now that make this problematic. In the Cold War defense model, risk was very much a matter of proportionality and the threat to critical maritime infrastructure was distinctly military. In considering the “worst case” scenario, planners envisioned enemy actions in the littoral focusing on submarine attack, offensive mining, and special operations attacks against critical military infrastructure—in other words, attacks “from” the sea by conventional military means. It was assumed that “terrorist” actions would be sponsored by the enemy state and, as part of the enemy strategy, would not be directed against targets with limited or no military significance.

These core assumptions aided the defense effort considerably. In the re-supply of Europe scenario, “risk” was by no means an equal proposition. Ports were rated in strategic priority based on the amount of support they provided military forces overseas, the ports with the highest priority receiving the lion’s share of the defensive forces. This strategy worked on a “floating” scale and was subject to change based on the evolving scenario; when New York City, for example, had completed its out load operations the priority (and subsequent defensive forces) shifted to the next port, allowing for a strategically “phased” defense.<sup>7</sup> In other words, we only needed to be strong in areas that were important to the war effort overseas—and this defensive strength was transitory at best.

The difference between “then and now” is telling when we consider potential targets and the subsequent effort required for defense. In the “old days,” a strictly civilian target such as the WTC would not have been considered a valid target in New York City. The major weapons out load point at Earle, NJ, however, was Priority One for infrastructure protection. Obviously this has changed; targets in GWOT can be anywhere or anything. Maritime infrastructure that would not be considered critical in a Cold War scenario now has the potential to be targeted as a means of obtaining an economic or psychological victory. In this “new” scenario with its plethora of non-military targets and the potential offensive power of the enemy, there are not enough defensive forces to go around. This requires that we consider force multipliers beyond simple assets to improve the viability of the defense.

This is not to say that the Cold War model is completely invalid, or that we cannot learn from the lessons of history. What worked in the MDZ era was the establishment of a construct that emphasized joint communications, multi-service planning, and, above all, a multi-agency approach to defense of the port and its infrastructure. Force multipliers that can be employed in the current scenario revolve around the collection and use of multi-agency intelligence in a similar command and control construct for the protection of critical maritime infrastructure. In the “old” model, military intelligence sufficed to deal with a specific military threat against known target areas, with a response that was distinctly military. The new threat requires that we expand this model to consider all agencies within the port vital for total protection.

## New Defensive Strategies

Maritime law enforcement (and by extension, protection of maritime critical infrastructure) is traditionally a Coast Guard mission. This has obviously evolved considerably as a result of the events of 9/11. When examining current port command and control proposals, it is useful to examine this evolution and how previous relationships can be employed in current operations.

**A. Pre-9/11 Port Operations:** Prior to 9/11 the Coast Guard port and offshore tactical constructs were divided into two separate areas of responsibility based on the type of law enforcement being conducted. In major ports the traditional Captain of the Port (COTP) position was assigned to a respective Marine Safety Offices (MSOs) responsible for the regulatory functions, such as vessel inspection, environmental response, licensing, etc. COTPs were (and are) responsible for merchant vessels entering and leaving port, conducting vessel inspections for maritime safety, and coordinating incident response. Maritime law enforcement conducted by MSOs was distinctly regulatory in nature; many vessel inspectors and recreational boating safety personnel performed their duties unarmed. Operations of a more traditional law enforcement variety, such as counter-narcotics or fisheries enforcement, search and rescue, and other offshore operations were the responsibility of a “Group” that maintained command and control of subordinate “Stations” in the Area of Responsibility (AOR) assigned that Group.<sup>8</sup> While this description is admittedly overly simplistic, it would be fair to say that MSOs “owned” the ports and all responsibilities for large merchant vessel and container operations that traditionally required regulatory attention, while Groups focused offshore and conducted law enforcement operations dealing with smaller maritime traffic or search and rescue. Afloat operational assets (utility boats, patrol boats, and small cutters) were generally “owned” by the Groups and used offshore in traditional law enforcement, although there was limited cooperation with the MSO for close inshore operations that required these assets.<sup>9</sup> It is important to note that both MSO/COTP and Group organizations maintained extensive relationships with other agencies working within the port and their respective areas of responsibility.

While this relationship and division of responsibility made sense prior to 9/11, the new asymmetric threat altered the equation considerably, requiring a merging of traditional responsibilities across established lines of command. The expanded threat spectrum now reached directly into the ports. Pure regulation, although still important for security, no longer sufficed; a direct law enforcement response capability (traditionally the role of Groups) was now required in the ports. Tracking and intercept of large merchant vessels, traditionally an MSO function, took on a new meaning as these vessels represent a potential threat to the security of the United States. Subsequently, merchant vessel regulation focusing on maritime security was “pushed” far offshore with the establishment of a layered defense.<sup>10</sup> The new threat also affected other agencies with maritime security concerns. Ports with a high Navy interest (including ports with Navy bases, research facilities, critical infrastructure, and out load responsibilities) that traditionally had some degree of Navy security immediately implemented extensive anti-terrorist force protection (ATFP) procedures to prevent, among other things, a “USS COLE” style attack on potentially vulnerable warships. U.S. Customs immediately

implemented increased forms of container and cargo security measures that were completely lacking prior to 9/11. It is clear from these new multi-agency security requirements that the somewhat laissez-faire command system exercised in the ports prior to 9/11 would no longer suffice in light of the new threat.

**B. Post 9/11 Reorganization:** The Coast Guard's answer to the post 9/11 threat was a merging of responsibility under a newly designed "Sector" organization, an effective combination of responsibilities and assets that has sole responsibility for all Coast Guard missions in one geographic area.<sup>11</sup> Sectors represent a merging of traditional Group and MSO/COTP functions, a significant cultural shift to "one mission" from several within each port. This re-organization soon took on a multi-agency nature. As noted, Coast Guard commands traditionally have close ties to other agencies in the ports, including Customs, Immigration, commercial organizations, and local, state, and federal law enforcement. This was reflected in the design of the new Sector Command Centers (SCCs). Tailored to meet local requirements, most SCCs possess either electronic links to other agencies operating in the port or staff positions for representatives from agencies to work in direct liaison with Coast Guard personnel on a daily or continuous basis. There are currently 44 SCCs operating or nearing completion.

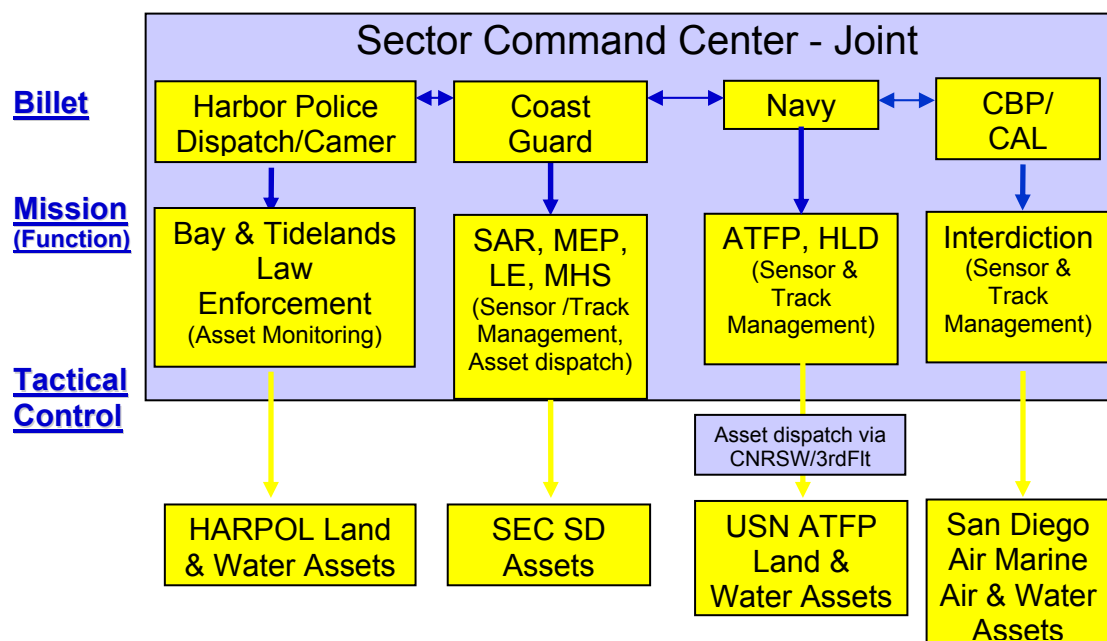
**C. JHOCs:** SCCs perform traditional port security and regulatory functions, but do not generally coordinate with DOD. In terms of critical maritime infrastructure protection this can be problematic, as much of the infrastructure is located in ports with a DOD presence, or is considered essential to DOD, and will therefore potentially fall under the auspices of Homeland Defense. This was recognized early in the SCC design process; the solution was similar to that employed during the MDZ era and stressed multi-service cooperation. Building on established infrastructure, Coast Guard and Navy designed a specialized SCC called the Joint Harbor Operations Center (JHOC), an experimental fusion center that quickly demonstrated its utility in providing for tactical operations between the Services. Recognizing a mutually beneficial interest in coordinating operations, the first JHOCs focused on fusing Coast Guard and Navy operations in port protection and ATRF in ports where the Navy had a large fleet presence.<sup>12</sup> Given their multi-agency approach to port security and littoral operations, JHOCs are a natural choice for the implementation of tactical port operations for maritime critical infrastructure protection. As such they can serve as a model for future execution of this mission.

JHOCs are far more than a merging of CG traditional roles and responsibilities with USN security procedures. Rather, they represent an important model for the fusing of intelligence and coordination of all multi-agency operations necessary for maritime critical infrastructure protection. As we have seen, Coast Guard and Navy cooperation is neither new nor particularly unique. Since the earliest days of each organization, both have used similar equipment and procedures in order to effectively operate together during time of war. But despite overseas operations in GWOT, U.S. ports are not on a war footing; rather, commerce and port operations continue at the normal pace, albeit under increased security procedures. Recognizing the number of agencies that operate in ports and the vast information requirements for maritime security and infrastructure protection, an effort was made to make JHOCs truly inter-agency by providing linkage to these agencies, including the establishment of formal liaison positions and data sharing

protocol, effectively merging regulation, law enforcement, and anti-terrorist force protection data and procedures.

The first experimental JHOCs were constructed and successfully tested in San Diego and Norfolk, ports that represented high strategic interest due to major Navy presence and the volume of overseas commercial traffic. These JHOCs' multi-agency design was based on relationships the Coast Guard had previously established during its normal operations within each port. This experimental design is illustrated in Figure 1 below:<sup>13</sup>

**Figure 1: JHOC Structure**



JHOCs possess several unique capabilities that contribute significantly to port and critical infrastructure protection. As command and control centers for ports and their immediate vicinity, JHOCs have inherent surveillance capability that can be fused into one multi-agency common operating picture (COP). Using the San Diego JHOC as an example, these systems include:

- USCG Coastal Radar
- USN Port control/offshore radar system
- Automated Identification System processors
- San Diego port control camera system (civilian)
- Navy waterside security system
- Border patrol camera/thermal imagery system

The initial success of JHOC San Diego and Norfolk led to a joint Coast Guard-Navy study to expand the project to all ports of strategic interest, using a three-tiered approach. Ports with navy presence, high commercial infrastructure, and 'outload' capability (loading of wartime material and supplies critical for overseas efforts) were considered for JHOC installation.

### **The Next Step: JHOCs as an Element of MCIP**

Although there are only two fully functional JHOCs today, their evolving construct serves as a model for a future development of multi-agency cooperation in maritime critical infrastructure protection. Given the importance of our ports to national strategy, MCIP is a critical vulnerability that must be addressed by both DHS and DOD in one coordinated effort. We must recognize that this mission goes beyond traditional port security operations or anti-terrorist force protection, and as such demands a command and control construct that can truly fuse the myriad of responsibilities and operations in ports.

Multi-agency JHOCs offer several advantages for merging effective port operations and critical infrastructure protection. This is evident in the areas of intelligence fusion, coordinated planning, and tactical command and control.

#### **A. Tactical intelligence fusion**

In the post-9/11 analysis one of the greatest weaknesses cited by the 9/11 Commission was a lack of intelligence fusion between respective government agencies. JHOCs are designed to address this weakness on the tactical level, serving as fusion centers that effectively merge the various intelligence databases of each respective agency participating in the JHOC. Currently, these databases include the Coast Guard's Maritime Information Safety and Law Enforcement system, the Automated Regional Justice Information System (Naval Criminal Investigative Service), and intelligence from the local Joint Terrorism Task Force.<sup>14</sup> As JHOCs expand to include other agencies, this fusion function can naturally expand to include additional databases. In addition to using established databases, JHOCs also use inter-agency sensors and local inter-agency liaison to collect, fuse, and disseminate information that is critical for achieving a multi-agency tactical picture. This increased multi-agency awareness provides for streamlined operations between all port agencies, while the use of multi-agency sensors and databases allows for a tremendously enhanced capability for surveillance and anomaly detection, a crucial element in maritime critical infrastructure protection.

#### **B. Coordinated planning for MCIP**

One of the great advantages of a JHOC is the joint personnel structure that allows for both rapid and long-term on-scene multi-agency cooperation. Although primarily staffed by Coast Guard personnel, billets are being established for personnel from all agencies that have responsibility in the port, representing a unique merger of personnel with regulatory, law enforcement, and military expertise.<sup>15</sup> This liaison system is fundamental to the success not only for coordination of operations, but also to reach an understanding of multi-agency procedures and practices and infrastructure that each agency allots priority for protection. This is critical for tactical multi-agency planning. Given the large

number of regulatory agencies operating in each port, there are a number of procedures specific to each agency that can impact other multi-agency operations. Customs container inspections, for example, are a critical part of vessel tracking and re-routing performed by the Coast Guard; FBI tracking of potential terrorist suspects is a key element of ATRP for the Navy and facilities security forces. This type of information and, perhaps more importantly, how these procedures are carried out, can be provided immediately by effective liaison that merges agency operations into one efficient cooperative effort.

### **C. Multi-agency Command and Control**

Ultimately maritime critical infrastructure protection is about the tactical coordination of multi-agency assets conducting port security and defense operations. JHOCs are first and foremost operations centers, possessing considerable command and control capability that can be used by multi-agency assets. By acting as combined, multi-agency fusion centers, JHOCs provide a unique tactical picture that all users can employ at the port level. Through its command and control apparatus, it is possible to coordinate tactical actions not only in crisis, but also in day-to-day port operations and exercises meant to improve multi-agency coordination.

## **CONCLUSIONS**

Access to the sea is vital for economic expansion and as a means to project national power. Ports are essential in maintaining this link. But ports are not fortresses; as open industrial and commercial centers, port infrastructure is particularly vulnerable to a dedicated enemy. An effective attack against critical maritime infrastructure has the potential to cause major economic disruption nationwide, create mass casualties, and limit or halt deployment of naval power. As such, ports are logical targets for terrorists bent on striking at vulnerabilities; the destruction of ports would have significant impact on our nation.

Lessons from the past indicate that the key to effective defense is tactical coordination through dedicated multi-agency command and control. During the Cold War, the Coast Guard-Navy model for command and control was to deal with a military threat from the sea, but this has changed with the new asymmetric threat of GWOT. The diversity of the threat against our ports and the number of regulatory agencies that oversee critical infrastructure requires an expanded comprehensive command and control system that fuses multi-agency intelligence, has understanding of multi-agency capabilities, and can provide direction to these forces in the field. The JHOC concept has proven to be effective in multi-agency intelligence fusion and coordinated tactical port operations essential for maritime critical infrastructure protection and should be considered a model for coordinated port defense.

---

<sup>1</sup> [www.dhs.gov/dhspublic](http://www.dhs.gov/dhspublic)

<sup>2</sup> J.Z. Heck, "Port Security: Nation Faces Formidable Challenges in Making New Initiative Successful" (Washington D.C.: GAO Publication No. GAO-2-993T (United States General Accounting Office), 3.

<sup>3</sup> [www.cato.org/pus/pas/pa090.html](http://www.cato.org/pus/pas/pa090.html)

<sup>4</sup> Michael Gannon, *Operation Drumbeat*, (New York: Harper and Row, 1990), xviii.

<sup>5</sup> R. B. Watts, "Coastal Defense: Now More than Ever," (Annapolis: U.S. Naval Institute *Proceedings*, Dec. 1990), 66.

<sup>6</sup> Author's experience as an MDZ planner, 1988.

<sup>7</sup> The composition of Groups varies considerably. Traditionally, Groups are composed of a command center and have direct control of a number of smaller afloat assets, such as patrol boats and buoy tenders, and occasionally were co-located with air stations and controlled the helicopters/planes assigned to that station. "Stations" are smaller CG commands that maintain small offshore utility boats for near coastal SAR and law enforcement. Author's operational experience. See also P.J. Capelotti, "The Coast Guard's Response to 9/11," *Joint Center for Operational Analysis and Lessons Learned*, 4, Issue 4, September 2004.

<sup>8</sup> Each Group/MSO had individual Standard Operating Procedures (SOPs) that detailed this relationship, which varied in individual ports. The characterization/summary of these relationships is based on the author's operational experience.

<sup>9</sup> *Maritime Strategy for Homeland Security* (Washington D.C: U.S. Coast Guard, July 2002)

<sup>10</sup> Where applicable, Sector organizations also include Vessel Traffic Services (VTS) and CG Air Stations.

<sup>11</sup> It is important to note that at the time of this writing DOD participation in JHOCs are limited to ATPF, so USN presence in JHOCs are currently limited to areas of fleet or asset concentration. R. Watts, "JHOC Working Group Meeting/Briefing to Maritime Security Integration Group," 22 June 2005.

<sup>12</sup> "Pacific Area Capabilities and Interoperability for Homeland Security/Homeland Defense," Alameda: Unclassified briefing to Honorable Paul McHale, December 14" 2004.

<sup>14</sup> MSIG brief, 28 Feb 2004.

<sup>15</sup> Coast Guard Pacific Area (PACAREA) JHOC brief to author, December 2003

# *Homeland Security Affairs*

---

*Volume I, Issue 2*

2005

*Article 4*

2005

---

## Using Organizations: the Case of FEMA

Charles Perrow\*

\*Yale University, [charles.perrow@yale.edu](mailto:charles.perrow@yale.edu)

Copyright ©2005 by the authors. *Homeland Security Affairs* is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of *Homeland Security Affairs* or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in *Homeland Security Affairs* rests with the author(s) of the article. *Homeland Security Affairs* is the online journal of the Center for Homeland Defense and Security (CHDS). <http://www.hsaj.org/hsa>

# Using Organizations: the Case of FEMA

Charles Perrow

## Abstract

FEMA was used once before, under President Reagan, for counter-terrorism and as a result, natural disaster response and mitigation suffered. It was repaired under President Clinton, but again, counter-terrorism has eaten up FEMA's natural disaster budget and skills.

**AUTHOR BIOGRAPHY:** Charles Perrow is a Research Scholar and Emeritus Professor of Sociology at Yale University. The author of several books and many articles on organizations, he is concerned primarily with the impact of large organizations on society (*Organizing America: Wealth, Power, and the Origins of Corporate Capitalism*, 2001) and their catastrophic potentials (*Normal Accidents: Living with High-Risk Technologies*, 1999). His current interests are in the vulnerabilities of the country's critical infrastructures to natural, industrial, and deliberate disasters.

**KEYWORDS:** organizations, politics

## Introduction\*

Organizations are tools; their masters need not use them for their nominal ends. The focus of FEMA under President Clinton was natural disaster emergency relief and preparedness. Under the Bush administration the focus was shifted to combating terrorism, and disaster relief capabilities decayed. That left us unprepared for Hurricanes Katrina and Rita. This lack of preparedness led to the massive organizational failures we have been treated to by a shocked media.

For days following Katrina, air conditioned trucks with no supplies drove aimlessly past “refugees” who were without water or food or protection from the sun. Reporters came and went, but food and water and medical supplies did not.<sup>1</sup> The Red Cross was not allowed to deliver goods because it might discourage evacuation.<sup>2</sup> Evacuation by air was slowed to a crawl because FEMA said that post 9/11 security procedures required a (prolonged) search for more than 50 federal air marshals to ride the airplanes, and to find security screeners. At the gates, inadequate electric power for the detectors held things up until officials relented and allowed time consuming hand searches of desperate and exhausted people.<sup>3</sup> Their only food, emergency rations in metal cans, was confiscated because the cans might contain explosives.<sup>4</sup> Volunteer physicians watched helplessly; FEMA did not allow them to help because they had not been licensed in the state.<sup>5</sup> Without functioning fax machines to send the required request forms, FEMA would not send help that local officials begged for. Perhaps a fifth of the New Orleans police force simply quit, exhausted and discouraged, under fire from looters, or were themselves looting. A large National Guard force hid behind locked doors in the convention center, saying they were unprepared to help. A Navy ship idled off-shore, waiting for days to be called. Almost five days after Rita struck, at least one severely damaged Texas town remained without any outside help, out of power, water and food, with an alerted TV camera crew being the first to arrive. And so on.

Did these failures reflect what has been called “prosaic” organizational failures such as all organizations are likely to have in times of stress? Were the organizations simply overcome by an unprecedented challenge? Or had the resources for meeting natural disasters decayed or been diverted towards terrorist disasters? If it was the latter, decay and diversion, we will have to explain why relief organizations other than FEMA also failed.

---

\* This is a section of a manuscript in preparation, “Disasters Evermore? Reducing U.S. Vulnerabilities to Natural, Industrial, and Terrorist Disasters.” Thanks to Lee Clarke for many suggestions and corrections. For other sections of the manuscript see “The Department of Homeland Security, our second great disaster after 9/11,” forthcoming in *Homeland Security Affairs* and “Disasters Evermore? Reducing U.S. Vulnerabilities...” forthcoming, Havidan Rodriguez, E. Quarantelli and R. Dynes, eds., *Handbook of Disaster Research* (Springer, 2006).

The failures involved government agencies and the military at all levels, not just FEMA. But FEMA was the organization most responsible for disaster response. What happened to it? It seemed to have performed reasonably well the previous year when four hurricanes struck Florida (though there were charges of gross mismanagement in the dispersal of funds). A review of its history is not encouraging, and will offer some possible explanations for its failures in 2005.

### **FEMA's rocky history**

FEMA got off to a modest but fairly good start when it was founded by President Jimmy Carter in 1979, in one of his last attempts to restructure the federal government. But the bungled Iranian hostage crisis drove him from office and put Ronald Reagan in. When it was first formed by Carter the agency had two goals. The main one was disaster relief, prevention, and mitigation. The secondary ones were coping with a nuclear attack and, vaguely, national security, something normally in the hands of other agencies. Under Reagan the first goal was neglected and starved of resources, while the secondary ones flourished. FEMA set up a "Civil Security Division" with a training center for over 1,000 civilian police to handle riots and political disturbances (not disaster relief). A file was gathered on U.S. left-wing activists and internment camps were planned. One national training exercise envisioned incarcerating 100,000 "national security threats".<sup>6</sup> A top secret National Security Directive (NSDD 26) that Reagan issued in 1982 effectively linked FEMA with the military and the National Security Council (NSC). Within FEMA, a small division, the National Preparedness Directorate (NPD), was charged with developing a classified computer and telecommunications network to insure the continuity of the government in the event of a nuclear attack. The network was developed by the National Security Council and subsumed within the broader DOD national defense information network. Though originated by FEMA, and drawing upon more and more of FEMA's budget, FEMA's disaster relief personnel could not have access to the network. It was "top secret;" only the DOD and the NSC could access it. Congress could not examine the activities or budget of the Civil Defense part of FEMA.<sup>7</sup> As a result, "FEMA developed one of the most advanced network systems for disaster response in the world, yet none of it was available for use in dealing with civilian natural disasters or emergency management."<sup>8</sup>

The FBI was jealous and alarmed, and so was the Justice Department. The head of FEMA, Louis Giuffrida, was forced to resign when the Justice Department brought suit in 1985 over cronyism in the agency's contract awards and a lavish bachelor pad for Giuffrida in Manhattan using FEMA funds. His collaborators, Lt. Col. Oliver North and the equally controversial General Richard Secord, had already left FEMA. But the organization continued to ignore natural disasters and, when disasters came, the personnel were poorly trained and funded and quite possibly inept. Hurricane Hugo in 1989 prompted U.S. Senator "Fritz" Hollings to declare that FEMA was "the sorriest bunch of bureaucratic jackasses I've ever known."<sup>9</sup> The next year, when disasters hit California, Representative Norman Y. Mineta of California declared that FEMA "could screw up a two car parade." Two years later, when Hurricane Andrew hit in 1992,

the primitive communications system of the agency forced it to buy Radio Shack walkie-talkies in last minute preparations, while the state-of-the-art system FEMA had paid for remained unavailable. President Bush had to call in federal troops and move the FEMA director aside. If this sounds familiar to those who watched the Katrina disaster, recall that the agency had been hijacked by those preoccupied with nuclear defense and domestic radicals. Its failure helped William Clinton push the first President Bush aside.

FEMA recovered remarkably well under the leadership of James Lee Witt, an experienced disaster manager appointed by President Clinton in 1993, and performed as well as we might expect any agency to perform. It not only handled emergency relief well, but set up far-seeing programs to minimize damage from future disasters, for example, buying up vulnerable land to prevent the establishment of settlements – the “mitigation” program. Employees performed well and shared the goals of the organizational masters. It had a minimum of political appointments.

### **FEMA under a Bush**

But FEMA swerved abruptly to the right again under President G.W. Bush, emphasizing privatization of disaster response and counter-terrorism rather than natural disasters. FEMA's Project Impact was a model mitigation program created by the Clinton administration; it moved people out of dangerous areas and retrofitted structures.<sup>10</sup> For example, when the Nisqually earthquake struck the Puget Sound area in 2001, homes that had been retrofitted for earthquakes and schools with FEMA funds were protected from high-impact structural hazards. The day of that quake was also the day that the new president, G.W. Bush, chose to announce that Project Impact would be discontinued.<sup>11</sup> Funds for mitigation were cut in half, and those for Louisiana were rejected. Disaster management was being privatized, with the person who was to be promoted to head the agency, Michael Brown, saying at a conference in 2001, "The general idea – that the business of government is not to provide services, but to make sure that they are provided – seems self-evident to me."<sup>12</sup> The administration tried to cut federal contribution for large-scale natural disaster expenditures from seventy-five percent to fifty percent, but Congress balked.

Worse still, when a Department of Homeland Security was forced upon President Bush by Senator Joseph Lieberman and other Democrats, FEMA lost the cabinet status President Clinton had given it and was folded into the new department. The Government Accountability Office, Congresspeople, the Brookings Institution, and others warned that this could hobble the agency's natural disaster programs, and it did. Top personnel left (some to the companies that privatization of emergency relief and preparedness enriched); a union survey of eighty-four union personnel found eighty percent saying it was a “poorer agency,” and sixty percent said they would leave if they could get the same salary in another agency; and the GAO rated its morale as one of the lowest of any government agency.<sup>13</sup> While funds for the agency have actually increased somewhat in the last two years, those for disasters have shrunk while expenditures for counterterrorism have soared. FEMA has lost control of the federal preparedness grants to local

and state governments. Those are distributed by a separate office and, as a result, three out of every four grants are now spent on counterterrorism. (Much of the money spent on counterterrorism goes to corporations and private businesses; natural disaster money is more likely to be spent on training first responders, hardly a corporate feeding place.) This has been a major blow to states such as Louisiana that are prone to weather disasters.

FEMA, it is charged, not only shifted from natural disasters to counterterrorism, but to political favoritism, another example of using organizations, and it had consequences. Representative Bennie Thompson of Mississippi, hard hit by Katrina, said that during the Bush administration, "FEMA went back to being treated like a political resting place for favors that were owed," and called for the resignation of FEMA head Michael Brown. Brown was brought into the agency in 2001 by his college roommate, Joe M. Allbaugh, who had run Mr. Bush's first presidential campaign. Even Brown's small claim to have disaster experience turned out to be fabricated. He said on a Thursday evening TV appearance, three days after Katrina struck, that he had just learned of the plight of thousands stranded at the convention center in New Orleans without food or water. They had been there since Monday, but that Thursday Mr. Brown told an incredulous TV interviewer, Paula Zahn, "Paula, the federal government did not even know about the convention center people until today."<sup>14</sup>

It also did not know where the ice was. Ninety-one thousand tons of ice cubes, intended to cool food, medicine, and victims in over 100 degree heat, were hauled across the nation, even from Maine, by 4,000 trucks, costing the taxpayers over \$100 million. Most of it was never delivered. In an age of sophisticated tracking (FedEx, DHS, Wal-Mart, etc.), FEMA's system broke down. Asked about the vital ice, Mr. Brown invoked privatization, and told a House panel "I don't think that's a federal government responsibility to provide ice to keep my hamburger meat in my freezer or refrigerator fresh."<sup>15</sup> The ice was not needed for his refrigerator, but to keep drugs and medicine fresh, to treat people with heat exhaustion, and to keep the sick, old, and frail cool.

### **Some explanations of recent failures**

FEMA was not the only organization to fail so massively, but it, and its parent organization, the Department of Homeland Security under Michael Chertoff, was certainly a key one. Can we attribute this to the evisceration of FEMA under the Bush administration? Did its enfeeblement also enfeeble the response of the National Guard, the military when it was called in, and local and state agencies? At the present writing, October, 2005, it is not clear and much more research is needed to understand the response to Katrina and Rita. For we have three observations, and the lessons from them remain to be investigated: the response to four hurricanes in Florida in the previous year; the response to Katrina; and the response to Rita.

It is possible that FEMA was not deteriorating, but just overwhelmed by Katrina, and recovered somewhat under Rita. The response to Rita has been declared much better by some news stories and almost as bad by others.<sup>16</sup> Rita should have been easier. It was less destructive;

citizens were more likely to evacuate early based on the experience with Katrina; major cities were not hit; top FEMA officials would be unlikely to again be unable to alert the President; and state guards and the military were already mobilized. Here are four possible interpretations of the varying responses to the Florida hurricanes, Katrina, and Rita.

1). FEMA's natural disaster potential deteriorated steadily through 2005, as it was used for other purposes, but this was not noticed in 2004. The hurricanes in that year were not as serious as those in 2005, and we did not get as many news stories about failures in 2004. (A close investigation of the Florida responses would be needed to judge the importance of this explanation.)

2). The response to the Florida hurricanes was good, despite the deterioration, because Florida was a politically key state for the administration; Louisiana was not, and Texas was already in Republican hands. Therefore FEMA officials paid more attention to Florida. (FEMA approved payments in excess of \$31 million to Florida residents who were unaffected by the 2004 hurricanes, for example.)<sup>17</sup> Research has shown that presidents designate areas as eligible for disaster relief, and give out much greater assistance, when these areas are politically important for them. Political scientists have found that nearly half of all disaster relief is motivated politically rather than by need.<sup>18</sup> The fact that President Bush had yet to establish a plan for housing evacuees, or a commission to oversee the rebuilding of New Orleans and other coastal cities in three states a month and a half after the hurricane, suggests a lack of political incentive.

3). Katrina and Rita ("KatRita") were so much more powerful and damaging that even a well-performing FEMA would have been overwhelmed. This explanation does not assume deterioration on the part of the agency's ability to deal with natural disasters. It assumes a tipping point, and when disasters are involved, the tipping point may bring about a sudden, rather than gradual, decline. Once it is challenged beyond its capabilities, the failures can be sudden and wide-spread even if the organization is not weak.

This explanation is persuasive. But the problem is that the failures of FEMA in KatRita at all levels seem so enormous and widespread it is hard to argue that common sense and obvious responses would evaporate so widely. Disaster agencies have to be flexible and innovative, even if the challenge is overwhelming. This one frequently appeared to revert to rote training and inappropriate rules.

4. The final explanation offered is that undoing an agency that had been performing well takes time, and that this undoing was speeded up greatly by having an unprecedented task. While the previous explanation has obvious merit, this explanation maintains that substantial undermining of the agency had taken place, and KatRita exposed this more fully than the Florida hurricanes of 2004 could have.

The examples given at the beginning of this article, and there are many more, seem to go well beyond "prosaic" failures, or even the "overwhelming" explanation in alternative number three.

They did not involve panic, enormous overload, nor unfamiliar tasks or settings, which would accompany failures in unprecedented events. They involved going by the rules. Rather than being flexible and innovative, even when the challenge was overwhelming, these personnel appeared to revert to rote training, insistence upon following inappropriate rules, and an unusual fear of acting without official permission. This could be the result of the agency's downgrading the importance of responding to natural disasters, replacing or losing personnel skilled in that area, and diverting funds to the commercially, and politically, more attractive alternatives of buying equipment such as chemical detection devices, bio-hazard suits, and perimeter surveillance devices, and paying for industrial and port upgrades that have little to do with terrorist threats.

Organizational dynamics could be at work, also. I suggest that as the top ranks of the agency lost experienced personnel with high morale and commitment, who were replaced by political appointments, the next level would gradually lose confidence in their superiors, and their morale would slacken. I know of no statistics regarding FEMA, but nationally the Bush administration has increased the number of political appointees for government agencies by fifteen percent since 2000.<sup>19</sup> (In President Clinton's second term, the percentage of political appointments declined.) FEMA has always had many political appointees; most agencies do. But if they increased by fifteen percent it would have an impact.

In time, the low morale of upper managers who were not political appointments would spread to lower management, and then to employees in general. In an organization with low morale it may be that sticking to the rules to protect your career is better than breaking them even if the rules are inappropriate. This defensive posture might spread to allied agencies, such as the Transportation Security Administration, which is already less concerned with safe transit than terrorists' potential to use transportation as a weapon. A hypothetical situation could prompt these questions: Is the TSA official in charge of the security of a local airport very likely to tell his employees to stop doing their principle job and just let the evacuees through? Not if he knows that FEMA officials are not sending water and food to the airport because airport staff cannot send the proper requisitions because the faxes are out. The message may be that in perilous times it is best to go by the book. (While not unreasonable, this is not substantiated by research, as far as I know). This is a different explanation than "they panicked" or "the storm was so large and the task so unprecedented."

A further consideration is that the reorganization of FEMA into the Department of Homeland Security imposed a top-down, command-and-control model on an agency that most experts say should maximize the power of those at the bottom. Maximizing the ability of the lowest level to extemporize and innovate will minimize the bureaucratic responses that so characterized FEMA. A frequent criticism of FEMA was that the centralized DHS model, and the removal of authority for preparedness to other parts of DHS, would inhibit its responsiveness to unique events.<sup>20</sup>

We are left with at least two interpretations. One is that FEMA was not hurt by incorporation into the Department of Homeland Security. It performed well in 2004, had an unprecedented task

with Katrina and could be expected to fail, but recovered and performed reasonably well in Rita, which was less devastating than Katrina but more so than the Florida hurricanes.

A second interpretation is that FEMA was progressively deteriorating; the deterioration was not picked up by the press in 2004, but was evident when the Katrina challenge was greater. The agency did only marginally better with Rita, a lesser challenge and with the advantages of very recent experience, more credible warnings, and mobilized relief forces.

Each disaster is unique, and routines, such as pre-positioning and ordering ice ahead of time, certainly help. These appear to have been inadequate in KatRita. More important, the ability to scramble, extemporize, and innovate, seems to have degraded. (Privatization fans have a point that some of the most creative responses came from private business, but this may reflect the state of FEMA rather than a public/private comparison.)<sup>21</sup> It is possible that this was the most important failing. If so, it may be attributed to the use of the organization for purposes other than those for which it was designed. It may have been used to reward political friends and loyalists, to further an image of being “tough on terror” for political image reasons, and to make expenditures that favored private enterprises and political constituencies rather than on training and on first responders.

---

<sup>1</sup> Staff 2005b, ""Hope is fading" at New Orleans Convention Center," NBC, MSNBC.  
[http://www.truthout.org/docs\\_2005/090205L.shtml](http://www.truthout.org/docs_2005/090205L.shtml).

<sup>2</sup> American Red Cross, "Hurricane Katrina: Why is the Red Cross not in New Orleans?" 2005.  
[http://www.redcross.org/faq/0,1096,0\\_682\\_4524,00.html](http://www.redcross.org/faq/0,1096,0_682_4524,00.html).

<sup>3</sup> Robert Block, et al., "Behind poor Katrina response, a long chain of weak links," *Wall Street Journal*, September 6, 2005, 1

<sup>4</sup> Larry Bradshaw and Lorrie Beth Slonsky, "Hurricane Katrina -- our experiences," EMS Network News, 2005.  
[http://www.emsnetwork.org/artman/publish/article\\_18427.shtml](http://www.emsnetwork.org/artman/publish/article_18427.shtml).

<sup>5</sup> John Tierney, "Going (down) by the book," *New York Times*, 2005.

<sup>6</sup> Ward Churchill, and Jim Vander Wall, *The COINTELPRO Papers: Documents from the FBI's Secret War Against Dissent in the U.S.* (Boston MA: South End Press, 2002); Diana Reynolds, "FEMA and the NSC: the rise of the national security state," *Covert Action Information Bulletin* 33 (1990); Robert Ward, Gary L Wamsley, Aaron D Schroeder, and David B. Robins, "Network organizational development in the public sector: a case study of the Federal Emergency Management Administration (FEMA)," *Journal of the American Society for Information Science* 51 (2000) 1018-32

<sup>7</sup> Ibid., Robert Ward, et al.

<sup>8</sup> NSDD 26 (1982) 1023. See also Churchill and Wall, "*The COINTELPRO Papers*," and Diana Reynolds, "FEMA and the NSC."

<sup>9</sup> NSDD 26, (1982) 1024

<sup>10</sup> Elliston, Jon, "Disaster in the making," *Independent Weekly*, September 22, 2004.  
[http://www.indyweek.com/durham/2004-09\\_22/cover.html](http://www.indyweek.com/durham/2004-09_22/cover.html)

<sup>11</sup> Eric Holdeman, "Disasters keep coming but FEMA phased out," *New York Times*, August 31, 2005

<sup>12</sup> Jon Elliston, "Disaster in the making."

<sup>13</sup> Ibid.

---

<sup>14</sup>Eric Lipton and Scott Shane, "Leader of federal effort feels the heat," *The New York Times*, September 3, 2005. <http://www.nytimes.com/2005/09/03/national/nationalspecial/03fema.html>

<sup>15</sup>Scott Shane and Eric Lipton, "Stumbling storm-aid efforts put tons of ice on trips to nowhere," *New York Times*, October 2, 2005.

<sup>16</sup> Spencer S. Hsu and Steve Hendrix, "Hurricanes Katrina and Rita were like night and day," *Washington Post*, September 25, 2005; Block, et al., "Behind poor Katrina response"; Staff Writers 2005b, "Katrina redux? Beaumont paper finds federal storm failures in Texas," *Editor & Publisher*, September 25, 2005.

<sup>17</sup> Jason Leopold, "FEMA chief Brown paid millions in false claims to help Bush win Florida votes." *The Free Press*, September 15, 2005. <http://www.freepress.org/departments/display/20/2005/1459>; Staff 2005a "FEMA: a legacy of waste." *South Florida Sun-Sentinel*, September 18, 19, 2005. <http://www.sun-sentinel.com/news/local/southflorida/sfl-femareport.0.7651043.storygallery?coll=sfla-home-headlines>

<sup>18</sup>Thomas A. Garrett and Russell S. Sobel, *The political economy of FEMA disaster payments* (Federal Reserve Bank of St. Louis: St. Louis, MO, 2002).

<sup>19</sup> Staff Writers 2005a, "Bush cronyism weakens government agencies," *Bloomberg*, September 30, 2005. [www.bloomberg.com/apps/news?pid=10000087&sid=aJzwLcLRZiek](http://www.bloomberg.com/apps/news?pid=10000087&sid=aJzwLcLRZiek)

<sup>20</sup> David Glenn, "Disaster sociologists study what went wrong in the response to the hurricanes, but will policy makers listen?" *Chronicle of Higher Education*, September 29, 2005. <http://chronicle.com/free/2005/09/2005092904n.htm>

<sup>21</sup> Gardiner Harris, "Storm and crisis: Early reaction," *New York Times*, September 11, 2005. <http://select.nytimes.com/gst/abstract.html?res=F30712FF3B550C728DDDA00894DD404482>

# *Homeland Security Affairs*

---

*Volume I, Issue 2*

2005  
2005

*Article 5*

---

## Changing Homeland Security: An Opportunity for Competence

Christopher Bellavita\*

\*Naval Postgraduate School, christopherbellavita@gmail.com

Copyright ©2005 by the authors. *Homeland Security Affairs* is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of *Homeland Security Affairs* or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in *Homeland Security Affairs* rests with the author(s) of the article. *Homeland Security Affairs* is the online journal of the Center for Homeland Defense and Security (CHDS). <http://www.hsaj.org/hsa>

# Changing Homeland Security: An Opportunity for Competence

Christopher Bellavita

## Abstract

Hurricane Katrina shattered belief that the nation's homeland security system was ready for a major terrorist attack. Public administrators staff that system. Katrina provides an opportunity to review the central normative premise of public administration: competence. This article briefly reviews the changing competence frameworks that have guided public administration since the 1880s. Over the last one hundred years, administrators have been seen as artisans, scientists, social reformers, and managers. The ineptness of the public sector's response to Katrina reminds us – however briefly – that for the last 30 years, government has been seen as the enemy, the problem to be solved – not the partner in finding solutions. The result is a demoralized and dysfunctional public workforce. The American homeland can never be secure until the public workforce recreates the spirit of competent service so glaringly absent in the wake of Katrina.

**AUTHOR BIOGRAPHY:** Christopher Bellavita teaches at the Naval Postgraduate School's Center for Homeland Defense and Security.

**KEYWORDS:** preparedness, public administration, Katrina

***What has happened down here is the winds have changed.  
Clouds roll in from the north and it started to rain.***

“It’s absolutely horrible,” says one of the women. “Babies aren’t getting food.”

“And they’re all black babies,” says the second woman.

“Old people are dying in wheelchairs. And they’re just leaving them to die,” says the first one.

“People can’t get out of the city,” says the second.

The scene is a metropolitan airport. It is early September. The nation is watching Katrina on television. The two women are in their early twenties. They are on break from their job at an airport coffee kiosk.

A man, waiting for his plane, hears the conversation.

“What are you guys going to do to make sure that never happens again?” he asks.

“What do you mean?” says the first one.

“What’s happening is horrible. You’re right. So what are you going to do about it? What are you going to do to make sure Americans never have to go through anything like this again?”

“What can we do?” shrugs the second one.

The man says nothing.

“Besides,” says the first one, “no one’s going to listen to anything people our age say.”

The man mumbles something unintelligible and walks toward his gate.

The woman is right. What is she going to say? “Y’all need to do a better job implementing the National Response Plan.” Or, “We need more of those communities to be NIMS compliant.” And even if she does have something to say, to whom is she going to say it? Whose job is it to fix the preparedness mess unmasked by Katrina?

---

***Rained real hard and it rained for a real long time.  
Six feet of water in the streets of Evangeline.***

There is one profession responsible for making sure Americans are not systematically ignored the next time catastrophe strikes: public administrators. It is ultimately their job to prevent terrorism, respond to disaster, and lead the tedious and often thankless task of recovering from catastrophe.

All the talk over the past four years about the perniciousness of “stovepipes” obscures the foundation that connects those pipes: public service.<sup>1</sup>

Public administrators, at least in theory, are responsible for conducting the public’s business, acting in the public’s interest, and conscientiously balancing formal requirements with the wisdom to do the right thing.

That is theory. The reality of public administration is considerably less Panglossian.

State, local and the national governments performed incompetently preparing for Katrina and responding to Katrina.<sup>2</sup> Strategies were ignored. Plans were not executed. Resources were wasted. We spent four years preparing for the unthinkable. The thinkable happened and we were not ready.

The entire preparedness system – staffed essentially by public administrators – failed to perform government’s primary job: to secure the unalienable right to life. With a few notable exceptions,<sup>3</sup> individuals and agencies were unable to bring together the knowledge, skills, abilities, or resources to do what the unraveling situation required. How could this incompetence be? How could this incompetence have happened?

Katrina provides an opportunity to think about what historically has been the normative bedrock of public service: competence.

---

***The river rose all day.  
The river rose all night.***

The history of public administration in the United States is a story of the changing relationships between public servants and their polity. The Founding Fathers paid some attention to the administrative problems associated with running a nation, but during the initial century of the American empire, there was a general aversion to the idea of a permanent group of civil servants.

In 1887, Woodrow Wilson – then a professor at Bryn Mawr College – made the first serious claim that administering the public’s business should be a professional discipline. Wilson wrote that the discipline’s central focus should be effectiveness and efficiency.

*It is the object of administrative study to discover, first, what government can properly and successfully do, and secondly, how it can do these proper things with the utmost possible efficiency and at the least possible cost either of money or of energy.<sup>4</sup>*

Wilson’s effort to bring competence into public work was motivated by a desire to remedy what he termed “a civil service which was rotten full fifty years ago.”<sup>5</sup> In words that read like they were prepared for testimony to the U.S. House Select Committee on Hurricane Katrina, Wilson wrote (in 1887):

*The poisonous atmosphere of city government, the crooked secrets of state administration, the confusion, sinecurism, and corruption ever and again discovered in the bureaux at Washington forbid us to believe that any clear conceptions of what constitutes good administration are as yet very widely current in the United States.<sup>6</sup>*

The corruption and incompetence in the public sector of the 19<sup>th</sup> and early 20<sup>th</sup> century contributed to the growth of the progressive movement.<sup>7</sup> In time, that led to civil service reform and to the demand, in Robert Biller’s phrase, “that the public’s business be conducted with competence, efficiency and care.”<sup>8</sup>

***Some people got lost in the flood.  
Some people got away alright.***

In the first few decades of the 1900s, the “public’s business” remained an inconsequential part of the America enterprise. The nation was under the normative sway of the “rugged individualist” and the economic direction of corporate interests. Herbert Hoover spoke of government as an umpire, not a player in economic life. He believed that government involvement in the private sector would threaten democracy and individual freedom.<sup>9</sup>

By 1932, twenty five percent of the U.S. workforce did not have a job. The Great Depression drained the ruggedness from the individualist mythos and forced a reconsideration of government’s role in American life. Franklin Roosevelt’s election accelerated an expansion of government that lasted for fifty years.<sup>10</sup> For people who grew up during the Great Depression, getting a government job, with its reliable paycheck and steady tenure, was a good career move.

From the 1900s until the late 1940s, public administration’s competence framework was constructed by practitioners who were guided by what Wilson called “stable principle.” People learned to do their work as apprentices. Elders who relied on experienced-based principles – what in today’s homeland security world might be called “doctrine” – tutored the new workers. In many respects, public administration was a guild.

---

***The river has busted through clear down to Plaquemines.  
Six feet of water in the streets of Evangeline.***

In 1946, Herbert Simon challenged the prevailing competence frame by arguing that a true science of administration could not be built on those stable principles, or what he called “proverbs.” Administration had to be based on the products of operational definitions of concepts and empirical theory – i.e., normal science.<sup>11</sup> Simon and other intellectual leaders transformed public administration from a domain where competent practitioners were guided by heuristics, to a realm where competence was defined by an “administrative science” that provided objective guidance about the right things to do and the right ways to do them. Government service became another – although somewhat second-class – home for the archetypical Organization Man.<sup>12</sup>

The socially chaotic 1960s and the early 1970s brought renewed attention to the role government could play in improving people’s lives. The normative premise of what came to be called the New Public Administration was captured by Todd LaPorte’s vision that “the purpose of public organization is the reduction of economic, social and psychic suffering, and the enhancement of life opportunities for those inside and outside the organization.”<sup>13</sup>

Public service attracted people who wanted to end economic and social inequality, both in the United States and in other countries. Competence was defined largely by having good intentions and the skills to turn those intentions into programs that improved people’s lives.

Lyndon Johnson’s Great Society marked the twilight years of public administration as an activity to enhance “life opportunities” for Americans. People started getting elected by arguing that government was the problem. Presidents Nixon, Ford, Carter, Reagan,

Bush, and Clinton sought to end – at least semantically – the “era of big government.”<sup>14</sup> From the time Johnson decided not to run for a second term through the 2001 terror attacks, government programs and rules became anathema to the economy, the good life, and individual liberty.<sup>15</sup>

The waxing distrust of government, and the growing economic opportunities in the private sector contributed to the considerable decline in the desirability of government jobs.<sup>16</sup> In the 1980s and 1990s, public service was frequently perceived as an organizational sanctuary for the unambitious, for people who could not succeed in the competitive, entrepreneurial, and unforgiving world of the private sector. It was a place for drones.<sup>17</sup>

---

***President Coolidge came down in a railroad train,  
With a little fat man with a note-pad in his hand.***

Woodrow Wilson’s 118-year-old dictum that “the field of administration is a field of business” is today’s dogma. The private sector – even in the face of Enron, WorldCom, Tyco, ImClone, Adelphia, Global Crossing and other examples of incompetence and corruption – remains the primary normative framework for public sector administrative aspirations. The language of business has suffused the public sector in ways too numerous to recount. Agencies have business plans and supply chains; they use benchmarks to identify best practices and industry standards. Public administrators are public managers. Citizens morphed into clients and customers. The DHS Secretary talks about his desire to “re-engineer” preparedness and “re-tool” FEMA.<sup>18</sup>

The comparatively few remaining administrators who entered government in the 1970s will be leaving public service within the next few years. Fifty percent of federal workers are eligible to retire in the next four years. Three quarters of those people are senior executives.<sup>19</sup> These administrators depart with their substantive and tacit knowledge, and with memories of a time when government and business operations were not synonymous.

Government service continues to be uninviting. As a February 2005 report from the Partnership for Public Services described the dilemma, “Many Americans view government careers as uninteresting or unappealing, or believe the federal workplace is in need of reform, making it difficult to attract and retain talent.”<sup>20</sup> Have you ever heard a child say, “When I grow up, I want to be a public administrator?”<sup>21</sup>

---

***The president say, "Little fat man isn't it a shame  
What the river has done to this poor cracker's land."***

Public administrators have taken a beating for over thirty years. What once was a domain of service is a fallow of despair.<sup>22</sup> Homeland security – with its myriad agencies defiled by the mediocrity of its Katrina response – symbolizes the status of much of the public sector.

A 2005 survey of people who work for the national government found “only 12 percent of the more than 10,000 DHS employees who returned a government questionnaire said they felt strongly that they were ‘encouraged to come up with new and better ways of doing things’.”<sup>23</sup> It is difficult for imagination or initiative to flourish in

an organization where only 3 percent of the workers are confident personnel decisions are "based on merit," only 18 percent feel strongly that they are "held accountable for achieving results," and only 4 percent are certain "creativity and innovation are rewarded."<sup>24</sup>

One could argue – based on the Katrina, Rita and Wilma headlines about response – that public sector incompetence is chiefly the result of unqualified leaders. But that explanation is too narrow. Followers are as critical to the competence equation as the men and women who carry the title of leader.<sup>25</sup> Incompetence is the result of government workers who accept less than an impassioned best from elected officials, appointed leaders, co-workers, and themselves. Incompetence is the result of a governance philosophy that belittles governance.

So what to do?

Mechanistically-minded reformers have already noted a need for structural and functional corrections to our preparedness system. DHS will be re-organized on the basis of its Second Stage Review – an analysis conducted before the Hurricanes. There are calls for competency-based hiring and for more concerted effort to promote people based on merit.<sup>26</sup>

The mechanical prescription to “find the problem and fix it” may be too powerful to allow consideration of an alternative strategy.<sup>27</sup> The machine metaphor has guided a century of reform efforts.

The public sector has been organizing, reorganizing, searching for excellence, downsizing, reinventing itself, outsourcing, and hiring competence for years.<sup>28</sup> The Katrina cataclysm offers yet another opportunity for what one government executive called the “Troika of Doom” to move into action: think tanks will sell ideas about improving preparedness to substantively inexperienced political leaders, who then award contracts to favored Washington Beltway companies.<sup>29</sup> What comes out of this largely unexamined churn will be more paper producing, acronym generating, PowerPoint numbing programs for “improving” the nation’s preparedness.

There is another approach to reinvigorating public sector competence and preparedness. It looks first to the spirit of public service rather than the sterility of standards.

---

***Louisiana, Louisiana.***  
***They're tryin' to wash us away.***  
***They're tryin' to wash us away.***

Americans disagree about the rightness of involving American troops in the Terrorism Wars in Iraq, Afghanistan and elsewhere. But practically every American “supports our troops.” There is an admiration, compassion and appreciation for what these warriors have volunteered to do. The military’s warrior ethos does not come solely or even most directly from standards-based training. It comes from an inner belief – reinforced by their leaders and by each other – that what they are doing is right for their nation.<sup>30</sup>

To be effective, the ethos of public sector has to come from a similar source. It cannot be mandated by law, “incentivized” by bonuses, or built in to a program. The

competence of the public administrator is more organic than mechanical. It has to be grown and nourished.

For the next catastrophe – whether hurricane, terrorist attack, or pandemic – Americans are told to be ready to take care of themselves for 72 hours to several weeks before the cavalry arrives. Self-reliance is good counsel for the public sector as well. The responsibility for returning competence to the core of public work rests with individual administrators.

Steven Covey writes about the “circle of influence and the circle of concern.”<sup>31</sup> Public workers have been slimed by the abysmal Katrina response. Those who care about that should be *concerned* about competence in the public sector. But each person has a different *circle of influence*; a different way to contribute to eliminating what Woodrow Wilson called “the poisonous atmosphere..., the crooked secrets..., the confusion, sinecurism, and corruption.”

For a few emergency managers with many years’ experience it might mean a willingness to disrupt their lives and finances to rebuild a federal system that died from neglect. For someone just starting government service, it could be no longer tolerating the co-worker who spends hours everyday checking email and surfing websites. For another person, it could be taking the responsibility to eliminate unproductive meetings. It could be refusing to notionalize the difficult parts of a preparedness exercise, and instead insisting that participants “exercise in the red zone.” It could be creating new ways to work effectively with other agencies, contractors, and the private sector.

---

***Louisiana, Louisiana.  
They're tryin' to wash us away.  
They're tryin' to wash us away.***

A dominant metaphor characterizes each era of public administration’s evolution as a discipline. At first, administrators were artisans, skilled at the public’s business. Next, the competent ones aspired to become scientists, guided by the truth of empirical reality. In the 1960s and 70s, administrators struggled to enact the metaphor of social reformer, looking to improve life. The present era depicts public administrators as managers.

All metaphors eventually lose their power. Katrina convincingly demonstrated the sedentary emptiness of the “public administrator as manager” metaphor. But it is not clear what will replace it.

For a brief time, Katrina had the potential to transform the nation’s expectations about government and the public sector. That time may be gone. In less than four months, the attention of unaffected publics has moved on to other matters.<sup>32</sup> Organizational curtains have veiled the dispirited chaos of the preparedness world. The public sector risks descending further into denial.

Ten years before Wilson wrote his generative public administration essay, Japan’s Tokugawa period came to an end and with it that nation’s feudal society. The social turmoil brought forth *ronin*, samurai who no longer had a master. *Ronin* were forced by their circumstances to think freely, to develop structural independence, and to lead the way to Japan’s new social system.<sup>33</sup>

Public administrators who care about their calling are in an analogous state. Like *ronin*, they too work in a realm that has lost its masters and principled center. Individual

administrators have an opportunity to develop a new ethos of competence by breaking the tradition of psychic feudalism that is the public sector. It requires acting from personal courage instead of personal fear. It requires personal adaptability, autonomy and an insistent excellence.<sup>34</sup> It requires – in Gandhi’s phrase – being the change you want to see.

---

*They're tryin' to wash us away.  
They're tryin' to wash us away.*<sup>35</sup>

The unthinkable is still out there: detonation of a nuclear device, biological attacks, terrorist assaults on schools. Thinkable catastrophes are also visible: a major earthquake in San Francisco, a chemical plant explosion in New Jersey, and Avian flu everywhere. The public sector has a second chance to get better prepared.

Spirit does not return easily. It will take years to return the ethos of competence. It is not obvious that we have that much time. But no one is going to bring competence back except the people who care about the *service* part of public service.

In 1776, Thomas Jefferson wrote:

*Prudence, indeed, will dictate that Governments long established should not be changed for light and transient causes; and accordingly all experience hath shown, that mankind are more disposed to suffer, while evils are sufferable, than to right themselves by abolishing the forms to which they are accustomed.*

Jefferson and the fifty-five other men who signed the Declaration of Independence asserted that whenever any form of government fails to accomplish its basic purposes,

*...it is the Right of the People to alter or to abolish it, and to institute new Government, laying its foundation on such principles and organizing its powers in such form, as to them shall seem most likely to effect their Safety and Happiness.*

What happened after Katrina struck was the insufferable sadness of systemic incompetence. The American people deserve a government and a public service that does not allow that to happen again.

---

<sup>1</sup> National Commission on Terrorist Attacks Upon the United States, *9/11 Commission Report* (New York: Barnes & Noble Publishing, Inc., 2004), 403, 418.

<sup>2</sup> For some examples, see U.S. Congress House Committee on Government Reform, *A First Look at Lessons Learned from Katrina*, September 15, 2005; Bob Herbert, "A Failure of Leadership," *New York Times*, September 5, 2005; Susan B. Glasser and Josh White, "Storm Exposed Disarray at the Top," *Washington Post*, September 4, 2005, A1; Tim Naftali, "Department of Homeland Screw-Up," *Slate*, September 6, 2005.; "Miscommunication Cited In Katrina Response," Associated Press, <http://www.nytimes.com/aponline/national/AP-Katrina-Military.html> (accessed October 12, 2005); Donald F. Kettl, "The Worst Is Yet to Come: Lessons from September 11 and Hurricane Katrina," *Fels Government Research Service Report 05-01* (September 2005); and Pew Research Center, "Two-In-Three Critical Of Bush's Relief Efforts. Huge Racial Divide Over Katrina and Its Consequences," September 8, 2005. The accusations of incompetence continued beyond September 2005: "FEMA still does not know any more about what it was doing last week than it was a month ago," Representative David R. Obey of Wisconsin, the ranking Democrat on the House Appropriations Committee, said. "It is still, as far as I am concerned, an incompetent agency," quoted in Eric Lipton, "Number Overstated for Storm Evacuees in Hotels," *New York Times*, October 19, 2005. <http://www.nytimes.com/2005/10/19/national/nationalspecial/19housing.html> (accessed October 20, 2005).

<sup>3</sup> Initial exceptions include the United States Coast Guard and several responder agencies in Alabama and Mississippi. As response and recovery activities stabilized, individual and agency performance improved.

<sup>4</sup> Woodrow Wilson, "The Study of Administration," *Political Science Quarterly* 2, no. 1 (June 1887), in Jay Shafritz and Albert C. Hyde, *Classics of Public Administration* (Wadsworth Publishing, 1978), 3.

<sup>5</sup> *Ibid.*, 8.

<sup>6</sup> *Ibid.*, 5.

<sup>7</sup> Waldo, Dwight, *The Administrative State*, 2nd ed. (Holmes & Meier Publishers, 1983), Chapter 1; Richard Hofstadter, *Age Of Reform* (Knopf, 1955). The Pendleton Act, adopted in 1883, was the first significant national reform of civil service. Ari Hoogenboom, *Outlawing the Spoils: A History Of The Civil Service Reform Movement, 1865-1883* (University of Illinois Press, 2000).

<sup>8</sup> Robert Biller, "Some Implications of Adaptation Capacity for Organizational and Political Development," in Frank Marini (ed.), *Toward A New Public Administration: The Minnowbrook Perspective* (Scranton: Chandler Pub. Co, 1971), 94

<sup>9</sup> Contrast Hoover's views with those attributed to Mike Brown, former FEMA director, in 2001: "The general idea -- that the business of government is not to provide services, but to make sure that they are provided -- seems self-evident to me." (Jon Elliston, "Disaster in the making," *Independent Weekly*, September 22, 2004, <http://www.indyweek.com/durham/2004-09-22/cover.html>; cited by Charles Perrow, in "Using Organizations: the Case of FEMA," *Homeland Security Affairs* 1, no. 2, (Fall 2005).

<sup>10</sup> See, for example, the four volume work by Arthur M Schlesinger, Jr., *The Age of Roosevelt* (Houghton Mifflin Company, 1959). It has been suggested that Roosevelt only continued the trend of expanding the size of government that began before the Progressive era. See Randall G. Holcombe, "Federal Government Growth Before the New Deal," September 1, 1997 <http://www.independent.org/publications/article.asp?id=360> (accessed October 25, 2006).

<sup>11</sup> Herbert Simon, "The Proverbs of Administration," originally published in 1947, reprinted in Jay M. Shafritz and Albert C. Hyde, eds., *Classics of Public Administration*, 4th ed. (Harcourt Brace, 1997), 127-41. Simon's concerns are echoed in contemporary calls for homeland security metrics.

<sup>12</sup> William H. Whyte, *The Organization Man* (Doubleday, 1956).

<sup>13</sup> Todd La Porte, "The Recovery of Relevance in the Study of Public Organization," in Frank Marini, (ed.), *Toward A New Public Administration: The Minnowbrook Perspective* (Chandler Pub. Co, 1971), 32.

<sup>14</sup> George W. Bush, as David Brooks argues, has not been part of this legacy – either forced by circumstances or directed by philosophy. Brooks quotes Bush that "Government should help people improve their lives, not run their lives," and observes that "This is not the Government-Is-the-Problem philosophy of the mid-'90s, but the philosophy of a governing majority party in a country where people look to government to play a positive but not overbearing role in their lives." David Brooks, "The Savior of the Right," *New York Times*, October 23, 2005 (<http://select.nytimes.com/2005/10/23/opinion/23brooks.html?n=Top%2fOpinion%2fEditorials%20and%20Op%2dEd%2fOp%2dEd%2fColumnists%2fDavid%20Brooks>) (Accessed October 29, 2005.)

<sup>15</sup> For examples, see The Pew Research Center, "How Americans View Government: Deconstructing Distrust," March 10, 1998. Available at <http://people-press.org/reports/display.php3?ReportID=95> (Accessed October 29, 2005).

<sup>16</sup> Gregory B. Lewis & Sue A. Frank, *Public Administration Review* 62, Issue 4 (July/August 2002), 395.

<sup>17</sup> See "Attitude About Public Service" data in The Pew Research Center, "How Americans View Government: Deconstructing Distrust," March 10, 1998, op.cit.

<sup>18</sup> Spencer S. Hsu, "Chertoff Vows to 'Re-Engineer' Preparedness," *Washington Post*, October 20, 2005, A2. Spence S. Hsu, "After the Storm, Chertoff Vows to Reshape DHS. Secretary Pledges to Learn From Mistakes of Katrina," *Washington Post*, November 14, 2005, A11.

<sup>19</sup> David M. Walker, "Managing Human Capital in the 21<sup>st</sup> Century," (Government Accountability Office), March 9, 2000; and Leonard Wiener, "Brain Drain: Half Of All Federal Workers Can Retire In Five Years," *U.S. News and World Report*, November 22, 2004.

<sup>20</sup> Partnership for Public Service and National Academy of Public Administration, "Where the Jobs Are. The Continuing Growth of Federal Job Opportunities," February 2005. Available at [http://www.ourpublicservice.org/publications3735/publications\\_show.htm?doc\\_id=260717&page=1](http://www.ourpublicservice.org/publications3735/publications_show.htm?doc_id=260717&page=1)

<sup>21</sup> The 1998 PEW poll (op. cit.) found little change in numbers of people recommending government service to a child, in a hypothetical. More than half said no. The impact of Katrina on perceptions of government is evident in a September 22, 2005 Pew Research Center survey. More than half the adults polled agreed with the statement "Government is almost always wasteful and inefficient." That represents an increase from 47% in December 2004 to 56% in September 2005.

<sup>22</sup> United States Office of Personnel Management, "What Do Federal Employees Say? Results from the 2004 Federal Human Capital Survey," (no date), available at <http://www.fhcs2004.opm.gov/Published.htm> (accessed October 28, 2005).

<sup>23</sup> David E. Rosenbaum, "Study Ranks Homeland Security Department Lowest in Morale," *New York Times*, October 16, 2005. The story also noted "... in answer to the question "How would you rate the overall quality of work done by your workgroup?" only 22 percent of Homeland Security employees answered "very good." Only 20 percent strongly agreed that "My work gives me a sense of personal accomplishment." Only 27 percent strongly agreed that "people I work with cooperate to get their job done," and 13 percent strongly agreed that "my job makes good use of my skills and abilities." In each of these instances, the department's employees were less positive about their jobs than were workers at any other department or agency in the study."

<sup>24</sup> Quotes from <http://www.stephensonstrategies.com/2005/10/24.html>; see United States Office of Personnel Management Agency (op. cit.), Parts 1 through 5 for specific survey results.

<sup>25</sup> John W. Gardner, *On Leadership* (Free Press, 1993), 1, 2, 48.

<sup>26</sup> Michael Chertoff, "Statement by Homeland Security Secretary Michael Chertoff before the United States House Select Committee on Hurricane Katrina," October 19, 2005. Available at <http://www.dhs.gov/dhspublic/display?content=4896> (accessed November 1, 2005).

<sup>27</sup> For a homeland security-related discussion of how the uncritical application of the machine metaphor can affect policy deliberations, see Richard A. Posner, "The 9/11 Report: A Dissent," *New York Times*, August 29, 2004.

<sup>28</sup> For examples, see David M. Walker, "Managing Human Capital in the 21<sup>st</sup> Century," (op. cit.) <http://govinfo.library.unt.edu/npr/> and <http://www.opm.gov/employ/html/COMPTNCY.HTM>

<sup>29</sup> Comment made by a Department of Homeland Security manager in an off-the-record meeting, September 5, 2005.

<sup>30</sup> Dexter Filkins, "The Fall of the Warrior King," *New York Times*, October 23, 2005; and Dave Grossman, *On Killing* (Back Bay Books, 1996), 291-292. This idea is also captured in a quote from General George C. Marshall: "The soldier is a man; he expects to be treated as an adult, not a schoolboy. He has rights; they must be made known to him and thereafter respected. He has ambition; it must be stirred. He has a belief in fair play; it must be honored. He has a need of comradeship; it must be supplied. He has imagination; it must be stimulated. He has a sense of personal dignity; it must be sustained. He has pride; it can be satisfied and made the bedrock of character once he has been assured that he is playing a useful and respected role. To give a man this is the acme of inspired leadership. He has become loyal because loyalty was given to him."

<sup>31</sup> Stephen R. Covey, *The 7 Habits of Highly Effective People* (Free Press, 1990), 81.

<sup>32</sup> "Forgotten already," (*New Orleans*) *Times-Picayune*, November 13, 2005; Cathy Booth Thomas, "New Orleans Today: It's Worse Than You Think," *Time*, November 20, 2005.

<sup>33</sup> Beverly Potter, *The Way of the Ronin: Riding the Waves Of Change* (Ronin Publishing, 2001), 61.

---

<sup>34</sup> Ibid., p. 68 and 69. See also David Brown, “When Disaster Strikes, You Need To Take Matters Into Your Own Hands,” *Seattle Times*, October 9, 2005. During the Katrina response, there were numerous examples of individuals and groups who violated rules clearly inappropriate for the situation. In one example, helicopter pilots disobeyed their orders in order to save more stranded people. There were also instances where rules were inappropriately obeyed. For example, some volunteer police officers were not allowed to help with the response until they completed a sexual harassment course. There are times when disrupting convention or breaking rules is the right thing to do, and times when it clearly is wrong. People who pick incorrectly face consequences. A more complete discussion of when to obey rules and when to disobey them – and the consequences of following a *ronin* path – goes beyond the scope of this article.

<sup>35</sup> Louisiana 1927, by Randy Newman, *The Boston Globe*, September 7, 2005. [http://www.boston.com/news/globe/editorial\\_opinion/oped/articles/2005/09/07/louisiana\\_1927/](http://www.boston.com/news/globe/editorial_opinion/oped/articles/2005/09/07/louisiana_1927/) (accessed October 29, 2005). “The lyrics ... tell the story of the Louisiana flood of 1927, which killed hundreds and displaced hundreds of thousands across six states. The disaster is credited with sparking one of the great voting movements of the 20th century -- the shift in Southern black allegiance from the Republican to the Democratic Party -- and with spurring the New Deal politics of big government.” See also John. M. Brody, “The Prologue, and Maybe the Coda,” *New York Times*, September 4, 2005. Secretary of Commerce Herbert Hoover was in charge of the 1927 flood rescue activities. His successful efforts helped him get elected to the Presidency in 1928.

# *Homeland Security Affairs*

---

*Volume I, Issue 2*

2005  
2005

*Article 6*

---

## Unified Command and the State-Federal Response to Hurricane Katrina in Mississippi

William L. Carwile\*

\*NPS, carwilewilliam@aol.com

Copyright ©2005 by the authors. *Homeland Security Affairs* is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of *Homeland Security Affairs* or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in *Homeland Security Affairs* rests with the author(s) of the article. *Homeland Security Affairs* is the online journal of the Center for Homeland Defense and Security (CHDS). <http://www.hsaj.org/hsa>

# Unified Command and the State-Federal Response to Hurricane Katrina in Mississippi\*

William L. Carwile III

## Abstract

Unified Command, as a part of the National Incident Management System (NIMS), was successfully used in the state-federal response to the catastrophic disaster caused by Hurricane Katrina in Mississippi in 2005. Four elements to determine the members of a Unified Command include: authority, co-location, parity and common understanding. Modifications made to ICS in the Mississippi response include extending the unified command concept down the chain to facilitate joint decision-making at all levels. Unresolved issues include the role of the Federal Coordinating Officer and Principal Federal Official, federal management of multi-state disasters, and the inclusion of components of the Department of Defense in a Unified Command.

**AUTHOR BIOGRAPHY:** William L. Carwile III served in senior positions for the Federal Emergency Management Agency on major U.S. disasters since 1996, including: the 9/11 World Trade Center response, as Federal Coordinating Officer for the 2003 California Wildfires, Hurricanes Charley, Frances, Ivan and Jeanne in Florida in 2004 and the 2005 Hurricane Katrina disaster in Mississippi. He retired from Department of Homeland Security in 2005. Prior to joining FEMA, Mr. Carwile retired as a colonel after serving 30 years in the US Army in command and operational staff positions in Special Forces, Infantry, and headquarters organizations. He holds a Bachelor of Arts Degree in Political Science from the University of Tulsa, Master Degree in Public Administration from Shippensburg University, Pennsylvania, and is a graduate of the U.S. Army War College. He is currently affiliated with the Naval Postgraduate School's Center for Homeland Defense and Security.

**KEYWORDS:** Unified Command, emergency management, federal-state-local, Hurricane Katrina

---

\*Although the ideas contained in this paper are my own, many individuals have contributed to my understanding of the unified command during actual field operations including W. Craig Fugate, Director, Florida Department of Emergency Management, Robert R. Latham, Director of the Mississippi Emergency Management Agency, and my friend and colleague, Robert Fenton. Thanks to my wife, Anne H. Carwile for assistance in the preparation of this manuscript.

In October 2005, Michael D. Brown, former Undersecretary, Department of Homeland Security for Emergency Preparedness and Response, and Director, Federal Emergency Management Agency (FEMA), testified before a committee of the United States Congress on the federal response to Hurricane Katrina. U.S. Representative William Shuster, (R-PA) in his questioning of former Undersecretary Brown, said:

We've talked a lot about unifying command today and I want to try to get more in detail on that. I think it's, first, important for you to explain to us your view of what the Unified Command looks like to the American people, because I don't think anybody understands what that looks like. We might understand it in military terms but it's different when FEMA is on the ground. So could you give us, sort of, a sketch of what it looks like?<sup>1</sup>

Representative Shuster was correct to characterize a military Unified Command as different from a Unified Command as envisioned by National Incident Management System (NIMS). In the wake of Hurricane Katrina, the need for clear and coherent command arrangements during a disaster response has become obvious. A great deal of emphasis has been placed on the need for a Unified Command to deal with large-scale man-made or natural disasters. Most would agree that a strong local, state, federal, volunteer agency, and private sector partnership is required; however, there is no nationally understood, accepted, and implemented definition of what constitutes a workable Unified Command in a catastrophic disaster.

This article describes the general concepts, background, and history of Unified Command, as well as the use of Unified Command principles in the disaster response to the 2004 Hurricanes in Florida and to the 2005 Hurricane Katrina in Mississippi.

### **Unified Command: General Concept**

A Unified Command is, in its essence, a mechanism to define and achieve a set of objectives in situations where two or more political or functional entities have authorities and/or assets. In a unified command approach, representatives of the entities meet to set goals and decide how each can contribute to the achievement of those goals. There can be strong, formal command and control relationships between and among the entities, as is the case in a military Unified Command, or the command and control linkages can be based on informal but structured arrangements that recognize federal responsibilities and the legal sovereignty of state and local governments under our federalist form of government. In a disaster response involving elected and appointed officials, consensus building and a collaborative approach to problem solving are important aspects of Unified Command.

### **Unified Command in a Military Context**

The initial concept of a Unified Command derives from the military. It is an organizational arrangement in which commanders retain control over their units and assets while supporting the objectives of a larger command. Within the U.S. military, the term and practice of Unified Command have been used for some decades, especially since the National Security Act of 1947, later strengthened by the Goldwater-Nichols Department of Defense Reorganization Act of 1986.<sup>2</sup> The military has a straightforward and simple model to achieve unity of effort where different services work together. Department of Defense (DOD) doctrine defines Unified Command as “a command with a broad continuing mission under a single commander and composed of significant assigned components of two or more Military Departments that is established and so designated by the President, through the Secretary of Defense with the advice and assistance of the Chairman of the Joint Chiefs of Staff.”<sup>3</sup>

Military Unified Commands are made up of units that are assigned to the command through a joint document called the Unified Command Plan (UCP). The general mission is assigned by the President and the Secretary of Defense and in the National Military Strategy is further defined by the Combatant Commander. Within the United States military establishment a Unified Command is characterized by a geographic Area of Responsibility (AOR) which is assigned to a single combatant commander who has the authority to directly assign, or through other command arrangements, two or more “joint” forces from different services – Army, Navy, Marine Corps, and Air Force – within the designated AOR. An example would be the Commander, United States Pacific Command who directs the operations of all U.S. military forces in the Pacific AOR.<sup>4</sup>

Is the military model for Unified Command in any way useful within the context of local, state, and federal response and recovery operations in a domestic disaster? Probably not. Military command implies strong command and control, and the possibility of censure if direction by the combatant commander is not followed. In a civilian disaster response, there is a complex environment of multiple layers of government, each with its own elected and appointed officials responsible to their own constituents. Other, less hierarchical, directive organizational models, based on consensus building, must be developed and adopted.

### **Unified Command in the Fire Community**

After the disastrous wildfires in Southern California in 1970, firefighting agencies came together to form FIRESCOPE (Firefighting Resources of California Organized for Potential Emergencies) and develop the FIRESCOPE Incident Command System. This was later modified and, in 1982, was adopted as the National Interagency Incident Management System (NIIMS).<sup>5</sup> ICS is defined by The National Wildfire Coordinating Group (NWCG) as a “standardized on-scene emergency management concept specifically designed to allow its user(s) to adopt an integrated organizational structure equal to the complexity and demands of single or multiple incidents, without being hindered by jurisdictional boundaries.”<sup>6</sup> Unified Command is the command and control arrangement in incidents where agencies from different jurisdictions are involved. As defined by the NWCG, Unified Command is a part of ICS where “unified command is a unified team effort which allows all agencies with jurisdictional responsibility for the incident, either geographical or functional, to manage an incident by establishing a common set of incident

objectives and strategies. This is accomplished without losing or abdicating authority, responsibility, or accountability.”<sup>7</sup>

The success of the NWCG model for ICS and Unified Command led to its adoption for other disasters like oil spills and medical responses. The Oil Pollution Control Act of 1990 (OPA-90), which was enacted following the Exxon Valdez oil spill, mandates the use of NIIMS/ICS. OPA-90 also mandates that when a spill occurs, the management of the incident will use a Unified Command that includes the responsible federal official, state or local official, and the responsible party. The U.S. Coast Guard, in drafting the bill, included the responsible party because it will be liable for expenses in oil spills and so should participate in the overall management of, and decisions about, the expenditure of funds.<sup>8</sup>

### **Unified Command in the National Incident Management Systems (NIMS)**

In the aftermath of the terrorist acts of September 11, 2001, the President directed Tom Ridge, the Secretary of the newly formed Department of Homeland Security, to develop a plan that would include a comprehensive “all hazard” approach to disaster management. Released in 2003, The National Incident Management System (NIMS) is intended to provide a consistent nationwide approach for federal, state, territorial, tribal, and local governments to work effectively and efficiently together to prepare for, prevent, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. NIMS, parts of which were adapted from NIIMS, embraced ICS and articulated its concepts: common organizational structure and terminology; guidance for building organizations from the bottom up, using rules for establishing an effective span of control; “typing” or categorizing resources; and Unified Command.<sup>9</sup>

NIMS provided the doctrinal basis for the development of a National Response Plan (NRP). In a phased implementation, begun in December 2004, the NRP replaced the 1993 Federal Response Plan as the guidance for federal consequence management operations. The change in nomenclature from “Federal” to “National” was both symbolic of the fact that the NRP was to address not only Federal, but also local, state, volunteer agency, and private sector engagement in disaster responses, and an effort to combine into one document several separate federal plans.

The NRP addresses the “national” engagement in all sorts of hazards, including terrorist events, radiological accidents, oil spills of national significance, and others. Equally important is the fact that it was intended to address both consequence management (response activities to assist states in helping victims of disasters) and crisis management operations (law enforcement activities meant to prevent or apprehend and prosecute terrorists).<sup>10</sup> NIMS provides a standardized approach to incident management; it describes a uniform set of processes and procedures that emergency responders at all levels of government will use to conduct response operations. It is designed to address “all hazards” and addresses each of the dimensions of emergency management: prevention, preparedness, response, recovery, and mitigation. The remainder of this article focuses on response aspect of the NRP.

NIMS defines Unified Command as:

[An] application of ICS (the Incident Command System) used when there is more than one agency with incident jurisdiction or when incidents cross political jurisdictions. Agencies work together through the designated members of the Unified Command, often the senior person from agencies and/or disciplines

participating in the Unified Command, to establish a common set of objectives and strategies and a single Incident Action Plan.<sup>11</sup>

As a technical point, the NRP does not use the term “Unified Command” to describe the joint state/federal partnership in managing the disaster response. The NRP uses the term “Joint Field Office Coordination Group.” NRP says that “Utilizing the NIMS principle of Unified Command, JFO activities are directed by a JFO Coordination Group.”<sup>12</sup> The JFOCG includes federal and state officials with primary jurisdictional responsibility or functional authority; the State Coordinating Officer and the Federal Coordinating Officer are included in this group. While there are differences between a JFOCG and a Unified Command, the term “Unified Command” is used here to describe the group of individuals who sat at a table together and managed the disaster response in Mississippi.

While the NRP focuses on relationships between and among federal agencies during responses to major disasters, it recognizes the lead role of state and local responders. There is no dispute that the state and local officials retain their roles and responsibilities for domestic incident management. According to Homeland Security Presidential Directive (HSPD) 5, “The Federal Government will assist State and local authorities when their resources are overwhelmed, or when Federal interests are involved.”<sup>13</sup> In terms of what form the planning should take, the 2004 introduction of NIMS directed the use of ICS in domestic disaster response.

### **Transition from the FRP to NIMS in major disaster response in the field**

A partial transition to NIMS from the Federal Response Plan model was achieved in Florida by the State-Federal Emergency Response Team in 2004 in the responses to the four presidentially declared hurricane disasters: Hurricanes Charley, Frances, Ivan, and Jeanne. A Unified Command was implemented at the highest level through the partnership and collaborative efforts of the State Coordinating Officer and the State Emergency Response Team, and the Federal Coordinating Officer and the Federal Emergency Response Team.<sup>14</sup>

However, a full ICS response structure was not fully implemented, especially those measures to achieve acceptable spans of control through the use of geographic branches within the operations section. Florida has a robust emergency response system and a long history of successfully responding to hurricane disasters. Many lessons from the four 2004 hurricanes were used in structuring the response to Hurricane Katrina in Mississippi, where the applicable portions of the National Incident Management System and the Incident Command System were used to structure the entire response to a major disaster response for the first time.<sup>15</sup>

### **Who Sits At The Table?**

The participants of a Unified Command can vary depending on the nature of the disaster and may change during the course of a disaster response. Four elements fundamental in determining the personnel to be included in the Unified Command are Authority and Responsibility, Co-location, Parity, and Training and Common Understanding.

**Authority and Responsibility.** Jurisdiction or authority to direct resources that apply to the disaster response is a fundamental prerequisite for members of a Unified Command. Our

federalist system of government provides for the sovereignty of the state in managing a disaster within state borders: the Governor is in charge of the disaster response. The Governor has the ability to delegate authorities to designated individuals: the Governor's Authorized Representative and the State Coordinating Officer. During the 2004 Hurricanes in Florida, Governor Jeb Bush designated Craig Fugate as the Governor's Authorized Representative and Frank Koutnik as the State Coordinating Officer. In Mississippi, in 2005, Robert Latham was Governor Barbour's Authorized Representative and Michael Womack was the State Coordinating Officer.

On the federal side, when the Governor of a state receives a Presidential declaration for a major disaster, the President appoints a Federal Coordinating Officer, whose authority resides in the Stafford Act. The FCO has no authority to direct the state response, but does provide technical assistance, and expertise, and is authorized by the Stafford Act to mission-assign federal agencies, with or without reimbursement, to support the requests of the Governor and his/her representatives.<sup>16</sup> I was the FCO for the response and recovery in the Florida Hurricanes in 2004, and for the first weeks of the response to the Katrina disaster in Mississippi.

**Co-location.** It is important that the members of the Unified Command be able to meet regularly and be available to consult with one another. In the 2004 Florida hurricane responses, Craig Fugate and I were "joined at the hip." We traveled together to the devastated areas after all four storms and sat at the same table during the response phase of the disaster. In the days leading up to and just after landfall of the storms, I operated out of a mobile command center that was located in the parking lot of the Florida State Emergency Operations Center. When briefing Governor Bush, Craig and I did so together. Following landfall in three of the four hurricanes, the state-federal team moved forward to the most impacted counties for both situational awareness and to demonstrate that the unified state-federal command was on hand to assist the local elected and appointed officials.

In 2005, in the response to Katrina in Mississippi, I was similarly aligned with Governor Barbour's Representative, Robert Latham. Pre-landfall, an Initial Operating Facility (IOF) was established at the State Emergency Operations Center (EOC) in Jackson, the state capitol. Following the passing of the storm, Robert and I moved forward to establish a joint IOF in the parking lot of the Harrison County EOC. Our deputies remained in Jackson with the majority of the team to handle the requests for assistance from throughout the impacted areas of the State as well as the requests Robert and I developed from our interface with leaders along the coast. Later, we returned to Jackson, moved the joint emergency response team into a Joint Field Office (JFO), and established a Branch Field Office in Biloxi to manage operations in the six southern counties and the joint division supervisors in those jurisdictions.

Each day, the Unified Command held a morning Strategy Meeting to establish joint objectives for the next operational period and an afternoon Action Planning meeting to determine the adequacy of resources to meet the objectives. This close contact between individuals with decision making responsibilities results in an awareness of each other's actions and facilitates timely decision making.

**Parity: Members should be relatively equal in stature/rank.** The composition of the Unified Command will vary from state to state and with each disaster; however, a basic premise of the Unified Command is that its members be of roughly the same stature in terms of rank or position.

There should not be a large disparity in responsibility or authority between individual members of the Unified Command. This avoids dominance by any member by virtue of his or her relative rank or position.

**Training and Common Understanding.** Under the NIMS, common understanding is achieved through a comprehensive and shared knowledge of the Incident Command System. Members of the Unified Command must be trained and experienced in ICS as well as their assigned positions within the structure. With the directive to adopt NIMS from the Department of Homeland Security, FEMA instituted training in ICS for emergency managers.<sup>17</sup> State emergency management officials in Mississippi participated in NIMS training in the summer before Hurricane Katrina struck the coast. The FEMA emergency response team sent to Mississippi contained individuals who were involved in the FEMA ICS doctrinal and training program development. This training, and the experience of the federal emergency managers, proved invaluable in the rapid adoption of ICS, the establishment of the Unified Command, and the development and implementation of the Incident Action Planning process in Mississippi.

### **Who Sits At The Table In A Unified Command?**

Individuals with primary authority – the Governor’s Representative, the State Coordinating Officer and the FCO – are the core of the Unified Command. Depending on the nature of the disaster, others from the state, such as the Adjutant General, or from the federal side, the Defense Coordinating Officer, might join the command. In Florida, the Unified Command consisted of Craig Fugate and me as the FCO. In Mississippi, Robert Latham, the Director of the Mississippi Emergency Management Agency, his Deputy Director, Michael Womack, and I, as the Federal Coordinating Officer served as the three initial members of the command. Later, the Adjutant General and the Commissioner of Public Safety were added as full members of the Unified Command and participated in the action planning-cycle meetings. They were added to the leadership team because their assets were critical to the overall success of operations and had to be fully integrated into the overall effort. On the federal side, the Defense Coordinating Officer also sat in on the Unified Command meetings.

### **Joint Incident Action Planning**

In ICS doctrine a major function of the Unified Command is the “action planning process” to develop an Incident Action Plan. The joint Incident Action Plan is the engine that drives the response/recovery effort. In Mississippi, each day began with a Strategy Meeting in which the Unified Command, joint Operations Section Chiefs, joint Logistics Section Chiefs, and other supporting groups established the joint state-federal objectives for the operational period. The strategy meeting was followed by a joint Operations-Logistics meeting to coordinate the necessary measures to accomplish the objectives. Later in the day, a joint Action Planning meeting was held to finalize the objectives for the next operational period. Mississippi’s joint Incident Action Plan contained ICS forms 202 (incident objectives and Area of Responsibility map), 203 (organizational list), 204 (assignment list), 205 (communications plan), 207 (organization chart), and 220 (air operations worksheet). All of these proved extremely valuable in guiding response/recovery operations.<sup>18</sup>

Requests for resources were developed by the local emergency managers and relayed to the Operations Section of the Unified Command in Jackson. In the most-devastated counties, unified State-Federal Division Supervisors assisted county emergency managers and elected officials in identifying priority resource requirements. Based on the joint operational objectives, the unified Operations Section coordinated the most effective way to fill the requirements: State, Emergency Management Assistance Compact (EMAC), volunteer agency, or federal (FEMA or one or more Emergency Support Functions) resources were considered. The resource identified to meet the local requirement was requested through an Action Request Form (ARF). If Federal resources were selected, one or more Emergency Support Functions were ‘mission assigned’ or FEMA bought or provided available resources. The resources were coordinated with the State for distribution to the requesting jurisdiction and/or geographic branch of the Operations Section. Resources were tracked using the Joint Assignment List, ICS form 204.

### **Modifications to ICS in the Hurricane Katrina Response**

In “pure” ICS, as practiced by the fire service for example, the Unified Command exists only at the highest level. The sections, branches, and divisions below the Unified Command are directed by the most qualified member in that unit of the organization. In the response to the Hurricane Katrina disaster in Mississippi, we found this aspect of the ICS did not fit our organizational needs for this joint state-federal response. We realized that there was a need for “Unified Command” up and down the organization in order to address political and operational realities, and the fact that there might be no local “incident commander” with the capabilities to field a coherent response.

ICS, in its original configuration, is based on a “bottoms up” approach in which the local Incident Commander and his/her Incident Management Team develop an incident action plan and request required resources. In a catastrophic event this is impossible if the people at the “bottom” are overwhelmed and unable to fully form coherent response organizations. One of the modifications we made to the basic ICS was to have joint section chiefs in each of the ICS sections – one chief from the state and an equal chief from FEMA (a “Unified Command” at the section level). These two individuals worked together to accomplish the goals assigned to their section and reported jointly to the FCO/SCO Unified Command. We extended this “Unified Command” concept to the geographic branch directors and the division supervisors in the local areas.

The 2005 Katrina response in Mississippi was the first time joint division supervisors were co-located with emergency managers at the county level consistent with ICS doctrine. During the 2004 responses in Florida, FEMA liaisons were placed in some critical counties; this was primarily to provide advice to the local officials. County liaisons were just “liaisons” and did not have the authority to direct state or federal resources. Establishing joint geographic Branch Directors and Division Supervisors worked extremely well. “Pure” ICS may work well for fires and smaller disasters, but some substantial modifications are required for large scale events.

### **Communication of objectives**

Under ICS doctrine, joint operational objectives are determined by the Unified Command and articulated to key members of the State-Federal Response Team down the chain using the Incident Action Plan. It is important that every level in the chain understand the joint goals and that level's role in achieving those goals. The objectives passed to the branch directors and division supervisors serve to facilitate the planning efforts of the Unified Commands at that level. In Mississippi, the objectives were also highlighted during press conferences held by Governor Barbour, with the participation of the SCO, the FCO, and other appropriate state and federal officials. A critical piece of the joint Unified Command is consistent, coordinated public messaging. In both Florida and Mississippi, a Joint Information Center (JIC) was established early to ensure consistent messages were going out to the public.

### **Span of control**

One of the features of ICS is the decentralization of decision making; once the priorities have been set and communicated to the branches, the joint branch directors then have the authority to make decisions to support the priorities. ICS guidelines recommend that a manageable span of control is one supervisor to five to seven subordinates. Under the FRP, the span of control was much higher resulting in centralization of control and an unworkable number of "direct reports" to the FCO. One important point: ICS requires more personnel in leadership positions than the former FRP organization. Despite a shortfall in FEMA leaders, an acceptable span of control was achieved in Mississippi through the use of personnel from other federal agencies such as U.S. Forest Service and Bureau of Land Management. These individuals are often trained in ICS as a part of their primary jobs and performed well in the NIMS response.

### **Issues for Discussion**

Based on my experiences in Florida during the four hurricanes of 2004 and in Mississippi during Katrina in 2005, several issues regarding Unified Command were unresolved.

#### **Unified Command in a domestic disaster: Authority**

Unified Command in a disaster like Hurricane Katrina is different than Unified Command in a military or firefighting setting in that many of the participants are elected officials who may have diverse objectives and constituents. In a Unified Command with strict command relationships, an incident commander who acts outside the objectives and goals of the Unified Command is subject to censure. This is not the case in domestic disasters where elected officials have agendas that might not align completely with the objectives of the overall Incident Action Plan. Thus, the success of domestic response operations requires that all parties agree to cooperate and support not only the joint objectives, but the methodology to achieve those objectives. I believe that in Mississippi this was achieved, for the most part, because objectives were based on the priorities of the local officials; and they understood their concerns were being heard and acted upon, even in the face of resource shortages.

How does the “Unified Command” actually work when there are no well-defined lines of authority like those that underlie the Department of Defense’s definition of the Unified Command structure? A clear vesting of authority in emergency managers is vital for the formation and functioning of an effective Unified Command. Florida Governor Jeb Bush in his testimony before the Senate Committee on Homeland Security, said

Florida’s team is led by a Unified Command, to coordinate efforts, share resources, make decisions and provide direction with one voice. During a disaster, I designate Craig Fugate, Director of Emergency Management, to serve as the chief coordinating officer of our state response. I delegate statutory authority to him so he can do his job effectively and report directly to me.<sup>19</sup>

Governor Bush established his vision for an effective Unified Command and provided the requisite legal authority to empower his representative to direct state operations. Similarly, the Stafford Act gives authority to the FCO; the authority of the FCO comes directly from the President and that authority is vested in the FCO when the appointment is recorded in the Federal Register as part of the disaster declaration. In some states, the State Constitution gives considerable authority to local jurisdictions; this can make things a bit murky when attempting to establish hierarchical arrangements in a Unified Command.

### **FCO as a member of the Unified Command**

In defining the Unified Command in a disaster response, the NRP does not include the FCO as a member, but says “The FCO assists the Unified...Command.”<sup>20</sup> It is my belief this view should be revisited. Despite the fact that the FCO may not have “command authority” in the state, he/she has the responsibility to oversee the use of federal resources in the disaster operations. This commitment of federal resources is significant and decisions must be coordinated and synchronized with the overall effort in a timely manner – this is the function of a Unified Command. If, in a catastrophic event, the federal government is to “push” resources down to the state, rather than waiting for requests, it is imperative that the senior federal official with responsibilities for the commitment of resources have a “seat at the table” in a unified command structure. In both Florida and Mississippi, the priority was on the victims and the Unified Command, under the leadership of the state governors, performed well in coordinated and directed operations. In my experience, a federal-state joint Unified Command facilitates timely and effective decision making.

### **Unified Command in a disaster: Multi-state disasters**

Katrina exposed a weakness in the National Response Plan: there is no specific discussion of multi-state disaster management options. Hurricane Katrina impacted three states and each state received a separate disaster declaration from President Bush. As called for in the Stafford Act, the President appointed three federal coordinating officers, one for each state that received a declaration.

There were large differences in the response to the three disasters that arose in part from the extent and nature of the damage, the ongoing flooding in Louisiana, the differences in jurisdictional authority, the use of federal troops in Louisiana, and, I believe, in the use of ICS

and Unified Command in Mississippi. Initially, each response was separate and federal resources were managed by the Emergency Response Team (ERT) in the Emergency Operation Center in each state.

On Sept 3, a Principle Federal Official (PFO) was appointed by Department of Homeland Security Secretary Michael Chertoff to cover all three disasters.<sup>21</sup> Based on my understanding of the NRP and my training as a member of the PFO cadre for DHS, I did not feel that the appointment of a PFO affected the authority or mandate as FCO in any way. Reports were sent to the PFO to give him situational awareness regarding developments in Mississippi.

The position of PFO was created by HSPD-5 in 2003. By NRP definition

[The] PFO is personally designated by the Secretary of Homeland Security to facilitate Federal support to the established Incident Command System (ICS) Unified Command structure and to coordinate overall Federal incident management and assistance activities across the spectrum of prevention, preparedness, response, and recovery. The PFO ensures that incident management efforts are maximized through effective and efficient coordination. The PFO provides a primary point of contact and situational awareness locally for the Secretary of Homeland Security.<sup>22</sup>

More specifically, the PFO does not become the Incident Commander, nor direct or replace the incident command structure. He also does not have directive authority over the Senior Federal Law Enforcement Officer (SFLEO), Federal Coordinating Officer (FCO), or other federal and state officials.<sup>23</sup>

On September 21, the Presidential appointments of the three Federal Coordinating Officers were terminated and the PFO was appointed FCO for each of the three states.<sup>24</sup> While I continued to perform most of the duties of the FCO in Mississippi, my authority as a member of the Unified Command became problematic. Under Unified Command principles, participants must be co-located and should be the primary holders of legal authority.

This situation highlights the complex command and control issues associated with multi-state-federal response operations within the context of our Federalist system of government. As there is a high likelihood of disasters that can strike across state borders, whether due to a terrorist event, a tsunami on the West Coast, an earthquake on the New Madrid fault, or a pandemic flu, this important subject must be addressed. The position of FCO is clearly intended by the Stafford Act to provide an individual to serve as the President's representative to the Governor in one state. The NRP, building on HSPD-5's designation of the Secretary of Homeland Security as the President's "principal federal official" for domestic security, lists several responsibilities for a designated PFO. Most of these revolve around providing situational awareness, coordinating federal efforts, and serving as senior spokesperson. The PFO currently has no operational authority under the NRP.

During Hurricane Katrina operations, there were efforts to designate one federal official as the individual in charge of federal operations in the three states impacted most significantly by the storm. These efforts were not entirely successful. They highlighted the need for serious discussion of how the federal response should be most effectively managed in a multi-state catastrophic disaster. Is there a need for a level of federal organization, above the state level, to coordinate the response over state borders? Should this be a federal oversight organization, or a

regional group that includes representatives of the impacted areas, or an organization of federal agencies to coordinate resources much like the National Interagency Fire Center in Boise does for large wildfires?

In my opinion, what is really needed in a multi-state operation is not a single entity to direct operations in two or more states; each state should be assigned an independent FCO to work directly with the Governor and his/her representatives. A multi-state disaster scenario requires, on the federal side, an adjudicator of resource conflicts and a provider of situational awareness for the National leadership. I believe the organizational level of Area Command within ICS may provide a useful model on which to base discussions.

Any discussion of multi-state management of disaster response will require discussion with the states. In my experience, while state leaders are very supportive of one another during disasters, they would not like to be part of a “regional approach” that in any way inhibits direct dialog with the national leadership in Washington. Additionally, most state leaders believe that their states have unique circumstances that warrant individual attention and solutions.

### **Role for the Department of Defense**

Does the Department of Defense fit into the Unified Command? Should they have a seat at the table from the beginning? The federal military has substantial assets that should be called upon in a catastrophic disaster. A DOD representative, the Defense Coordinating Officer, is pre-designated and, when a major disaster is declared by the President, he or she is assigned to the Emergency Response Team to coordinate the use of DOD assets.<sup>25</sup> A seasoned DCO and his staff, the Defense Coordinating Element, were present in the Mississippi joint state-federal Emergency Response Team during the Hurricane Katrina Response. The DCO sat in on all Unified Command meetings. Active duty military troops under Joint Task Force Katrina were not deployed to Mississippi. Some small active duty units, such as the USN Seabees, were stationed in the state when the Hurricane Katrina struck and played a role in the response. Under EMAC, the deployment of significant numbers of National Guard resources from other states provided the Adjutant General of Mississippi with adequate forces to accomplish his assigned missions. Because of this, the DCO was not considered a full member of the Unified Command leadership in Mississippi.

U.S. Northern Command, established in 2002, has, in addition to its homeland defense mission, also the mission of coordinating and providing active-duty defense support to civil authorities.<sup>26</sup> In the event that active duty Title 10 forces are needed in the state to assist in the response, a DOD representative should be a full member in the Unified Command leadership. Well beforehand, however, there needs to be clarification about the interface between the National Guard command and NORTHCOM. Should only one officer, representing both the National Guard and active duty forces, be a part of the Unified Command? Or could both the Adjutant General and a senior active duty officer representing NORTHCOM simultaneously be members? Unity of effort and unity of command are both principles of war, and important operational features of successful military command and control relationships; this would also be true in a disaster response in which military forces are involved. Scott Wells, the FCO in Louisiana for the Hurricane Katrina Disaster, during testimony on December 8, 2005 before the Senate Committee investigating Hurricane Katrina, characterized the active duty military as an

“800-pound gorilla” that brought tremendous resources but operated independently.<sup>27</sup> For this reason, the command relationship between National Guard and Title 10 commanders should be worked out prior to any deployment of Federal forces. These relationships should not only be well understood, but also practiced in exercises before a large disaster strikes. In this case, it would be appropriate for the military commander(s) to be a full partner with the FCO and the SCO in determining the IAP and goals for the response. The Governor of the state would remain in charge.

### **The response in Mississippi**

Anyone who followed the news on the Katrina response in Mississippi realized that in the immediate wake of the disaster there were problems with the delivery of commodities such as ice, water, and MREs (Meals Ready to Eat).<sup>28</sup> A detailed look at this aspect of the disaster response revealed that this was primarily a result of the condition of the roads leading into the devastated areas and the inability of FEMA logistics to deliver the amount of commodities requested. However, the ICS and Unified Command structure handled requests from the field and had visibility over resources that arrived in the staging areas. ICS and Unified Command, especially with the modifications made in Mississippi, worked well and should be part of any disaster response. If sufficient commodities had been received in a timely manner, this aspect of the response would have been viewed as a success.

Former Undersecretary Brown expressed his frustration that in the initial response to the Katrina disaster in Louisiana there was no Unified Command established in that state.<sup>29</sup> I have not commented on the Katrina response in Louisiana; that response presented some very serious challenges to the emergency managers because of the ongoing flooding due to the levee break and the large number of people trapped and later displaced by the flooding. A study of the Louisiana operations could elucidate decisions made in the early hours and days of the disaster that resulted in differences between the response in Mississippi and in Louisiana.

### **Conclusions**

Hurricane Katrina provided the first major test of NIMS, the NRP, ICS, and Unified Command. In Mississippi, the Unified Command system worked well in reducing the chaos of this catastrophic disaster. A major factor in the success was the prior ICS and NIMS training of the individuals in the Unified Command and their staffs.

Hurricane Katrina, much like Hurricane Andrew in 1993, has the potential to make an indelible imprint on the manner in which America responds to large scale, multi-jurisdictional disasters. As the various hearings and public dialogue continue, I believe, based on my experiences with the very strong State of Florida emergency team during the four hurricanes of 2004 and participation in the 2005 State of Mississippi-Federal partnership, there are important lessons to be learned in achieving workable inter-governmental organizational structures.

A doctrine for large scale domestic response and recovery operations, especially in multi-state disasters, must be developed. Hurricane Katrina operations in Mississippi were far from perfect, but the use of the ICS, the Unified Command, and the partnership of state and federal

responders, down to the lowest levels, provided a functional tool to allocate the available resources in a way that minimized overlap and met the objectives of the joint incident action plan.

The next step is to re-examine the National Response Plan in light of the political and strategic realities of operating in a “really big one.” In a catastrophic event, either man-made or natural hazard, there will be pulls and tugs from many directions – elected and appointed officials of sovereign jurisdictions, the media, the leadership in Washington – in an environment of managing shortages. The organizational models contained in the NRP do not address these realities. Much work needs to be done on developing more useful models, perhaps based on a Unified Command, that will work in highly complex and politically charged catastrophic disaster operations.

---

<sup>1</sup> Michael D Brown, Former Director, Federal Emergency Management Agency, U.S. Department Of Homeland Security, *Testimony to the House of Representatives Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*, October 27 2005.

<sup>2</sup> *National Security Act*, July 26, 1947 (PL 235 - 61 Stat. 496; U.S.C. 402); *Goldwater-Nichols Department of Defense Reorganization Act*, October 1, 1986 (PL 99-433)

<sup>3</sup> *Department Of Defense Dictionary of Military and Associated Terms* (Government Printing Office, Joint Pub 1-02 DOD, 12 April 2001; as amended through August 2005.)

<sup>4</sup> Ibid.

<sup>5</sup> *A History of the Incident Command System (ICS)*, National Wildfire Coordinating Group Incident Command System (ICS), National Training Curriculum, October 1994. <http://www.nwccg.gov/pms/forms/compan/history.pdf>; NIMS Integration Center, “NIMS ICS Position Paper,” November 18, 2004.

<sup>6</sup> National Wildfire Coordinating Group, *Glossary of Wildland Fire Terminology*, PMS 205 (January 2005). <http://www.nwccg.gov/pms/pubs/glossary/pms205.pdf>

<sup>7</sup> Ibid.

<sup>8</sup> *Oil Pollution Control Act of 1990* (Public Law 101-380 and numerous amendments. 33 U.S.C. 2701); Jim Stumpf, “Incident Command System: The History and Need,” *The Internet Journal of Rescue and Disaster Medicine*, 2, No. 1 (2001). <http://www.ispub.com/ostia/index.php?xmlFilePath=journals/ijrdm/vol2n1/ics.xml>

<sup>9</sup> U.S. Department of Homeland Security, *National Response Plan*, December 2004

<sup>10</sup> Homeland Security Presidential Directive 5 (HSPD-5), February 28, 2003.

<sup>11</sup> U.S. Department of Homeland Security, *National Incident Management System*, March 1, 2004.

<sup>12</sup> U.S. Department of Homeland Security, *National Response Plan*, December 2004, 33

<sup>13</sup> HSPD-5.

<sup>14</sup> Craig Fugate and William Carwile, “Unified Command: A Coordinated Response Strategy by the State of Florida and FEMA to Cope with Four Major Hurricanes,” Presentation to the 2005 National Hurricane Conference, March 23, 2005, New Orleans; Michael Brown, Interviewed by Larry King, *Larry King Live: Coverage of Hurricane Frances*, CNN aired September 4, 2004. Director of FEMA Michael Brown states “.... What Governor Bush has set up down here through his emergency management operation is something that I want to take across the entire United States. We have a unified command here between the state government and the federal government. What you see behind me is this command center and the state and federal partners are together.”

---

<sup>15</sup>William Carwile, "Unified Command Made a Difference in Mississippi: Guest Opinion," *Jackson Clarion Ledger*, October 16, 2005, <http://www.msema.org/newsreleases/documents/UnifiedCommandMadeaDifferenceinMississippi.doc>; William Carwile, testimony to the U.S. Senate Committee on Homeland Security and Governmental Affairs, "Hurricane Katrina: Perspectives of FEMA's Operations Professionals," December 8, 2005

<sup>16</sup>*Robert T. Stafford Disaster Relief and Emergency Assistance Act*, as amended by Public Law 106-390, October 30, 2000 (§ 5143. Coordinating Officers {Sec. 302}).

<sup>17</sup>NIMS Integration Center. [www.fema.gov/nims](http://www.fema.gov/nims)

<sup>18</sup>Forms available from the National Wildfire Coordination Group Website at [www.nwcg.gov](http://www.nwcg.gov), and also at [www.fema.gov/nims](http://www.fema.gov/nims) or [www.nimsonline.com](http://www.nimsonline.com).

<sup>19</sup>Jeb Bush, Governor of State of Florida, Testimony before the House Committee on Homeland Security: "Federalism and Disaster Response: Examining the Roles and Responsibilities of Local, State, and Federal Agencies," October 19, 2005.

<sup>20</sup>U.S. Department of Homeland Security, *National Response Plan*, December 2004, 34.

<sup>21</sup>Office of the Press Secretary, Department of Homeland Security, "Update: United States Government Response to the Aftermath of Hurricane Katrina," September 3, 2005.

<sup>22</sup>*National Response Plan*, 33

<sup>23</sup>*Ibid.*

<sup>24</sup>Federal Register notices, Sept. 21, 2005: FEMA-1604-DR, Mississippi; Amendment No. 4 to *Notice of a Major Disaster Declaration*; FEMA-1603-DR, Louisiana; Amendment No. 3 to *Notice of a Major Disaster Declaration* [FEMA-1605-DR], Alabama; Amendment No. 5 to *Notice of a Major Disaster Declaration*.

<sup>25</sup>Department of Defense Directive 3025.16, *Military Emergency Preparedness Liaison Officer (EPLO) Program*, December 18, 2000.

<sup>26</sup>James Russell, "NORTHCOM to Coordinate DOD Role in Homeland Defense" (Monterey, CA: Center for Contemporary Conflict, Naval Postgraduate School, 2002).

<sup>27</sup>Scott Wells, Federal Coordinating Officer, Testimony to the U.S. Senate Committee on Homeland Security and Governmental Affairs: "**Hurricane** Katrina: Perspectives of FEMA's Operations Professionals," December 8, 2005.

<sup>28</sup>Associated Press, "Officials' Memos After Storm Vividly Spell Out Their Fears," *New York Times*, December 7, 2005; William Carwile, White Paper, "Hurricane Katrina: Mississippi 'In Preparation'"

<sup>29</sup>Michael D Brown, Testimony, October 27, 2005.

# *Homeland Security Affairs*

---

*Volume I, Issue 2*

2005

*Article 7*

2005

---

## Hurricane Katrina as a Predictable Surprise

Larry Irons\*

\*lirons@teleologic.net

Copyright ©2005 by the authors. *Homeland Security Affairs* is an academic journal available free of charge to individuals and institutions. Because the purpose of this publication is the widest possible dissemination of knowledge, copies of this journal and the articles contained herein may be printed or downloaded and redistributed for personal, research or educational purposes free of charge and without permission. Any commercial use of *Homeland Security Affairs* or the articles published herein is expressly prohibited without the written consent of the copyright holder. The copyright of all articles published in *Homeland Security Affairs* rests with the author(s) of the article. *Homeland Security Affairs* is the online journal of the Center for Homeland Defense and Security (CHDS). <http://www.hsaj.org/hsa>

# Hurricane Katrina as a Predictable Surprise\*

Larry Irons

## Abstract

The concept of predictable surprises, i.e. failures to take preventative action in the face of known threats, was outlined by Max Bazerman and Michael Watkins in their book by the same name. This paper discusses predictable surprises as primarily organizational events that result from failure of organizational processes to support surprise-avoidance rather than surprise-conducive actions by individual members. The analysis contends that learning organizations are characterized by processes that support surprise-avoidance. The affective heuristic is useful to prevention studies since it points to aspects of social cognition that are central to envisioning consequences for low probability events. Surprise-avoidance organizational processes are central to using the affective heuristic to bolster rational decision-making.

The paper asks whether the preparation and response of federal agencies in New Orleans to Hurricane Katrina was a predictable surprise. The discussion examines the role of the U.S. Army Corps of Engineers in preparing the levee protection system, asking whether its organizational processes supported surprise-avoidance, or were surprise-conducive. FEMA's Katrina response is also reviewed with the same concerns. The actions of each agency are considered along four characteristic traits of predictable surprises. The study offers several policy proposals, some presented by the Secretary of Homeland Security and others stemming from insights developed in the current analysis.

**AUTHOR BIOGRAPHY:** Larry R. Irons received his Ph.D. degree in sociology from Washington University, St. Louis. He consults with companies on issues of organizational intelligence, organizational learning, and learning communities. Larry is currently a Senior Fellow with the Institute for Preventive Strategies.

**KEYWORDS:** Predictable Surprise, organizational learning, affective heuristic

---

\*The author expresses his appreciation to the anonymous reviewers of Homeland Security Affairs, and for the comments offered by Philip Palin, Craig Baldwin, and John Bowen of Teleologic Learning.

## INTRODUCTION

How can a surprise be predictable? Paradoxically, many people think low-probability events are just that: low probability; not impossible but very unlikely. People find it difficult to sustain a high level of preparedness for events that are unlikely to happen on any given day, especially if the preparation requires spending scarce time and resources. As Max H. Bazerman and Michael D. Watkins observe in their recent book, *Predictable Surprises: The Disasters You Should Have Seen Coming, And How To Prevent Them*, “We don’t want to invest in preventing a problem that we have not experienced and cannot imagine with great specificity.”<sup>1</sup>

We all share a cognitive trait that inclines each of us, as individuals, to take the risk not to invest sufficient time and resources in the present to prevent a large, but low-probability, loss in the future, and choose instead to take smaller, certain losses in the present by investing less in preventative efforts. As a result, spending on prevention is too often minimized until the threats are more tangible, until people can imagine their results. At that point, it is often too late to avoid a large loss.

In an effort to understand these dynamics in the perception of risk, researchers in risk perception and risk communication explicitly address the interplay of rationality and emotion in peoples’ decisions about risk. Traditionally, the study of risk assumed that emotion (the affect) limits the degree of rationality in a decision-making process. It was assumed that emotion predisposes us to make one decision rather than another based on our perceptions of good or bad consequences. However, there is another side to the point.

Researchers in risk communication sometimes refer to the phenomena as an *affective heuristic* that can either limit rational decision-making, or enhance it.<sup>2</sup> By *affect*, we mean letting emotions about what is *good* or *bad* drive us in assessing the risk of doing something one particular way rather than another way. *Heuristic* means using those emotions as a rule of thumb for guiding the choices we make rather than having those emotions drive our choices. Therefore, following a hunch or gut instinct based on experience or professional judgment, though sometimes posing difficulty for planning and coordination can in principle enhance rational decision-making rather than limit it. The key question is how organizations can use the affective heuristic to enhance rational decision-making, and how it sometimes works against rational decisions.

We have all heard the Monday morning quarterbacking retort often made by people in charge when other people criticize decisions that went wrong. In fact, some of the official responses to efforts to understand how government at all levels prepared for, and responded to, Hurricane Katrina seem to echo the retort that criticisms are just Monday morning quarterbacking.<sup>3</sup> Yet reluctance to assess decisions can result in a failure to learn from poorly thought out choices, where emotion limited rather than enhanced the rationality of the chosen course of action. Bazerman and Watkins believe it is possible to develop criteria for deciding whether a surprise was predictable, and envisioned, but not acted on preventatively.

The analysis here asks whether the definition of a “predictable surprise” is applicable to Hurricane Katrina and its aftermath in New Orleans. It is not obvious that the event meets the criteria for the characterization, though at first glance most people probably assume it does. Bazerman and Watkins define a predictable surprise in the following way:

Unlike an unpredictable surprise, a predictable surprise arises when leaders unquestionably had all the data and insight they needed to recognize the potential for, even the inevitability of, a crisis, but failed to respond with effective preventative action.<sup>4</sup>

Our key focus is whether the impact of Katrina on the New Orleans levee system was predictable, along with an associated concern about whether the federal preparedness of the levee protection system by the U.S. Army Corps of Engineers, and response to the catastrophic disaster by FEMA, were surprising. Bazerman and Watkins outline four major characteristic traits of predictable surprises.

1. Leaders know problems exist and will not solve themselves.
2. Organizational members realize a problem is getting worse.
3. Fixing the problem requires significant cost in the present with no immediate benefit (rewards for avoiding the costs of prevention are uncertain but potentially larger than incurring the costs).
4. Humans tend to maintain the status quo if it functions (minorities protect their own interests, subverting efforts by leaders to implement change).<sup>5</sup>

We will consider each point in detail in the following discussion, and assess the fit of each to the planning for, and response to, the devastation from hurricanes like Katrina. The key analytic goal here is to outline organizational innovations that exhibit the capacity to address the most serious shortcomings evident in the federal preparation for, and response to, Hurricane Katrina. The organizational goal is to increase the likelihood that, in the future, representatives of federal agencies in catastrophic disaster situations, i.e. FEMA and the Corps of Engineers, will effectively collaborate with state and local officials as well as the private sector. The emphasis is on how *federal* agencies initiate and maintain support and collaboration since, by definition, a catastrophic disaster overwhelms local and state resources.

Bazerman and Watkins contend leaders can encourage surprise-avoidance or surprise-conducive organizational processes. The analysis below outlines the relevance of each type of organizational process to the key federal agencies involved in the Hurricane Katrina disaster, the U.S. Army Corps of Engineers and FEMA. Surprise-avoidance, as outlined by Bazerman and Watkins, is a characteristic goal of learning organizations.<sup>6</sup>

### **Learning Organizational Processes and Surprise-Avoidance**

A range of investigations is underway regarding the preparedness of the levee system to survive a Category 3 hurricane, including the Army Corps of Engineers’ study of its own design and maintenance preparations, with the American Society of Civil Engineers overseeing.<sup>7</sup> The

original legislation in 1965 that authorized the hurricane protection project was only intended to protect against Category 3 hurricanes, expected every 200-300 years.<sup>8</sup> In addition, Team Louisiana (a state sponsored team of academics and independent engineers), U.S. Senate and House committees, the Louisiana Attorney General, the FBI, and the National Science Foundation are involved. As the investigations continue, observers indicate that the failure of the levees points to issues in the way they were designed and prepared by the Corps of Engineers. Observers note that the Corps of Engineers failed to recognize the relevance of basic design and maintenance flaws, contending the oversight speaks to the institution itself as much as to the design of the levees. Combine that position with the common understanding that FEMA failed to mount an effective response to Hurricane Katrina and the organizational attributes of federal preparedness and response efforts in New Orleans become important concerns.

One basic lesson to learn from Hurricane Katrina is that organizations managing preparedness for flood control and hurricanes, such as the U.S. Army Corps of Engineers, as well as organizations managing responses to disasters, such as FEMA, can benefit from developing learning organizational processes. Those same processes make it more likely that staff will avoid surprises by recognizing them, prioritizing the challenges, and mobilizing resources to prevent them from developing.

Humans tend to take risks more seriously when the outcomes are vivid to us.<sup>9</sup> Bazerman and Watkins argue that the challenge of leadership is to “provide the vision for change, even when the need is not yet vivid.”<sup>10</sup> They emphasize the importance of leaders encouraging staff to remain aware of the conditions underlying predictable surprises, by providing organizational processes designed to “recognize emerging threats, prioritize action, and mobilize available resources to mount an effective preventative response.”<sup>11</sup>

A basic step in preparing an organization to use the affect of its people to enhance their efficiency and effectiveness is for its leadership to admit that it is not perfect, that operations require continuous improvement. Professional criticisms of operational performance must flow up the organization as well as down, with the organization encouraging such contributions. Indeed, a learning organization does the following:

- defines a clear mission, designed to inspire workers to do their best;
- creates a culture that emphasizes professionalism;
- provides top-notch technical training;
- provides leadership development for managers;
- pushes responsibility down the ranks so employees in the field are authorized to act quickly; and
- advocates continuous improvement.<sup>12</sup>

Learning organizations are challenged to promote a level of awareness sufficient to enable surprise-avoidance capability from their members. Indeed, the structure of large and complex organizations increases the difficulty leaders’ face in anticipating predictable surprises.<sup>13</sup> As the complexity of organizations, or even project teams, increases, the way expertise is coordinated tends to develop into silos. Organizational silos often disperse responsibility as well as information.<sup>14</sup> In other words, organizational silos encourage staff to “let someone else” deal with recognized problems, essentially supporting surprise-conducive processes.

The following discussion makes the point that surprise-conducive processes are one likely result of diminished professional identity in organizations like FEMA and the U.S. Army Corps

of Engineers. Developing surprise-avoiding processes means providing staff with the authority and resources to make decisions and an organizational hierarchy that listens for informed, professional judgments from subordinates, especially those in the field preparing for, or facing, challenges posed by the threat of disaster. This analysis begins with a discussion of what the leadership at the federal, state, and local levels knew about the vulnerability of the New Orleans levees.

### **Leaders know problems exist and will not solve themselves**

Leadership, as noted above, is a key point of interest when considering the way organizations attempt to avoid, or mitigate the impact of, predictable surprises. There is little dispute of the point that local, state, and federal leaders knew about the vulnerability of the New Orleans' levee protection system and the threats it posed to the city.<sup>15</sup> Although some officials initially claimed that no one expected the levees and floodwalls in New Orleans to collapse, most experts knew about the vulnerability for many years. Indeed, the *Houston Chronicle* ran a story in December 2001 by Eric Berger offering the following assessment.

New Orleans is sinking. And its main buffer from a hurricane, the protective Mississippi River delta, is quickly eroding away, leaving the historic city perilously close to disaster. So vulnerable, in fact, that earlier this year the Federal Emergency Management Agency ranked the potential damage to New Orleans as among the three likeliest, most catastrophic disasters facing this country. The other two? A massive earthquake in San Francisco, and, almost prophetically, a terrorist attack on New York City. The New Orleans hurricane scenario may be the deadliest of all. In the face of an approaching storm, scientists say, the city's less-than-adequate evacuation routes would strand 250,000 people or more, and probably kill one of 10 left behind as the city drowned under 20 feet of water. Thousands of refugees could land in Houston. Economically, the toll would be shattering.<sup>16</sup>

Surprisingly, a recent Congressional Research Service Report, *New Orleans Levees and Floodwalls: Hurricane Damage Protection*, indicates that "Failure (often called a breach) of levees and floodwalls reportedly was a contingency not central to emergency planning and response."<sup>17</sup> Indeed, Governor Blanco recently released an overview of her actions in preparing for and responding to Hurricane Katrina in which she states that "No one expected, or predicted, that the levees would fail in the manner which occurred after Hurricane Katrina."<sup>18</sup> The question is whether officials knew about the potential for breaches, regardless of whether people agreed on the scenario most likely to produce them. The evidence, outlined in the following two sections, indicates the U.S. Army Corps of Engineers knew about the threat of breaches, as opposed to overtopping, since the early 1980s. Moreover, all concerned agencies, including those at the local, state, and federal levels, knew about the threat of overtopping and consequent flooding in even a Category 3 hurricane.

The *Times-Picayune's* special edition issue from June 2002, titled "Washing Away," provides key insights into New Orleans' social, cultural, and geographical history, making it clear the vulnerability of the area to hurricanes was well known. The *Times-Picayune* summarized the choices faced by New Orleans in trying to manage a situation in which an area at or below sea level experiences sinking land and a rising Gulf of Mexico.

Higher levees, a massive coastal-restoration program and even a huge wall across New Orleans are all being proposed. Without extraordinary measures, key ports, oil and gas production, one of the nation's most important fisheries, the unique bayou culture, the historic French Quarter and more are at risk of being swept away in a catastrophic hurricane or worn down by smaller ones.<sup>19</sup>

The receding coastal wetlands were a well-known fact, increasing the vulnerability of Louisiana and New Orleans to hurricanes. A statement offered to the Times-Picayune by the general manager of the South Lafourche Levee District, Windel Carole, makes it clear, noting "The biggest factor in hurricane risk is land loss. The Gulf of Mexico is, in effect, probably 20 miles closer to us than it was in 1965 when Hurricane Betsy hit."<sup>20</sup> Therefore, anyone with limited knowledge of the history of hurricanes along the Gulf Coast was aware of the vulnerability of New Orleans to a Category 4 hurricane like Katrina.<sup>21</sup> Thus, as the environment surrounding the levees increased in its threat potential, the basic design choices made in constructing and maintaining the levees increased in importance.

Few people questioned the U.S. Army Corps of Engineers' competence, or diligence, in its oversight of the levee protection system. Although a contractor dispute (discussed below) pointed to the Corps of Engineers' failure to give fundamental consideration to soil composition in levee design, overall the authority of the Corps of Engineers went unquestioned by outside parties. Indeed, the draft report of Team Louisiana's investigation is expected to indicate, as its lead investigator, Ivor Van Heerden, testified to Congress, that the levee at the 17<sup>th</sup> Street Canal was built with "too little regard for the inherent weakness of the soil under the canal banks." The problem was repeated in the other major breaches in the levee system in New Orleans.<sup>22</sup> So, on the *preparedness* side, basic design flaws in the construction and maintenance of the levee infrastructure went unaddressed. The Army Corps of Engineers is currently investigating its role in the levee design and maintenance and, aside from an interim report, has not offered its own assessment of the preparedness failures evidenced in the levee breaches.<sup>23</sup> This issue is discussed in more depth in the next section of this paper.

On the *response* side of the disaster, the federal government developed the *National Response Plan* (NRP) in December 2004 for leaders to use in situations just like the Hurricane Katrina disaster. The NRP included provisions for dealing with catastrophic disasters in which state and local governments are overwhelmed. These provisions go into effect when the President declares an Incident of National Significance (INS), and the Secretary of Homeland Security activates the Catastrophic Incident Annex. In fact, a Presidential declaration of Katrina as an INS, issued on August 27, 2005, covered the states hit by the hurricane before it ever touched the coastline. It was, however, the first real test of the NRP and some confusion resulted in exercising it. Examining the confusion can provide lessons to take away from the response efforts.

Interestingly, Department of Homeland Security Secretary Michael Chertoff did not appear to recognize the implications of the designation made by the President for several days. Secretary Chertoff found it necessary to announce an INS again several days after the President, but still failed to activate the Catastrophic Incident Annex – even though the Hurricane Katrina disaster met not just one, but all four, criteria for an INS outlined in HSPD-5.<sup>24</sup> In early September, DHS spokesperson Russ Knocke explained that Chertoff's re-declaration of Hurricane Katrina as an INS was intended to create an "administrative paper trail" for the President's earlier announcement.<sup>25</sup> A month later, in mid-October, he contended that, "The

annex is intended to be used during no-notice catastrophic incidents when there is no awareness of an impending disaster and no pre-staging of people, resources, and response forces.”<sup>26</sup> In fact, reports indicate that the federal government’s authority to respond to an INS did not result from Homeland Security Secretary Chertoff’s memo, but from a statement issued by the White House on the night of August 27 while President George W. Bush was at his Crawford, Texas ranch.<sup>27</sup> Secretary Chertoff’s memo came thirty-six hours after the storm hit, declaring the Katrina disaster an INS, and, as discussed below, well after the only FEMA agent in New Orleans, Marty J. Bahamonde, knew the severity of the situation.

The President’s statement assigned William Lokey, a subordinate, as the “principal federal official” rather than FEMA Director Michael Brown. Chertoff’s memo re-declared an INS and assigned Director Brown as the “principal federal official.” We can assume the leadership at the federal level was well aware that the devastation from a hurricane like Katrina posed catastrophic risks, since the President declared it an INS before it hit land. Neither of the INS declarations activated the key provisions of the NRP that would support the proactive allocation of assets and capabilities by FEMA. As retired Admiral James Loy (who, as DHS deputy secretary, helped draft the NRP) indicated, one of the “dramatic lessons” to learn from the Hurricane Katrina response is in clarifying how and when to use the Catastrophic Incident Annex.<sup>28</sup> *Perhaps the baseline criterion to use in activating the NRP’s Catastrophic Incident Annex is whether proactive actions are required of FEMA and the agencies it coordinates to respond to any INS declaration.*

At first consideration, it is unclear why it was necessary to change the President’s designation of the “principal federal official,” especially if the Secretary of Homeland Security did not intend to activate the Catastrophic Incident Annex. Learning organizations push responsibility down the ranks so individuals faced with challenging situations are empowered to respond to them. Changing a Presidential designation so that the highest ranking bureaucrat is “officially” in charge makes it clear that FEMA, and by implication DHS, did not approach the challenges posed by the disaster with the point of view of a learning organization but, rather, as a top-down bureaucracy. Indeed, the inability of Marty J. Bahamonde, FEMA’s only agent on the ground in New Orleans immediately following the levee breach, to get the attention of the leadership in Washington D.C. is indicative of such an organization.

In describing his reporting to FEMA headquarters on Monday, August 29, Bahamonde told a Senate Committee “I believed at the time and still do today, that I was confirming the worst case scenario that everyone had always talked about regarding New Orleans,” i.e. as one of the top three most serious disaster scenarios in the United States.<sup>29</sup> There are clear indications from the Katrina response that FEMA is not organized in a manner conducive to learning, or to proactive response efforts in case of an INS. It is not unfair to characterize the agency’s processes as surprise-conducive.

Many news stories have discussed the exodus of personnel from the agency as the Department of Homeland Security integrated FEMA into its organization, and the negative impact of that reorganization on the professional identity of FEMA staff. A survey of employees last year found that eighty percent said the agency was weaker after joining DHS.<sup>30</sup> In addition, emails between FEMA officials in the field and their managers in Washington D.C. make it clear that Bahamonde, as the only FEMA official in New Orleans immediately after Katrina hit, was not empowered to solve problems on nearly the scale needed.<sup>31</sup> Moreover, it appears that the agency’s leadership either discounted, or ignored, much of his information about the dire circumstances in the Superdome, and the city in general.<sup>32</sup>

### **Organizational members realize a problem is getting worse**

Katrina, as a Category 4 hurricane, is one of sixteen such hurricanes to hit the United States over the past century. There were three Category 5 storms during that same time-period: Camille along the Gulf Coast in 1969; Andrew in 1992; and an unnamed storm hitting the Florida Keys in 1935. All told, there were 314 hurricanes recorded in the Atlantic Ocean since 1950. Of those, seventy-two hit the United States' coastline, with fifty striking along the Gulf Coast. Fourteen of the hurricanes hitting the Gulf Coast came on land within seventy-five miles of New Orleans. Five of those fourteen hurricanes were Category 3 or greater with one – Betsy in 1965 – a major hit on New Orleans. Based on the numbers, it is certainly not surprising that hurricanes have been a longstanding concern, especially around New Orleans.<sup>33</sup>

Before Katrina hit New Orleans, FEMA already considered the likely damage from a strong hurricane hitting the city to rank in the top three potential catastrophes facing the country. Moreover, a 2004 tabletop exercise on a hypothetical Hurricane Pam hitting New Orleans pointed to some strengths, but also significant weaknesses, in the readiness of authorities to respond to the likely devastation. A scheduled follow up exercise on evacuating New Orleans was not funded. Then Katrina triggered the actual evacuation plans of the state and city. As we know, these evacuation plans did not execute well. It seems fair to say that FEMA and the Army Corps of Engineers were well aware of the ongoing deterioration in New Orleans' capacity to withstand Category 3 hurricanes, much less a Category 4 or 5.

In the aftermath of Katrina, several investigations are underway relating to FEMA's performance in particular, but also into the U.S. Army Corps of Engineers' preparedness efforts, i.e. planning and design of the levees. The Opening Statement of Chairman Tom Davis of the House Government Reform Committee, in recent hearings on the response to Katrina, included the following key issues and questions:

I suspect we will find that government at all levels failed the people of Louisiana, Mississippi, and Alabama. I believe we will hear from Michael Brown, for example, that there simply was no unified command structure or clear lines of authority in Louisiana. That means we're confronted with profound questions about not only what went wrong with FEMA, but what may be wrong with our government at all levels when it comes to disaster preparation and response. Are we lacking a culture of urgency? A culture of getting things done? Or is it that, even when we have the best possible planning and prediction available, we come face to face with the vast divide between policy creation and policy implementation?<sup>34</sup>

A partial answer to the questions raised by Chairman Davis comes from what the former FEMA Director, Michael Brown, did not mention in his own testimony. Director Brown did not mention the National Response Plan or the "Incident of National Significance" concept anywhere in his testimony.<sup>35</sup> His concept of FEMA's role, as evidenced by his testimony, failed to consider the implications of an INS declaration for the overall framework within which the agency works. The leadership at the federal level clearly failed to provide the proactive resource allocation and engagement that the challenges of Hurricane Katrina required. The response efforts were largely reactive, i.e. bureaucratic.

Bureaucracies work by the rules in order to remain accountable. There were a number of criticisms of the federal bureaucracy's slowness to respond to Katrina's aftermath. To some extent, it resulted from a *duel of competing statutes* in the thinking of those responding to the

disaster of New Orleans post-Katrina. A Congressional Research Service (CRS) Report, "The Use of Federal Troops for Disaster Assistance: Legal Issues," recently indicated that:

Unless the President determines that a disaster implicates preeminently federal interests, the declaration of an emergency under the Stafford Act requires that the governor of the affected state first make a determination that the situation is of such severity and magnitude that the state is unable to respond effectively without federal assistance, *which determination must include a detailed definition of the type and amount of federal aid required.* [Emphasis added.]<sup>36</sup>

It is unclear whether the respective federal agencies understood the significance of an INS designation for the modality of the federal response. Federal officials, especially FEMA, stated several times that they needed the state of Louisiana to make specific requests. Yet, the NRP clearly makes the point in several places that federal officials need to *take the initiative* during incidents of national significance since local and state officials are likely overwhelmed by the event. It even calls upon FEMA to encourage and facilitate voluntary offers of assistance.

As the first sentence of our quote from the CRS document implies, an INS is in fact a statement that a disaster implicates preeminently federal interests. In point of fact, and as the CRS report indicates, such a declaration makes the Posse Comitatus Act *less restrictive* in its prescriptions of what federal troops can do in responding to disasters.<sup>37</sup> Nevertheless, the federal agencies responding to Katrina appeared to assume otherwise for several days into the disaster response effort. The delay in the federal response is discussed below in terms of differing groups attempting to sustain their own status quo. However, the immediate manifestation of those efforts to sustain a status quo was evidenced by the way key actors like Director Brown and Secretary Chertoff understood their own roles in the process.

In his testimony on the role of FEMA, Director Brown described it solely in the context of the Stafford Act, never mentioning the way in which an INS can alter the stipulations in the Stafford Act if the Secretary of DHS activates the Catastrophic Incident Annex of the NRP.<sup>38</sup> Moreover, in Secretary Chertoff's testimony he asserted that the NRP does not "give him any special powers that the FEMA director didn't have when President Bush declared a federal emergency the Saturday before Katrina struck on August 29."<sup>39</sup> FEMA did take proactive steps, as Director Brown's testimony indicates, by identifying Federal assets and capabilities, deployed strategically out of harm's way but within proximity. As indicated in the previous section, FEMA failed to maintain a proactive stance regarding movement of those assets and capabilities to the disaster scene after the hurricane passed. For example, on September 3 only a tiny fraction of the active duty U.S. military was engaged in rescue and relief efforts.

The situation frustrated senior military officers who attributed the issues in part to complex relationships with FEMA. Newhouse News Service quoted an officer (who asked not to be identified) as saying, "There is a tremendous amount of frustration here, that we have assets stacked up ready to go and we don't have the requests for them.... All we can do is nudge the folks at FEMA and say, 'How about if we do this or that?'" On the other hand, FEMA spokesperson Natalie Rule contended her agency's coordination efforts with the Pentagon were driven by the flow of requests from the State of Louisiana. "The military has been joined at the hip (with FEMA) since this storm was approaching Florida... We work with the state and look to the state as to what they need... If (a state request) has something to do with military assets, we would tap into those."<sup>40</sup> Indeed, DHS Secretary Chertoff has recognized the problem FEMA faced in using its own resources. He has promised to "re-engineer" the agency. The top two

weaknesses Chertoff intends to address are FEMA's logistical planning before and during disasters and its delivery of services to victims in the aftermath of disasters.<sup>41</sup>

On the face of it, Chertoff's "re-engineering" plan appears to address issues like the failure of FEMA to use its own pre-positioned assets and capabilities effectively, such as the difficulties in using military assets, and the reluctance of bus drivers and others to enter New Orleans because of the stories of violence. He proposed one innovative structure to incorporate surprise-avoidance processes in his recent testimony to the House Select Committee on Hurricane Katrina. Chertoff indicated that DHS is organizing emergency reconnaissance teams to go into disaster areas in the immediate aftermath of the catastrophe to provide real time situational reporting of facts on the ground. The new teams consist of FEMA specialists, Coast Guard personnel, and other DHS law enforcement officers.

The team innovation announced by Secretary Chertoff is a ready example of how to constrain the affective heuristic's impact on response decisions by putting in context exaggerated stories about what is happening on the ground.<sup>42</sup> A common shortcoming of the leadership during the response to Katrina from federal, state, and local leaders was their allowing vivid accounts of looting, rapes, and murder to affect their decision-making.<sup>43</sup>

More importantly, the major organizational and policy challenges lie on the other side of the affective heuristic, i.e. using it to enhance rationality. Secretary Chertoff has not spoken to how the agency will delineate the responsibilities of federal officials vis-à-vis state and local authorities in an emergency. In other words, *the key issue of how FEMA can act proactively during an INS remains unaddressed*. Much of the criticism federal officials made of local officials stemmed from the assumption that the federal government should take a reactive role to disasters. For example, Director Brown clearly discussed the inadequacies of the local response from the point of view of a federal administrator.<sup>44</sup> But he failed to keep in mind the way the NRP describes proactive actions:

Notification and full coordination with States will occur, but the coordination process must not delay or impede the rapid deployment and use of critical resources. States are urged to notify and coordinate with local governments regarding a proactive Federal response.<sup>45</sup>

Nowhere in the NRP does it say that the federal response to an INS is *conditional*, based on specific requests from the state or local governments. Nevertheless, FEMA's response was directed with that conception of the agency's role. Any "re-engineering" effort for FEMA must address this basic issue of what constitutes a "proactive" action by the agency and the scope of such actions when the Secretary of DHS does not formally activate the catastrophic annex of the NRP.<sup>46</sup>

The argument thus far is that leadership at the federal, state, and local levels was aware of the increasing vulnerability of the levee system in New Orleans to hurricanes at Category 3 and above. Key organizations, i.e. FEMA, failed to act proactively to mitigate the catastrophic disaster caused by the breach of the levees in New Orleans. The next section will consider issues relating to judgments made about the design of the levees as well as decisions made on funding ongoing maintenance and upgrades.

### **Fixing the problem requires significant cost in the present with no immediate benefit**

Improving the levee and floodwall system in New Orleans was a recognized challenge for decades, as was the challenge of a receding delta providing less protection to the New Orleans

area from the storm surges resulting from a hurricane. The Breaux Act of 1990 created a task force involving several federal agencies and gave it the mission of restoring wetlands. The task force received only forty million dollars per year to stop the erosion of the delta. A University of New Orleans study estimated the effort averted only about two percent of the overall loss, leaving an erosion rate of twenty-five square miles of delta per year.<sup>47</sup>

Basic flaws in the design of the levee protection system were first recognized over two decades ago, before the wetlands were so diminished. An outside contractor, Eustis Engineering, was the first to express concerns about the levee vulnerability to breaching in the early 1980s. In 1981, the New Orleans Sewerage & Water Board developed a plan to improve street drainage by dredging the 17<sup>th</sup> Street Canal. The Corps of Engineers issued permits to do the dredging in 1984 and 1992, though the Corps was not a partner in the project. As a *Times-Picayune* story explains:

Before the project, the canal formed a roughly symmetrical ‘U’ shape common to most canals. In the sections that would later fail during Hurricane Katrina, its average depth was about 12 feet below sea level and, at normal water levels, the Orleans side had about a 20-foot buffer of mud between the water and what was then a bare steel floodwall. That wall of sheet piling ran through the center of the levee to a depth of 9.8 feet below sea level. After the dredging, the bottom was 18.5 feet below sea level, and the canal-side levee had been shaved so narrow, water now touched the wall on the Orleans side. The ‘U’ was now lopsided and the water in the canal had shorter paths to the outside of the levee.<sup>48</sup>

Eustis Engineering contracted to do a design study for Modjeski and Masters, the consulting engineers on the project, and performed soil investigations on a section of the 17<sup>th</sup> Street Canal from south of the Veterans Memorial Boulevard bridges to just north of those structures.

They found that “the planned improvements to deepen and enlarge the canal may remove the seal that has apparently developed on the bottom and side slopes, thereby allowing a buildup of such pressures in the sand stratum.”<sup>49</sup> Eustis’ concerns about a “blow-out”, or breach, of the levee were strong enough that the company recommended test dredging before the final design. The company recommended that, without test dredging, the bottom of the canal needed sealing with a concrete liner or building a seepage cutoff wall, like sheet pilings, to a depth of 65 feet below sea level versus the existing 12 feet. Engineers studying the levee breaches consider the report by Eustis significant because the stretch of canal the firm studied is widely considered to exhibit stronger soil layers than those that breached during Hurricane Katrina.

The most puzzling point about the dredging project is that the Corps of Engineers planned to follow the project by raising the floodwall from 10 feet to 14.5 feet. It is unclear whether the Corps paid attention to the contractor’s concerns since most of the documents related to the work remain unavailable to the public. “Although the Corps of Engineers was not a direct partner in the dredging, it was aware of the work and knew it would have an impact on its later project.”<sup>50</sup> Indeed, contractors working for the Corps on the later project raised their own concerns about the soil and foundations of the levee.

Reports indicate that key sections of the levee system’s soil and foundation, particularly the floodwall on the 17<sup>th</sup> Street Canal where much of the serious flooding occurred, posed serious problems for the contractors involved. Court papers from 1998 show that Pittman Construction indicated to the Corps of Engineers as early as 1993 that the soil and the foundation for the walls were “not of sufficient strength, rigidity and stability” to build on. The construction company

claimed that the Corps of Engineers did not provide it with complete soil data when it developed a bid on the levee project.<sup>51</sup>

Though the construction company lost its suit against the Corps of Engineers, the gist of their complaints about the condition of the soil and existing foundation was not disproven. Engineers now say the difficulties Pittman Construction faced were early warning signs that the Corps of Engineers ignored.<sup>52</sup> In fact, testimony before the U.S. Senate's Committee on Homeland Security and Governmental Affairs by several witnesses point to soil-related issues as key causal variables in the failures of the 17<sup>th</sup> Street Canal, the London Ave Canal, and the Industrial Canal.<sup>53</sup> Indeed, Van Heerden summarizes the preliminary findings well, noting:

...in the case of the 17<sup>th</sup> Street Canal, London Ave Canal and the Industrial Canal, levee collapse and flood breaching reflected unstable soils conditions and a lack of foundation support and water percolation seals, given the soft, porous and highly organic nature of the soils.<sup>54</sup>

The Corps of Engineers officially disputed the points made by Pittman Construction regarding the soil conditions, though it now seems clear that the crucial breaches in New Orleans occurred in levees where the floodwall foundations were not as deep as the canals and that the Corps of Engineers was aware of the issue. The soil then allowed water to percolate under the levee and floodwalls, weakening the structure so that the storm surges from Hurricane Katrina moved it entirely, or breached it. *Would an organization with processes in place to support ongoing learning, and surprise-avoidance, fail to recognize the legitimacy of the contractor's point, rather than argue about purely budgetary issues related to the contract?*

The U.S. Army Corps of Engineers is historically an insular agency, known for doing things its own way. It is not possible to say whether surprise-avoidance processes are in place at the Corps of Engineers, until the public receives more access to internal documents. Robert Bea, a geotechnical engineer from the University of California at Berkeley, asserts "In my view, in the case of the 17<sup>th</sup> Street, London Avenue, and even the Industrial Canal floodwalls, fundamentally what we are looking at is a failure focused on the institutional side."<sup>55</sup> The failure of Corps' staff to recognize and prioritize the challenges of levee upgrades and receding wetlands to the city of New Orleans, and surrounding areas, strongly suggests that surprise-conducive processes characterize its organization. The Corps' organization has over the past few decades outsourced more work, lost many engineers to private industry, and consequently suffered a diminished capacity to attract top-notch engineers.<sup>56</sup>

Bazerman and Watkins note that predictable surprises play out over long time frames, sometimes longer than the typical tenure of organizational leaders. They contend "This creates a variation on the free-rider problem. 'Why,' a leader might ask, 'should I be the one to grapple with this problem and take all the heat when nothing is likely to go wrong during my watch?'"<sup>57</sup>

In other words, members of the U.S. Army Corps of Engineers, conceivably, made a collective bet that the unlikely occurrences that, in fact, did end up happening, were not worth the expense, from a professional or organizational initiative point of view. We will know more about the decision-making in the Corps, and its relationship to local agencies with levee responsibilities, as additional information is made available to the public. The sheer magnitude of the problems faced in the New Orleans levee protection system probably appeared overwhelming to members of an organization enduring ongoing budget concerns and staff turnover.<sup>58</sup>

Consider the scale of the plans offered to fix the levee challenges: A plan floated in early 2001 involved two to three billion dollars proposed to divert sediment from the Mississippi River

back into the delta, rather than allow the sediment to wash down the levee system and dump into deep water. The project was compared to the four billion dollar restoration initiative for the Florida Everglades. However, these projects are typically funded through matching grants in which the state has to match a federal dollar with one of its own. Louisiana was only able to match each dollar with fifteen to twenty-five cents. Facing the scale of such a challenge, and the state's limited ability to pay for its share of the costs, the response of most people was to maintain the status quo. The result was a catastrophic disaster that cost many times the few billion dollars needed to initiate a full-scale rebuilding program for the levee protection system and the surrounding wetlands. Essentially, those responsible for the levee protection system in New Orleans saved money in the short term only to permit one of the largest disasters in American history to occur over the long haul.

### **Humans tend to maintain the status quo if it functions**

We will understand the way the status quo for the New Orleans levee protection system was maintained, in the decision-making of the Corps of Engineers and their associated local agencies, as more documentation is made available to the public. On the preparedness side, the status quo self-evidently stopped functioning when the levee protection system catastrophically failed during Hurricane Katrina. The U.S. Army Corps of Engineers currently finds its authority questioned by many, not because of the competence of its engineers' expertise, but rather due to concerns about its organizational processes that allowed such basic design flaws to go without sustained questioning by engineers exercising professional judgment. More to the point, *the Corps actually contested lawsuits brought by contractors that related directly to design flaws stemming from the soil foundations of the levees.*

New Orleans had dodged the bullet many times, with the major force of hurricanes skirting around the area. Nevertheless, most people with a reason to know about it were aware that a Category 3 hurricane posed a severe threat to the New Orleans' levee protection system, and a Category 5 hitting land as a Category 4, as with Katrina, posed a catastrophic threat.

Looking at the status quo during the response effort to Katrina is a bit more complex. President Bush declared the oncoming storm an *incident of national significance* before it hit the coastline, due to widespread concern that it portended catastrophic damage and loss of life. As noted above, the NRP stipulates that the declaration of an INS will initiate a series of federal actions that, even though coordinated with the states and localities, nevertheless provides the designated authority for the "principal federal official" to initiate and take proactive steps in responding to a catastrophic disaster. In other words, when responding to a disaster where the President declares an INS, the director of FEMA is not required to wait for a request from the governor of the affected state to begin providing response aid.

The INS designation is intended to *shake-up* the status quo among federal agencies during catastrophic disasters, making agencies operate more like a network of resources than top-down bureaucratic organizations. Secretary Chertoff saw it this way when he responded to criticisms of his failure to activate the Catastrophic Incident Annex. As noted previously, he indicated that the Director of FEMA already had that authority, though director Brown did not assume the authority was his, and failed to act on it. If the authority passes automatically through the office of the DHS secretary to his designee (an insight that does not seem obvious from the NRP), there was no reason to make Director Brown the "principal federal official" for Katrina response in place of William Lokey, the first official put in charge by President Bush's declaration. The point is reinforced by the fact that the U.S. Coast Guard's Thad Allen replaced Brown as the

“principal federal official” for the Katrina response. It appears that the designation is more effective if the individual starts from an authoritative position within at least one agency in order to command belief in his/her potential effectiveness by leaders in other agencies. Though the “principal federal official” designation appears convincing on paper, in the NRP existing relationships between agencies at various levels of government dictate that the individual designated needs to already occupy a leading role in a response agency.

Nevertheless, the INS was effective in “shaking up” the status quo between federal agencies, imposing a supra-bureaucratic authority with a unified command structure for federal resources called the National Incident Management System (NIMS). Aside from reports about turf wars between the Department of Defense’s Northern Command and DHS, most federal agencies worked together successfully during the Katrina response. Consider, for example, the point made by Frank Cilluffo, director of the Homeland Security Policy Institute at George Washington University, who noted, “Quite honestly, at the federal level, the coordination was quite robust. It’s just the interface between federal, state and local where clearly we need to look to ways to improve the process.”<sup>59</sup> In other words, shaking up relations between agencies at the same level of government is one challenge. Shaking up relations between agencies across levels of government is a wholly different challenge.

Attempts to use the NIMS to manage the support relationship with the states, to federalize the response into a single, unified command structure, failed following Katrina. In the end, the Louisiana National Guard, Guard units dispatched from other states, and active-duty federal troops received direction through a joint command using the two existing command authorities, state and federal. Director Brown summarized the situation in his testimony as, “We federalized this operation without federalizing it.”<sup>60</sup> After several crucial days during the aftermath of Katrina, and failing to gain Governor Blanco’s consent to federalize the Louisiana National Guard to place it under the direction of the Federal Joint Task Force Katrina, President Bush designated a single military commander for the task force. Governor Blanco wrote to the President:

I also agree with your idea that – given the unprecedented requests for federal military assistance that I, and my fellow Governors in Mississippi and Alabama have made – a ‘single military commander’ of ‘Federal Joint Task Force Katrina’ be named for federal forces. I believe such a decision is critical to improving the timeliness of fulfilling and coordinating the requests for federal assistance that have already been made. This officer would serve as the single military commander for all Department of Defense resources providing support to the Department of Homeland Security and the State of Louisiana. This could also enhance the contribution of over 25 National Guard states currently being commanded by the Louisiana Adjutant General. I ask that you direct the assigned Federal Coordinating Officers at the Department of Homeland Security (FEMA) to co-locate with my Homeland Security and Emergency Preparedness Office at the Federal Joint Task Force headquarters. This would make the Joint Interagency Operations Center a truly integrated operation.<sup>61</sup>

The President’s decision followed several days of differences, described by some as a “political standoff,” between the federal and state governments over how to unify the command for the National Guard and federal troops in New Orleans. The differences between the state and

federal governments regarding the need for a “unified command” delayed the arrival of active-duty federal troops in New Orleans for several days. It is unclear what impact it had on FEMA’s seeming inability to act proactively, though some of the agency’s decisions not to commit resources stemmed from concerns about disorder and the safety of FEMA agents.

Governor Blanco, on August 29, a day after Katrina hit land, asked the President for “everything you’ve got,” including a specific request for a range of items, as well as 40,000 troops on August 31. President Bush sent 7,000 federal troops on September 3 after it was clear that the differences on how to organize a unified command were beyond reconciliation.<sup>62</sup> The new response “status quo,” implied by the NIMS, did not prove workable in the catastrophic disaster of Hurricane Katrina.<sup>63</sup>

## Conclusion

The occurrence of a hurricane like Katrina was not unexpected in New Orleans; neither were the complications faced in the aftermath of the storm. Given this understanding, and the neglect in preparing for a hurricane like Katrina, as well as the ineffective response preparations, it seems reasonable to assert that Katrina as well as its aftermath was a predictable surprise. The threats posed by the hurricane, and the likely aftermath, were well known and unsurprising to most who thought about the hurricane threat to New Orleans. Unfortunately, much of the local, state, and federal leadership, especially the U.S. Army Corps of Engineers, appears to have remained complacent about preparing the levees for a catastrophic hurricane. As more information is made public, the Corps appears increasingly to exhibit surprise-conducive organizational processes in its oversight of upgrades and maintenance to the New Orleans levee protection system.

Like any predictable surprise, the preparation and response to Katrina indicate that leaders need to create structures in which the affective heuristic is *constrained* in its ability to limit rationality and *enhanced* in its capacity to inform rationality in decision-making about hurricane protection. The preparation and response to Katrina clearly poses a challenge on how we go about building those structures, both within bureaucracies and across them at different levels of government. We have suggested a number of potential organizational changes to build structures that support surprise-avoidance processes, while discouraging surprise-conducive processes.

1. Explicitly specify in the NRP that the “principal federal official” designated by DHS is authorized to activate the Catastrophic Incident Annex, pushing the authority down the organization from the DHS Secretary to his/her designee.
2. Integrate learning organization principles into the U.S. Army Corps of Engineers, FEMA, and DHS.
3. View the status quo during disasters as a multi-level, governmental reality involving ongoing compromise between authorities at each level.
4. Review the NIMS requirement for a “unified command structure” to determine under what circumstances joint commands suffice for the mission.

When combined with Secretary Chertoff’s proposed DHS reconnaissance teams, intended to provide improved “situation awareness,” the organizational innovations suggested above promise an increase in the surprise-avoidance capability of FEMA.

---

<sup>1</sup> Max H Bazerman and Michael D. Watkins, *Predictable Surprises: The Disasters You Should Have Seen Coming, And How To Prevent Them* (Boston, Massachusetts: Harvard Business School Press, 2004).

<sup>2</sup> P. Slovic, M.L. Finucane, E. Peters, and D.G. MacGregor, “Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality,” *Risk Analysis* 24, 2 (2004), 1-12. They note, “the affective heuristic enables us to be rational actors in many important situations. But not in all situations. It works beautifully when our experience enables us to anticipate accurately how we will like the consequences of our decisions. It fails miserably when the consequences turn out to be much different in character than we anticipated.” 12.

<sup>3</sup> Consider, for example, the statement by Russ Knocke, a spokesman for Homeland Security Secretary Chertoff, that, speculating on whether the federal response could have been quicker if Chertoff understood the gravity of the situation sooner is playing “armchair quarterback.” Jan Moller, “News of Levee Breach Hit D.C. Late,” *The Times-Picayune*, December 4, 2005. <http://www.nola.com/search/index.ssf?base/news-4/1133683117177710.xml?nola> [Accessed on 12/08/05.]

<sup>4</sup> Bazerman and Watkins, *Predictable Surprises*, 4.

<sup>5</sup> *Ibid.*, 5-8. The authors actually outline six characteristics of predictable surprises. Four of them are basic to the concept while two others overlap with two of the basic ones, added in parentheses in our list.

<sup>6</sup> We will not delve into the theory of a learning organization. However, the initial statement of the approach is most readily available in the work of Peter M. Senge on the topic. Peter M. Senge, *The Fifth Discipline* (New York: Currency Doubleday, 1990).

<sup>7</sup> U.S. Army Corps of Engineers, “Summary of Field Observations Relevant to Flood Protection in New Orleans, LA. – Interim Report to Task Force Guardian,” *Interagency Performance Evaluation Task Force*, December 5, 2005. <https://ipet.wes.army.mil/> [Accessed on 12/10/05]

<sup>8</sup> “Army Corps of Engineers: History of the Lake Pontchartrain and Vicinity Hurricane Protection Project” (General Accountability Office: November 2005). <http://www.gao.gov/new.items/d06244t.pdf> [Accessed on 12/09/05]

<sup>9</sup> Researchers in the area have done several studies that confirm the point. One in particular dealt with risk perception in making decisions about investing in airplane safety. People were asked to evaluate how attracted they were to make a decision to purchase new equipment for use in responding to an airliner crash. People in one group were told the equipment has a chance of saving 150 lives threatened by such an event. People in a second group were told the equipment has a chance of saving 98% of the 150 people threatened. The researchers predicted that a chance to save 150 lives represents a diffuse good to people, whereas saving 98% of a number is very good. The researchers found, as predicted, that support for saving 98% was stronger. It was more vivid and, as a result, people were more able to envision the consequences, see P. Slovic, M.L. Finucane, E. Peters, and D.G. MacGregor, “The affective heuristic,” in T. Gilovich, D. Griffin, and D. Kahneman (Eds.), *Heuristics and biases: The psychology of intuitive judgment* (New York: Cambridge University Press, 2002): 391-420.

<sup>10</sup> Bazerman and Watkins, *Predictable Surprises*, 93. As the authors note, “In many real-life situations, people fail to act until confronted with vivid data. In the case of predictable surprises, action is required to avoid the disaster, but until the disaster occurs, the need for change is not vivid,” 92.

<sup>11</sup> *Ibid.*, 153.

<sup>12</sup> Brian Friel, “Weathering the Storm,” *Govexec.com*, October 26, 2005. <http://www.govexec.com/dailyfed/1005/102605mm.htm> [Accessed on 11/15/05]

<sup>13</sup> Bazerman and Watkins, *Predictable Surprises*, 102.

<sup>14</sup> *Ibid.*, 106.

---

<sup>15</sup> “New Orleans Disaster Was Predicted,” *Reuters*, September 2, 2005. [http://news.com.com/Experts+New+Orleans+disaster+was+predicted/2100-1008\\_3-5846233.html](http://news.com.com/Experts+New+Orleans+disaster+was+predicted/2100-1008_3-5846233.html) [Accessed on 10/10/05].

<sup>16</sup> Eric Berger, “Keeping Its Head Above Water,” *Houston Chronicle*, December 1, 2001. [http://www.hurricane.lsu.edu/in\\_the\\_news/houston.htm](http://www.hurricane.lsu.edu/in_the_news/houston.htm) [Accessed on 10/10/05].

<sup>17</sup> Nicole T. Carter, “New Orleans Levees and Floodwalls: Hurricane Damage Protection,” *CRS Report to Congress* (September 6, 2005), 1. “Levees are broad, earthen structures, while floodwalls are concrete and steel walls, built atop a levee or in place of a levee,” 2.

<sup>18</sup> “Overview of Governor Kathleen Babineaux Blanco’s Actions in Preparation for and Response to Hurricane Katrina,” *Response to the U.S. Senate Committee on Homeland Security and Governmental Affairs Document and Information Request Dated October 7, 2005 and to the U.S. House of Representatives Select Committee to Investigate the Preparation for and Response to Hurricane Katrina*. December 2, 2005, 18. [http://www.gov.state.la.us/assets/docs/PDFs/Gov\\_response.12.2.05.pdf](http://www.gov.state.la.us/assets/docs/PDFs/Gov_response.12.2.05.pdf) [Accessed on December 7, 2005]

<sup>19</sup> “Washing Away,” *The Times-Picayune*, June 23-27, 2002. <http://www.nola.com/hurricane/?/washingaway/> [Accessed on 10/10/05].

<sup>20</sup> John McQuaid and Mark Schleifstein, “In Harm’s Way,” *The Times-Picayune*. [http://www.nola.com/hurricane/index.ssf?/washingaway/harmsway\\_1.html](http://www.nola.com/hurricane/index.ssf?/washingaway/harmsway_1.html) [Last accessed on 10/10/05].

<sup>21</sup> Indeed, a recent report by the Government Accountability Office is critical of the Corps management of compensatory mitigation in the wetlands of the delta. Compensatory mitigation involves restoring a former wetland, as a condition of a permit when the loss of wetlands is unavoidable. It observed: “The Corps required monitoring reports for 89 of the 152 permit files reviewed where the permittee was required to perform compensatory mitigation. However, only 21 of these files contained evidence that the Corps received these reports. Moreover, only 15 percent of the 152 permit files contained evidence that the Corps had conducted a compliance inspection. The Corps districts provided somewhat more oversight for mitigation performed by the 85 mitigation banks and 12 in-lieu-fee arrangements that GAO reviewed. For the 60 mitigation banks that were required to submit monitoring reports, 70 percent of the files contained evidence that the Corps had received at least one monitoring report. However, only 36 percent of the mitigation bank files that GAO reviewed contained evidence that the Corps conducted an inspection. For the 6 in-lieu-fee arrangements that were required to submit monitoring reports to the Corps, 5 had submitted at least one report. In addition, the Corps had conducted inspections of 5 of the 12 arrangements.” “Corps of Engineers Does Not Have an Effective Oversight Approach to Ensure That Compensatory Mitigation Is Occurring” (Government Accountability Office: September 2005). <http://www.gao.gov/new.items/d05898.pdf> [Accessed on 12/09/05]

<sup>22</sup> John Schwartz and Christopher Drew, “Louisiana’s Levee Inquiry Faults Army Corps,” *New York Times*, December 1, 2005.

<sup>23</sup> U.S. Army Corps of Engineers, “Summary of Field Operations.”

<sup>24</sup> “The Secretary shall coordinate the Federal Government's resources utilized in response to or recovery from terrorist attacks, major disasters, or other emergencies if and when any one of the following four conditions applies: (1) a Federal department or agency acting under its own authority has requested the assistance of the Secretary; (2) the resources of State and local authorities are overwhelmed and Federal assistance has been requested by the appropriate State and local authorities; (3) more than one Federal department or agency has become substantially involved in responding to the incident; or (4) the Secretary has been directed to assume responsibility for managing the domestic incident by the President.” *Homeland Security Presidential Directive/HSPD-5*. <http://www.whitehouse.gov/news/releases/2003/02/20030228-9.html> [Accessed on 12/09/05]

<sup>25</sup> Shannon McCaffrey, Alison Young, and Seth Borenstein, “How Homeland Security Chief Missed Signs of Storm’s Severity,” *Pittsburgh Post-Gazette*, September 18, 2005.

<sup>26</sup> Chris Strohm, “DHS failed to use catastrophe response plan in Katrina's wake” *Govexec.com*, October 18, 2005. [http://www.govexec.com/story\\_page.cfm?articleid=32586&printerfriendlyVers=1&](http://www.govexec.com/story_page.cfm?articleid=32586&printerfriendlyVers=1&) [Accessed on 12/09/05].

<sup>27</sup> “Conflicting accounts from top on Katrina response,” *Reuters*, September 15, 2005. <http://abcnews.go.com/US/wireStory?id=1129877> [Accessed on 10/10/05].

<sup>28</sup> Chris Strohm, “DHS failed.” Admiral Loy’s comments are important because, as an author of the NRP, he is also aware of what the classified part of the NRP says, if anything, about activating the catastrophic annex.

<sup>29</sup> “Testimony of Marty J. Bahamonde to the Senate Committee on Homeland Security and Governmental Affairs,” October 20, 2005, 3. [http://hsgac.senate.gov/\\_files/102005Bahamonde.pdf](http://hsgac.senate.gov/_files/102005Bahamonde.pdf) [Accessed on 11/05/05]

<sup>30</sup> Angie C. Marek, Edward T. Pound, Danielle Knight, Julian E. Barnes, and Kevin Whitelaw, “A Crisis Agency in Crisis,” *U.S. News & World Report*, September 19, 2005. FEMA’s senior staff is currently made up of about a third “acting” employees.

<sup>31</sup> Bahamonde, “Testimony.”

<sup>32</sup> Mary Curius, “Insider Condemns FEMA Response,” *The Los Angeles Times*, October 21, 2005. <http://www.latimes.com/news/nationworld/nation/la-na-fema21oct21.0.5147785.full.story?coll=la-home-headlines> [Accessed on 11/05/05].

<sup>33</sup> The Category level of a hurricane indicates its intensity. It is estimated using the Saffir-Simpson Hurricane Scale, a 1-5 rating based on the hurricane's present intensity. <http://www.nhc.noaa.gov/aboutshs.shtml> [Accessed on 10/10/05].

<sup>34</sup> “Opening Statement of Chairman Tom Davis,” *House Select Committee to Question Former FEMA Director Michael Brown*, September 23, 2005. <http://reform.house.gov/GovReform/News/DocumentPrint.aspx?DocumentID=34826> [Accessed on 10/10/05].

<sup>35</sup> Statement of Michael D. Brown, *House Bipartisan Select Committee to Investigate the Preparation for and Response to Hurricane Katrina*, September 27, 2005. <http://reform.house.gov/UploadedFiles/FEMA%20-%20Brown%20Katrina%20Testimony.pdf> [Accessed on 10/10/05].

<sup>36</sup> Jennifer K. Elsea, “The Use of Federal Troops for Disaster Assistance: Legal Issues,” *CRS Report to Congress*, September 16, 2005, 5. <http://fpc.state.gov/documents/organization/53685.pdf> [Accessed on 10/10/05]

<sup>37</sup> *Ibid*, p. 4.

<sup>38</sup> As the NRP says, “while all presidentially declared disasters and emergencies under the Stafford Act are considered Incidents of National Significance, not all Incidents of National Significance necessarily result in disaster or emergency declarations under the Stafford Act.” “National Response Plan,” *Department of Homeland Security* December 2004, 7. [http://www.dhs.gov/interweb/assetlibrary/NRP\\_FullText.pdf](http://www.dhs.gov/interweb/assetlibrary/NRP_FullText.pdf) [Accessed on 12/08/05].

<sup>39</sup> Alison Young, “Chertoff Says Ex-FEMA Director was ‘Commander’ during Katrina,” *Knight Ridder/Tribune News Service*, October 20, 2005.

<sup>40</sup> David Wood, “Military Expresses Frustration Over Red Tape,” *Newhouse News Service*, September 3, 2005. <http://www.newhousenews.com/archive/wood090305.html> [Accessed on 12/08/05].

<sup>41</sup> Siobhan Gorman, “Homeland Security Chief Set to ‘Re-Engineer FEMA,’” *Baltimoresun.com*, December 6, 2005. <http://www.baltimoresun.com/news/weather/hurricane/bal-te.chertoff06dec06.1.7009208.story?coll=bal-nationworld-headlines> [Accessed on 12/09/05]

<sup>42</sup> Michael Chertoff, “Statement by Homeland Security Secretary Michael Chertoff before the United States House Select Committee on Hurricane Katrina,” October 19, 2005.

<sup>43</sup> As a recent Wall Street Journal article indicated, the stories of mayhem, and unsubstantiated rumors echoed by politicians and federal officials, led the military to feel compelled to plan for a military operation rather than a straightforward relief effort, delaying their response. FEMA officials delayed on-the-ground relief efforts, turning routine trips into armed escorted movements in response to the vivid accounts of violence reported in much of the media. Aside from the fact that much of the looting appears to have included local police, the Coroner of New Orleans, Dr. Frank Minyard, noted recently that he has found only around seven gunshot victims. He added, “Seven

gunshots isn't even a good Saturday night in New Orleans," Christopher Cooper, "Misinformation Slowed Federal Response to Katrina" *The Wall Street Journal Online*, September 30, 2005.

[http://online.wsj.com/public/article/SB112804420733656428-Zm6OU8yHnUC6B8RDoPaDUyKFJs4\\_20060929.html?mod=tff\\_main\\_tff\\_top](http://online.wsj.com/public/article/SB112804420733656428-Zm6OU8yHnUC6B8RDoPaDUyKFJs4_20060929.html?mod=tff_main_tff_top) [Accessed on 10/10/05].

<sup>44</sup> He asserted, "I assume that someone today will ask me about whether I did all that I could, or whether I would have done anything differently. The answer to that question is yes...I regret not being able to persuade Governor Blanco and Mayor Nagin to sit down and coordinate their response," Michael D. Brown, Statement, September 27, 2005, 13. Contrast Brown's statement with one reportedly made by Governor Blanco, "I believe my biggest mistake was believing FEMA officials who told me that the necessary federal resources would be available in a timely fashion." Joy Warrick, Spencer S. Hsu, and Anne Hull, "Blanco Releases Katrina Records,"

*WashingtonPost.com*, December 4, 2005. [http://www.washingtonpost.com/wp-dyn/content/article/2005/12/03/AR2005120301480\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2005/12/03/AR2005120301480_pf.html) [Accessed on 12/10/05]

<sup>45</sup> National Response Plan, 44.

<sup>46</sup> Martha Mendoza, "Red tape hampering assistance," *The Tribune*, September 6, 2005.

<http://www.tribtown.com/print.asp?ArticleID=15399&SectionID=1&SubSectionID=186> [Accessed on 12/09/05].

<sup>47</sup> Eric Berger, "Keeping Its Head Above Water," [http://www.hurricane.lsu.edu/in\\_the\\_news/houston.htm](http://www.hurricane.lsu.edu/in_the_news/houston.htm) [Accessed on 10/10/05].

<sup>48</sup> Bob Marshall and Sheila Brissett, "Dredging Led to Deep Trouble, Experts Say," *Times-Picayune*, December 9, 2005.

<sup>49</sup> Ibid.

<sup>50</sup> Ibid. J. David Rogers, a University of Missouri-Rolla professor who is an expert on levee failures summarized the situation as follows: "I can say that categorically, it's not something (an engineer) can debate. You were heightening the levee and not broadening the base. You were increasing the load but not the support. So your factor of safety had to be going down."

<sup>51</sup> *Pittman Construction Co. vs. Department of the Army*

[http://msnbcmedia.msn.com/i/msnbc/sections/news/050929\\_leveesuit.pdf](http://msnbcmedia.msn.com/i/msnbc/sections/news/050929_leveesuit.pdf) [Accessed on 10/10/05].

<sup>52</sup> John McQuaid and Bob Marshall, "Evidence Points to Man-Made Disaster," *The Times-Picayune*, December 8, 2005.

<sup>53</sup> See written testimony of Ivor L. Van Heerden, "Failure of Levee Systems Surrounding Greater New Orleans During Hurricane Katrina – Preliminary Assessment," November 2, 2005.

<http://hsgac.senate.gov/files/110205vanHeerden.pdf> [Accessed on 11/05/05]; Raymond Seed, "Hurricane Katrina: Performance of Flood Control System," November 2, 2005. <http://hsgac.senate.gov/files/110205Seed.pdf> [Accessed on 11/05/05]; Peter Nicholson, "Hurricane Katrina: Why Did the Levees Fail," November 2, 2005. <http://hsgac.senate.gov/files/110205Nicholson.pdf> [Accessed on 11/05/05].

<sup>54</sup> Ibid., 1. Van Heerden is the lead investigator of Team Louisiana, the investigative group for the State of Louisiana. The team consists of six L.S.U. professors and three independent engineers.

<sup>55</sup> John McQuaid, "Problems May Lie Within, Some Say," *The Times-Picayune*, December 8, 2005.

<sup>56</sup> Ibid.

<sup>57</sup> Bazerman and Watkins, *Predictable Surprises*, 107.

<sup>58</sup> An overview of the Corps of Engineers budget issues is available in "Army Corps of Engineers: History..."

<sup>59</sup> Martha Mendoza, "Red Tape."

<sup>60</sup> Chris Strohm, "DHS failed."

<sup>61</sup> Letter from Governor Blanco to President Bush on Saturday, September 3.

[http://www.nola.com/katrina/view.ss?katrina/blancodocs/Bob\\_Mann\\_Documentation.pdf](http://www.nola.com/katrina/view.ss?katrina/blancodocs/Bob_Mann_Documentation.pdf) [Accessed on 12/10/05].

---

<sup>62</sup> See the full discussion of this issue from the perspective of Governor Blanco in “Overview of Governor Kathleen Babineaux Blanco’s Actions...,” 12-15.

<sup>63</sup> Indeed, this observation builds on a point offered by James J. Carafano in his testimony on the FEMA response to Katrina. He noted: “State and local governments assume in virtually every instance, state and local leaders will remain in charge and national assets, whether they come from other states, the private sector, or the federal government, will be in support of their efforts. That is the right approach, even for catastrophic disasters,” James J. Carafano, “Improving the National Response to Catastrophic Disaster,” Statement before the Committee on Government Reform, September 15, 2005, 6. <http://www.heritage.org/Research/HomelandDefense/tst091505a.cfm> [Accessed on 12/05/05]