Finalist Essays from the Center for Homeland Defense and Security's First Annual Essay Competition, 2008

Essay Question

What single aspect of Homeland Security has been most successful, and what single aspect will be most critical to Homeland Security success?

Winning Essay

Reducing the Risk
Matthew Allen, Staff Scientist, Sandia National Laboratories

Finalists

(listed in alphabetical order by last name)

Brick by Brick: The Strategic Re-Building of the Public Health Infrastructure
Meredith Allen, Epidemiologist, Department of Health in Bucks County, PA

Ascendency through Perception: The Importance of Dedicated Investment in Academic Homeland Security Research and Inquiry
William L. Gardella, Deputy Marshal, Maine Judicial Marshal Service

Making Consequence Management Work: Applying the Lesson of the Joint Terrorism Task Force
Will Goodman, Assistant for Plans, Office of the Secretary of Defense

Proliferation of Biodefense Laboratories and the Need for National Biosecurity
Jesse Tucker, Graduate Student, University of Alabama

About the Competition

The Center for Homeland Defense and Security (CHDS) announces the winner and finalists of its first annual essay contest. CHDS launched the contest last year to provide people from around the country the opportunity to express their opinions on homeland security issues and to suggest new ideas. The winner and four finalists were selected from eighty contest submissions by a committee comprised of CHDS staff, faculty, and alumni. The variety of the essay topics submitted, as well as the backgrounds of the authors, highlights the vast scope of the impact that homeland security policies, programs, and challenges have on our communities and professions. This year's contestants were asked to answer the question "What single aspect of Homeland Security has been most successful, and what single aspect will be most critical to Homeland Security success?"

Congratulations to this year's winners. We hope reading their essays will accomplish the contest objective of stimulating thoughts and ideas and promoting discussion and debate on homeland security and defense issues.

More information about the competition, including the question and guidelines for the current competition and an archive of questions and finalist essays from previous competitions can be found at the following web address:
http://www.chds.us/?essay/overview

REDUCING THE RISK

Matthew M. Allen

Matthew Allen is a scientist at Sandia National Laboratories. He is currently serving as an ASME Congressional Fellow at the Committee on Homeland Security, House of Representatives. The views of Matthew Allen do not necessarily reflect the views of any member or committee of Congress. Mr. Allen can be contacted at mallen@sandia.gov.

The effective use of rhetoric in communicating public policy cannot be overstated. In democratic governments, elected officials must be able to accurately and (equally as important) concisely convey their actions in a way that explains both the problem and solution. Since the establishment of the Department of Homeland Security in 2002, the department's mission has sometimes been difficult to understand. What the government is doing to protect its citizens from terrorism, and how the government is doing it, is something few people can articulate. Not until recently has the administration found the proper rhetorical tools that explain both the challenges the nation faces with respect to terrorism and how the government is addressing those challenges. As will be shown below, the concept of "reducing the risk," more than any other aspect of homeland security policy, will be critical in guiding the actions of policy makers for years to come.

THE IMPORTANCE OF RHETORIC

Rhetoric can be defined as the art of speaking or writing effectively or the use of speaking and writing as a form of persuasion. In this paper, the term rhetoric (and rhetorical phrase) describes the use of language to communicate a challenge faced by the nation and the means of meeting that challenge.

When the nation is threatened by ideological opposition, it is often rhetorical arguments, in the form of catch phrases, that galvanize the public in support of a common goal. Although these rhetorical phrases can be sweeping generalizations and may provide few specifics (if any) as to how opposition can be overcome, such phrases are useful in communicating to the public challenges faced by the nation.

In February of 1861, Jefferson Davis was elected provisional president of the Confederate States of America. On April 12th of the same year, Fort Sumter was attacked and destroyed by Confederate forces – thus beginning the Civil War. To prepare the nation for war, President Lincoln called a special session of Congress on July 4, 1861. In his statement to the Senate and House of Representatives, he asked the Congress to legitimize his recent call-up of troops, his blockade of the ports of secessionist states, and his suspension of the writ of *habeas corpus*. Lincoln's justification for becoming the most centralized president in

history was his perception that the president had a constitutional duty to "preserve the union." This rhetorical statement was direct and to the point. It described the struggle against secession in a way the American people, the Congress, and the United States courts could easily understand and support.

The Cold War represented a similar ideological challenge. George Keenan's 1947 paper, "The Sources of Soviet Conduct," gave a very detailed analysis of the factors influencing Russian, Communist, and Soviet thinking of the time. However, the message many policy makers took away from his now famous paper was the following sentence:

In these circumstances it is clear that the main element of any United States policy toward the Soviet Union must be that of a long-term, patient but firm and vigilant containment of Russian expansive tendencies.[1]

Much to the author's surprise, this concept of "containment" became the foundation of diplomatic, economic, and military policy toward communist countries for the next forty years.[2]

Why did this happen? Why was this one sentence interpreted so broadly? The answer is quite simple: It was excellent rhetoric. Much like Lincoln's mission to "preserve the union," Keenan's concept of containment was direct and to the point. With that one word, policy makers could explain both the problem (in this case Russian expansive tendencies) and the solution: containment. This rhetoric provided a simple framework to counter communism, an ideology that was difficult for most people to understand. For forty years, government actions were measured by their success in containing the communist threat.

The modern ideological challenge to the United States (and the rest of the Western world) is that of radical Islam. How do we counter this ideologically driven opponent with no well-defined geographical base or known constituency?

At a recent Congressional hearing, Secretary of Homeland Security Michael Chertoff was asked to summarize his strategy for dealing with terrorists. He answered, "In a nutshell it's: reduce risk... And we do it by looking at all the elements in the chain of risk."[3] This clear and concise statement described a framework for the Department of Homeland Security's enduring mission. The simple statement, *reducing the risk*, describes both the problem (we are at risk) and the solution: we must work to reduce this risk. This concept of *reducing the risk*, more than any other aspect of homeland security policy, has succeeded in communicating the challenges we face; reducing the risk will continue to be the most critical aspect in shaping of homeland security policy.

THE FORMALISM OF RISK

While the rhetorical statement, reducing the risk, may be simple, the definition of risk (at first glance) may appear difficult. The formulation of risk is not new or rare in either the private or public sectors. Engineers, economists, political analysis, and public health

professionals all employ some method of risk analysis in their decision-making processes. Academics have made an industry out of quantifying risk and adding contributing factors to risk equations.

Fortunately, although every field's understanding of risk may be slightly different, the meaning of risk vis-à-vis homeland security can be described by three fundamental factors: threat, vulnerability, and consequence. What is more, risk is the product of these terms not the sum. If any one of them is zero then the risk is zero.[4] Likewise, if any of the terms is much greater than the others, it can drive the risk higher even when the other terms may be small.

Taken together, these three factors describe – either qualitatively or quantitatively when possible – our nation's risk with regard to terrorism. In the following sections, each of these terms is discussed in relation to their influence on terrorism risk assessment.

THREAT

In the post-9/11 world, it is common to hear talk regarding the "probability" of terrorism. Probability, however, is best suited for naturally occurring phenomena such as lightning strikes, hurricanes, and rain. The more relevant term for homeland security purposes is the *threat* of terrorism, where threat is a combination of intent and capability.

The role intent plays in threat assessment can be illustrated by a comparison of two homes. On the one hand, there is my mother's home in a small town in western Pennsylvania. Although al-Qa'ida may be capable of blowing up her home, they have (as far as I know) no intent to do so. On the other hand, there is my apartment in Washington, DC, conveniently located between the U.S. Capitol Building and the White House. While I doubt Osama Bin Laden has my name on his list of targets, my apartment's proximity to other targets increases the risk to my home. Terrorist *capability* is the same in both cases, but terrorist *intent* to cause destruction is understandably higher in Washington, DC. than it is in a small town in western Pennsylvania.

Capability can be explained in a similar manner. The threat of an improvised explosive device (IED) such as those used in Iraq or Afghanistan is obviously higher than that of an improvised nuclear device (IND). Although al-Qa'ida has stated their *intent* to acquire and use nuclear devices, they are simply not as capable of acquiring INDs as they are of acquiring IEDs. This makes the threat of nuclear terrorism low as compared to the threat of terrorism by conventional explosives. Does this mean the *risk* of nuclear terrorism is low? Certainly not –keep reading.

VULNERABILITY

When some people think of vulnerabilities, they think of the impact a terrorist strike would have on components of our critical infrastructure or key resources. Vulnerability of targets depends on such factors as target hardness or single-point failures, as well as redundancy and reconstitution capability. A target's hardness refers to the ease or difficulty with which

a terrorist attack could be effectively accomplished. A critical facility with a firm structure and guards at the entrance is harder to attack than one with multiple points of access and no guards at the door.

Some systems are vulnerable due to single-point failures. Our nation's aging electrical grid is a prime example. In August of 2003, the shutdown of one power plant in Northern Ohio caused an electrical blackout throughout much of the American Northeast. Single-point failures are also common in transit systems and production facilities. It is the wide-spread nature of this problem that makes it such a great vulnerability. Options for mitigating single-point failures are built-in redundancy and the ability to reconstitute a capability if it were lost. Alternatively, the absence of redundancy and reconstitution capability is a further vulnerability.

CONSEQUENCE

Consequence is the one risk factor that — with a few assumptions – can be quantified A successful terrorist attack would result in the loss of life and/or property – both things that are relatively easy to correlate with geographical regions. This allows us to compare the consequence of different types of terrorist attacks and the consequence of similar attacks at different locations. A powerful car bomb, for example, would have different levels of consequence in a small town in western Pennsylvania than the same size bomb would have in New York City. Although the destructive force of the bomb might be similar, a successful attack in New York City – with the highest population density in the country and the nation's third largest economy – would have much higher consequence.

Quantifying consequence in this way also allows us to rank the risk of various forms of attack. Weapons that claim many lives and destroy a lot of property naturally have greater consequence. This is what drives the risk of nuclear terrorism. As discussed above, the threat of nuclear terrorism may be low, but the consequence of the successful detonation of a nuclear device in an urban area would be catastrophic, resulting in thousands of fatalities and tens of billions of dollars in damage. This level of catastrophic consequence is what makes the *risk* of nuclear terrorism high, even though the threat may be low.

It is also important to note that consequence is the summation (not the product) of loss of life and property. It is possible to imagine a terrorist attack that claims only life and leaves infrastructure intact (such as the Sarin gas attacks in Tokyo's subway in 1995) or an attack that claims no lives but has dire economic consequences (such as the detonation of a dirty bomb) by disrupting service or denying access to critical infrastructure.

UTILIZING RHETORIC

With the above formalism, we have answered the question of how to confront the ideological threat of terrorism: by reducing the risk. However, this is not enough. While rhetoric is an effective means of galvanizing the public, rhetoric alone is not sufficient to indefinitely sustain public support. Public support can only maintained by implementing effective policy that is accompanied by demonstrable success.

The next logical question we must ask is: how do we measure success? Surely, no one believes that the risk of terrorism can ever be reduced to zero. Even the current administration feels we will never reach a terrorism-free environment. The *National Strategy for Homeland Security* states:

Recognizing that the future is uncertain and that we cannot envision or prepare for every potential threat, we must understand and accept a certain level of risk as a permanent condition.[5]

If we must accept a "certain level of risk as a permanent condition," how can we tell if reducing the risk is an effective strategy? Will we know when we've reduced risk to the proper level?

In a recent paper, Philip Gordon, a senior fellow at the Brookings Institution, described what is and is not required to win the War on Terror. He argues that rather than concentrating on every possible threat, the government should concentrate on reducing the risk of terrorism. He even suggests the acceptable level of risk that policy makers should strive to attain:

[Winning the War on Terror] will mean not the complete elimination of any possible terrorist threat...but rather the reduction of the risk of terrorism to such a level that it does not significantly affect average citizens' daily lives, preoccupy their thoughts, or provoke overreaction. At that point, even the terrorists will realize their violence is futile.[6]

According to Gordon, success is attained when the risk of terrorism has been reduced to such a level that it does not "significantly affect average citizens' daily lives, preoccupy their thoughts, or provoke overreaction." If lack of overreaction is an indicator, we must be having some success at reducing the risk. After all, we haven't had a run on duct tape since 2003!

Although the rhetorical phrase of *reducing the risk* has only recently made its appearance, the Department of Homeland Security's efforts to accomplish this goal have been ongoing for the past six years. What makes the rhetoric so important is the ability it gives policy makers to answer the question: Are we safer today than we were six years ago? The answer is a resounding yes. Over the past six years, the government has limited terrorists' capability to harm us, thereby reducing the threat. They have worked to reduce our vulnerability by hardening targets and increasing the resiliency of our critical infrastructure. They have worked to mitigate consequence by acquiring medical countermeasures against biological, chemical, and radiological agents of terrorism.

All of these successes have been achieved through the government's operations to deter, detect, and disrupt terrorist activity along with implementing procedures for response to and recovery from successful terrorist attacks. Of course, people have made an industry of adding terms to this methodology, but all of these tactics play their role in reducing single or multiple factors in the risk equation.

The risk of terrorism will occupy the minds of our leaders far into the foreseeable future. Homeland Security's enduring mission of reducing the risk should guide policy makers in every aspect of their decisions on how to confront this challenge. The same concept should be used to measure success of government actions and policy implementation. Just as Keenan's philosophy of containment galvanized the Western world throughout the Cold War, the concept of "reducing the risk" will help Americans understand both the challenge and the solution for as long as terrorism dominates the political landscape.

---

[1] George F. Kennan (published under the name "X"), "The Sources of Soviet Conduct," *Foreign Affairs* 25, no. 4 (July 1947)

[2] George F. Kennan, "CONTAINMENT: 40 Years Later: Containment Then and Now," *Foreign Affairs* 65, no. 4 (Spring 1987).

[3] United States Congress, House of Representatives, Full Committee Hearing, Committee on Homeland Security, 110th Cong., Sess. 1 (Wednesday, September 5, 2007).

[4] Henry Kissinger used a similar formalism in his early work on nuclear deterrence. Henry Kissinger, *Necessity For Choice: Prospects of American Foreign Policy* (New York: Doubleday/Anchor, 1961), 12.

[5] Homeland Security Council, *National Strategy for Homeland Security* (Washington, DC: Government Printing Office, October 2007), 25.

[6] Philip H. Gordon, "Can the War on Terror Be Won?" *Foreign Affairs* 86, no. 6 (November/December 2007): 54.

BRICK BY BRICK: THE STRATEGIC RE-BUILDING OF THE PUBLIC HEALTH INFRASTRUCTURE

Meredith Allen

Meredith Allen is currently the epidemiologist for the Bucks County Department of Health, where her daily responsibilities include disease surveillance, outbreak control, and bioterrorism preparedness. She is a dissertation candidate in the DrPH program at Drexel University's School of Public Health. Her research focuses on community inclusion in governmental preparedness drills and its effect on participant's level of confidence in government emergency preparedness planning. She holds a master's degree in epidemiology with a concentration in infectious disease from Harvard University and a bachelor's in biology from the University of Delaware. Ms. Allen may be contacted at mgallen@co.bucks.pa.us.

The events of September 11, 2001 and the ensuing anthrax attacks have highlighted the need for public health preparedness in the United States. The public health infrastructure of the United States has eroded during the last twenty years due to a "lack of funding, focus, and national attention." [1] There has been a decrease in the number of laboratories and public health personnel which has, in turn, diminished the ability of professionals to collect and analyze data, conduct disease surveillance, and design interventions for the community. [2] The public health system had been "chronically under-funded for the past several decades and the 'infrastructure had greatly deteriorated.'" [3] The anthrax attacks of 2001 served as a wake-up call for public health and medical professionals, the American public, legislators and those tasked with homeland security; the nation's public health system was not equipped to rapidly and effectively respond to a bioterrorism attack whether small or large in scale. [4]

To help the nation rebuild the public health infrastructure to respond adequately to any terrorist attack, Congress has passed the Public Health Threats and Emergencies Act of 2000 and the Public Health Security and Bioterrorism Act of 2002, which has led to the influx of approximately ninety-nine million dollars into the rebuilding the public health infrastructure. [5] In addition to the increase in funding directed at the strengthening of the public health infrastructure, public health has finally been included as a member of the homeland security "team." On October 18, 2007, President George W. Bush issued Homeland Security Directive-21 regarding public health and medical preparedness. The directive sets forth a *National Strategy* for protecting the health of Americans during a disaster. Homeland security funding has provided for the reversal of the last twenty years

of public health infrastructure erosion resulting in the emergence of a stronger, more prepared public health system. Although the strengthening of the public health infrastructure has been the most successful aspect of homeland security, its ability to sustain the newly strengthened infrastructure by ensuring that newly funded programs and staffs are able to protect the nation's health during times of crisis while maintaining healthy communities during daily life is public health's greatest challenge.

The Department of Homeland Security (DHS) was formed to serve as the unifying force to lead a national effort to protect and secure America and its people. While the public health community is not a centralized federal department, public health professionals aim to protect and secure the American people from poor health, illness, and disease. The strategic goals developed by DHS (awareness, prevention, protection, response, recovery, service, and organizational excellence) serve as important benchmarks by which to measure the success of the revitalization of the American public health infrastructure.

The public health community has increased its *awareness* of disease movement and illness occurring throughout the community by enhancing its surveillance systems and hiring epidemiologists trained in recognizing disease trends and outbreaks. One such example of a surveillance program, introduced by the Department of Homeland Security in conjunction with the Environmental Protection Agency (EPA), is BioWatch. BioWatch is a program which utilizes biological pathogen detectors in conjunction with EPA air quality monitors to collect particles from the air which are then analyzed by public health laboratory professionals. [6] In the event of a pathogen release, the goal of the BioWatch system is to provide early warning to public health professionals before the affected population begins to present at their doctor's offices and local emergency rooms. [7]

In addition to BioWatch, some local Departments of Health have been able to implement syndromic surveillance programs due to the increased funding provided by DHS. Syndromic surveillance programs allow public health professionals to collect and analyze data on health trends (i.e. visits to the emergency department and flu medication sales). Syndromic surveillance allows for the categorization of patients' chief complaints of symptoms into coded syndromes (i.e. vomit, diarrhea, and rash). Syndromic surveillance allows public health professionals to have access to "real-time" data allowing for the detection of a sudden increase in any syndrome without waiting for final diagnoses or lab results. While syndromic surveillance can serve as an alerting system that there is an unusual health event in the community, it is also prone to false alarms from truly sporadic cases of illness; therefore it is imperative that trained public health professionals respond to the "alarms." Homeland security funding has often provided the funding for the hiring of additional Epidemiologists for local health departments.

Not only will increased surveillance capacity aid public health professionals in detecting any suspicious pathogen releases, it can also be used routinely to detect naturally occurring or seasonal outbreaks in communities. The influx of homeland security funding which was in part used to bolster surveillance systems has helped to rebuild the public health infrastructure needed to maintain healthy communities throughout the country, not just to protect them in the event of a bioterrorist attack.

Each year in the United States approximately 36,000 people die from the seasonal flu. [8] While increased surveillance has aided public health professionals in monitoring the annual flu season, homeland security funds have also helped public health professionals *prepare* for the seasonal flu outbreaks. In the event of any large-scale bioterrorism attack, local health departments may need to provide preventive medication and/or vaccine to their citizens (mass prophylaxis). Homeland security funding has allowed local health departments to plan for and practice their mass prophylaxis plans. Many health departments have used their seasonal influenza vaccination program, giving free flu shots to members of their community immunizing them for the upcoming flu season, to test their mass prophylaxis plans. One local public health department (Bucks County, PA) was able to immunize 4,664 people on a Saturday at four locations which would be used in an emergency for mass prophylaxis. Homeland security funding allowed the health department to order additional supplies in order to give community members free flu shots, along with providing the funding for staff on a Saturday – a more convenient time for many working adults who would like to be vaccinated. While local health departments are preparing for and practicing the delivery of mass prophylaxis, which may be necessary in the event of a bioterrorism attack, they are able to help prevent seasonal influenza in their communities. Local health departments will be able to sustain a state of readiness by holding practice drills of their mass prophylaxis plan each year in addition to providing a needed immunization free of cost to their local community.

While public health professionals aim to *protect* the public from disease and illness, homeland security initiatives have allowed public health departments to begin to help protect the nation's food supply. Public health professionals have long been involved in restaurant inspections; however public health is now involved in planning for and responding to agroterrorism, the deliberate introduction of a plant or animal disease. Homeland security initiatives have allowed public health professionals to be involved in food safety from "farm to table." The increased involvement of public health has allowed for an increase in education about food-borne illness. Food-borne illnesses are not always caused by improper food handling, but sometimes are a result of actions that occur on the farm. Homeland security has allowed for formation of professional relationships among public health, agriculture, and distribution professionals along with retail companies. The formation of these relationships and the resulting understanding of the "farm-to-table" process allow public health professionals to know who to call during outbreaks, such as the 2007 spinach outbreak related to California spinach producers.

Homeland security initiatives have also allowed for a more coordinated *response* to not only bioterrorism emergencies but to any naturally occurring outbreak. Homeland security has provided for the formation and upgrading of many communication systems (Health Alert Network) which have assisted public health professionals in recognizing multi-jurisdictional outbreaks, thus breaking down the jurisdictional silos that often limit the flow of information between colleagues.

In addition to an increase in communication systems, DHS has also provided for the opportunity for cross-jurisdictional training. One such program, Forensic Epidemiology, provides for public health professionals and law enforcement professionals to train

together resulting in a better joint understanding of job functions and specimen collection, developing joint patient interviewing, and establishing chain of custody of samples. In the event of a bioterrorism attack, law enforcement and public health will need to work together to identify the source of the attack and the pathogen. While the importance of the alliance of public health and law enforcement is easy to see in the event of an attack, the alliance also has important implications for routine operations. Law enforcement professionals are often involved in transporting criminals, who may claim to have (or do have) infectious diseases such as tuberculosis (TB). The formation of the linkage between public health and law enforcement has given each discipline a resource. Any officer who has questions about his or her possible exposure to TB after a transport will know who to call to obtain exposure information.

Not only have homeland security initiatives assisted public health professionals in successfully responding to events, they have also helped public health professionals to assist in the *recovery* after a major event such as bioterrorism. Homeland security has made public health professionals part of the first responder community and as part of that community public health professionals are responsible for the health and safety of other first responders. Public health professionals can provide vaccinations and prophylaxis to first responders and their families so that they are able to continue their response in an emergency.

The anthrax attacks of 2001 demonstrated the importance of effective public education and media relationships. Homeland security initiatives have allowed for public health professionals to have media training. It became clear that during a health emergency, such as the anthrax attacks of 2001, the public wanted to hear information from medical personnel, not public information spokespersons. Public health professionals have received media training and will be able to assist in the recovery efforts by providing accurate and appropriate health information and instructions.

The Department of Homeland Security is a unifying department in the federal government, which exists to serve the people of the United States. While serving the American population, homeland security initiatives have also provided opportunities for the American population to ***serve*** each other and volunteer. The Medical Reserve Corps (MRC) was founded in 2002 and is a federal program aimed at strengthening the resources of local communities. The MRC provides an opportunity for interested community members to volunteer to help their community prepare for and respond to local emergencies, along with promoting healthy living. [9] In a true health emergency, public health and emergency workers will not be able to provide the staffing resources needed to operate enough centers to accomplish mass prophylaxis in a community; MRC volunteers are a surge support that local public health agencies can call upon in an emergency.

Not only will MRC volunteers be an invaluable resource during an emergency, they can also increase community connectedness with local public health departments. When public health professionals do their jobs well, it often is not public knowledge. When an outbreak is prevented, there are no news stories or press releases, so much of the public is unaware of the great resource a local public health department can be. MRC volunteers provide

public health professionals an important link to the community they serve. By becoming a more visible and trusted part of the local community, public health messages delivered may be heeded in times of calm as well as during an emergency.

The rebuilding of the public health infrastructure was also greatly influenced by the final strategic goal of homeland security: *organizational excellence*. The public health system in the United States is a segmented system consisting of independent local health departments, state health departments, and, at the federal level, the Centers for Disease Control and Prevention (CDC). The introduction of the National Incident Management System (NIMS) has provided all public health agencies with a standardized management system with which to respond to emergencies large and small. NIMS incorporates best practices from other management models and provides a consistency throughout all agencies. NIMS has not only enabled different public health agencies to speak the same language but has also enabled public health agencies to communicate effectively with other first responder agencies. The introduction of NIMS has eliminated the use of professional jargon in emergency response and has created a system where responders can plug into a response regardless of whether or not it is being led by their jurisdiction.

With the increase in opportunities for multi-jurisdictional and multi-disciplinary training, the introduction of NIMS has allowed for a seamless response to emergencies. The introduction of ICS (the Incident Command System, a sub-section of NIMS) has eliminated the need for specific profession-related job titles and has allowed first responders from different agencies and from across the country to effortlessly "plug-in" to an active response. NIMS has created a standard operating procedure for the many different first responder agencies that provides a form of unity across all jurisdictions.

The public health infrastructure in the United States had been slowly eroding throughout the past few decades. Homeland security funding has begun the re-building of the nation's public health system. Each of the seven strategic goals of DHS (awareness, prevention, protection, response, recovery, service, and organizational excellence) has directly impacted the re-building of the public health infrastructure. The most critical aspect of the success of homeland security initiatives is the ability to use the improvements made possible by DHS in routine incidents as well as those which are emergencies. Creating a strong viable public health infrastructure will always ensure that there will be qualified professionals conducting surveillance for pathogens, practicing mass prophylaxis, safe-guarding the food supply, participating in cross-jurisdictional training and communication efforts, participating in media training, keeping first responders healthy, creating volunteer opportunities and community outreach, along with continuing the development of a consistent approach to incident management. Each one of those activities will help to protect the community from homeland security threats and will also protect the community from everyday hazards such as the presence of E.coli in spinach and seasonal influenza outbreaks. The improvements in the public health infrastructure will help during everyday occurrences but can also be scaled-up to handle large scale bioterrorism attacks. Homeland security must become a part of our everyday lives, not something which we concentrate on only when the security threats are raised. To be a part of our daily lives, homeland security programs must be sustainable and applicable to everyday life. The

continued strengthening of the public health infrastructure allows for the use of homeland security improvements and initiatives while also preparing to identify and respond to any threat to our security.

---

[1] B. Frist, "Public Health and National Security: The Critical Role of Increased Federal Support," *Health Affairs* 21, no. 6 (2002):119.
[2] Ibid.
[3] S. Hearne, L. Segal, M. Earls, C. Juliano, and T. Stephens, "Ready or Not? Protecting the Public's Health from Diseases, Disasters, and Bioterrorism," 1, http://www.healthyamericans.org.
[4] Frist, "Public Health and National Security."
[5] D. Santiago and A Richter, "Assessment of Public Health Infrastructure to Determine Public Health Preparedness," *Homeland Security Affairs* 2, no. 3 (October 2006), http://www.hsaj.org.
[6] D. Shea and S. Lister, *The Biowatch Program: Detection of Bioterrorism* (2003), http://www.fas.org/sgp/crs/terror/RL32152.html.
[7] Ibid.
[8] Centers for Disease Control and Prevention, *Key Facts About Seasonal Influenza* (n.d.), http://www.cdc.gov/flu/keyfacts.htm.
[9] Medical Reserve Corps, *Overview of the Medical Reserve Corps* (n.d.), http://www.medicalreservecorps.gov/QuestionsAnswers/Overview.

ASCENDANCY THROUGH PERCEPTION: THE IMPORTANCE OF DEDICATED INVESTMENT IN ACADEMIC HOMELAND SECURITY RESEARCH AND INQUIRY

William L. Gardella

William L. Gardella is employed as a deputy marshal for the State of Maine Judicial Marshal's Service, which is responsible for providing a safe and secure environment for members of the public accessing the judicial system of the State of Maine. A lifelong resident of Maine, Mr. Gardella attended Clark University in Worcester, MA.

There are a multitude of definitions for the term homeland security. What precisely constitutes a nation secure? And what balance must be employed to ensure that such safety does not lie in the marginalization of the freedoms all citizens desire? The pursuit of academic insight and understanding will guide our nation's pathway to security. The questions that such analytical pursuits generate will give rise to answers within uncertainty. Uncertainty will remain a constant in the terrorist equation, an element of every question regarding terrorism. It is a surety that such questions need to be continuously addressed.

The concept of homeland security, or the ideal of a safe and secure nation, is not new. It is not a recently contrived or generated thought or purpose, catalyzed by the events of September 11, 2001. The tenets of a safe and secure nation existed even before our nation states coalesced into a united political and governmental structure. It is the continuance of an existing ideal, more sharply illuminated by the September 11th tragedy, which has narrowly focused our perception upon this purpose. The September 11th terrorist attack has immeasurably and forever altered America's perception of what constitutes a secure nation. There can be no singularly applied investment or strategy which will yield a safe and secure homeland. But the premise underlying the connective applications of this objective contains a thread of commonality. What reveals this similarity? What derivative underlies the vast investments made into answering the question: in what direction must our nation focus its security efforts?

The single most important aspect of homeland security has been, and will be, the dedicated investment in academic research and inquiry led by our nation's institutes of higher education and learning. Insight and direction are gained with knowledge and understanding. But within the clarity of insight lies a complexity which reveals both the dynamic nature of the threat and the vulnerable nature of our nation's infrastructure.

A DYNAMIC THREAT

Terrorism, by its very nature, employs a hidden and shrouded operational method. Uncertainty as to where, when, or how terrorists may strike deepens our fear of the terrorist agenda. Additionally it scatters the finite resources available to protect and secure our nation's infrastructure. Threats against the nation that were once orderly in nature now display the highest states of disorder, the resulting entropy leads to uncertainty as to how such threats can be surmounted. The allocation of limited resources cannot protect every structure, harden every target, secure every length of border, or encase the nation in a totally secure or impenetrable position. Therefore what discrete steps may be taken to achieve the daunting task of securing a nation which bases its existence on openness and freedom? The best and most informed manner in which that question can be answered is through academic research and inquiry.

Finite resources demand the selective and intensive scrutiny of critical insight and analysis. There is no aspect of human endeavor where academic inquiry has not led to a higher understanding of a problem and therefore a basis on which to proceed toward a solution in an educated and informed manner. Research into the operational methods and philosophical underpinnings of particular terrorist entities, foreign or domestic, will provide a pathway for securing our nation based upon clearly defined analytical interpretations. The knowledge gained through such academic pursuits will allow limited resources to be directed to significant areas of concern or risk. Areas that are deemed essential and assigned risk profiles – qualifying such areas as having a dynamic and cascading domino effect on the volatility of succeeding infrastructures – must be identified. A clear and precise accounting of our nation's infrastructure and the closely paralleled and linked systems upon which such infrastructure depends, must be undertaken to illuminate which areas deserve the highest consideration.

The terrorist operational methodology, employing an asymmetrical approach, particularly enforces the necessity to examine the executed terrorist operations – both discretely and within the totality of the circumstances inherent in such attacks. Every terrorist attack perpetuated by a particular and distinct organization has a certain linkage to other attacks – even if such linkage is formed only by a thin and slightly similar philosophical or operational agenda. Terrorism is a defined means to achieve a sociological or political objective in which fear and intimidation play a central role. The purpose and intent of such an incident sheds light on the effects the terrorist entity desires to achieve and provides insight into how a particular organization wishes to carry out its intended goal.

How can academic inquiry lead to a safe and secure Homeland? Through quantitative study and analysis the terrorist structure and operational functionality can be "reverse engineered" (borrowing a term associated with the applied science of engineering). The terrorist actions, through careful examination, inspection, and study, will yield the information through which the structural and operational functionality of the terrorist organization is exposed and will further reveal the mechanism for response.

It is difficult (if not impossible) to assign any degree of certainty to such events which, by their very nature, incorporate such a dynamic and non-linear basis of function. Once rigid and stabilized threats against the United States, that were clearly defined and readily discernable, now have fractured into an unstable and chaotic threat potential. The terrorist operational method purposefully employs such characteristics and uncertainty has become a most effective weapon of choice.

STRUCTURES OF UNCERTAINTY

The structure of a complex organization often provides a very real insight into how the organization plans to accomplish its goal. The mechanics of structure portray the operational functionality of the organization. But the fractured cellular nature of terrorist organizations and their lack of a clearly defined structural apparatus produces uncertainty of how the terrorists plan to achieve their objective. This uncertainty is woven as a fiber into the methods employed by the terrorists and results in a lack of a clear perception as to where, when, or how the threat will be manifested. This disordered structure assists the terrorist entity by prohibiting a definitive course of preventative action. This is particularly applicable when limited resources prevent the securing of every point of vulnerability. At any given moment, the threat to our national security remains intact.

How is it possible for academic research and study to provide a solution to the complex nature of this type of threat? Despite the fact that the United States has the most technologically advanced military in the world, employing the most highly trained and well equipped soldiers in the world, our nation remains at risk. Some have argued that it is only a matter of time before the United States once again suffers an attack similar in size and pernicious intensity to the September 11th terrorist attack. The utilization of a chemical, biological, or nuclear component in such an attack remains a possiblity and certainly remains a favorable and potentially desired method for the terrorist community.

Uncertainty is the hallmark of complexity. But the complexity of the terrorist ideal demands the rational insight gained from academic investigation. Solutions may be derived as to how to effectively secure the nation by assessing the vulnerability of the nation's infrastructure. Research must span the entire spectrum of terrorist operations. Funding of academic research must be a priority and must be strengthened. The course of action yielded from this approach will illuminate where finite resources can be applied to diminish the terrorist objective.

THE ACADEMIC INVESTMENT

What course of human conduct has not been touched by academic insight? Our nation's academic and research institutions have established a superior and unsurpassed perspective into almost every area of human endeavor. The capacity to formulate solutions to highly dynamic and complex problems requires a sustained academic expenditure. Practical and common sense solutions are derived from the results of such academic inquiry. Research requires a constant and prolonged financial infusion. The federal

government of the United States, charged with the task of protecting every citizen, must directly invest significant financial resources into our nation's academic institutions.

The threat to our nation's security is no longer symmetrical in appearance, form, or function. But the lack of a uniform threat mandates the necessity of a clear academic understanding. The application of technologically advanced solutions must be tempered with knowledge. There can be no replacement for a clear and rational understanding of the complex blueprint of national security. Uncertainty will remain a definitive element of the process of understanding, but uncertainty can be diminished by perspective.

But uncertainty may lead to an undesired and counterproductive end result, based on what the terrorist desired to achieve. The consequence of uncertainty has affirmed the necessity of vigilance. The recognition that vulnerability lies at the hub of the terrorist wheel has led institutions to question and refine the definition of what constitutes a secure homeland. What was once a nation that never envisioned the totality of terror wrought from the September 11, 2001 terrorist attack on New York City, now realizes that the security of our nation forever lies within the nature of our preparation. Preparedness must employ a decisive recognition that through academic research and inquiry the path to a secure homeland will be resolved. Uncertainty will always remain a definitive element of this task. Through knowledge and understanding, the precise nature of what lies ahead may be determined. The smallest and most imperceptible detail forms a part of the fabric of solution. Academic institutions have no rival in their ability to address highly complex and analytical problems. That ability will lead to answers as to how our nation will achieve security.

There are a multitude of definitions for the term "homeland security." There are a multitude of questions as to how to precisely achieve this most highly prized and desired objective, of which academic research and inquiry is our nation's most secure investment.

MAKING CONSEQUENCE MANAGEMENT WORK: APPLYING THE LESSON OF THE JOINT TERRORISM TASK FORCE

Will Goodman

Will Goodman serves as the assistant for plans to the Assistant Secretary of Defense for Homeland Defense & Americas' Security Affairs. In this role, Mr. Goodman oversees operational and contingency plans on behalf of the Assistant Secretary. He also participates in National Level Exercises and manages several counterterrorism projects and portfolios. Mr. Goodman is a recipient of the Office of the Secretary of Defense Exceptional Civilian Service Award. The views expressed in this article are those of the author and do not necessarily represent the views of the Department of Defense, its components, or the United States government. Mr. Goodman can be reached at william.goodman@osd.mil.

ROLLED UP

At about 9:00 p.m. on May 7, 2007, Dritan and Shain Duka arrived at a home in Cherry Hill, New Jersey. [1] They had an important meeting that night—a meeting long in the making. They rang the doorbell and waited. Their appointment was to purchase AK-47 and M-16 assault rifles, the first installment of weapons needed for a terrorist attack against targets in the U.S. The Dukas must have been nervous; Osama bin Laden himself had not successfully attacked the United States at home since September 11th. The Dukas probably did not attribute al Qa'ida and bin Laden's failure to an innovation in U.S. government counter terrorism organization. Perhaps they should have. Members of the South Jersey Joint Terrorism Task Force (JTTF) closed in, arresting the Dukas and four other alleged co-conspirators. Work by the JTTF, involving law enforcement personnel from a sweeping range of local, state, and federal agencies, had turned a single tip into six arrests.

That tip, from Circuit City clerk Brian Morgenstern, began an eighteen-month long investigation by the South Jersey JTTF. [2] Over a year and a half, the JTTF tracked the suspects and their activities by drawing on the expertise, contacts, and unique knowledge of individual JTTF members from law enforcement agencies at every jurisdictional level. The team collaborated to build an investigation on thorough and convincing evidence of the suspects' conspiracy to attack the U.S. Army base at Fort Dix, New Jersey, as well as possibly other military bases and public

events. On May 7, 2007, the "Fort Dix Six" were arrested and accused of conspiring to commit murder. Since that time, one of the conspirators has pled guilty to weapons charges. The other suspects await trial.

HOMELAND SECURITY AND INNOVATING BUREAUCRATIC ORGANIZATION

The Joint Terrorism Task Force is a homeland security success because of the "mission-first" attitude inherent to its organization. The JTTFs, as "cross-functional teams," are composed of officers from nearly every major law enforcement entity in the United States. This organization makes the mission paramount by subordinating traditional institutional and bureaucratic boundaries to the critical counterterrorism tasks at hand. The fact that terrorists have not successfully conducted a domestic terrorist attack against the United States is not an accident and is not for lack of effort on the terrorists' part. Dr. James Carafano of the Heritage Foundation notes at least sixteen major terror plots disrupted by U.S. law enforcement since the World Trade Center attack. [3] The case of the Dukas' conspiracy is just one thread in a tapestry of counterterrorism and homeland security successes by the JTTFs since 9/11.

Consequence management, the ability of the U.S. government to respond to and recover from a devastating terrorist attack or natural disaster, will be the most critical element of homeland security success in the future. Even if we are able to prevent every future terrorist attack, the U.S. government must still be capable of responding to catastrophic natural disasters to save lives and diminish damage to property. As President Bush and others have said, while the U.S. government must be right every time, the terrorists need only be lucky once. Hurricane Katrina painfully demonstrated that when local, state, and federal agencies respond to catastrophes, the whole is far less than the sum of its parts. Though some progress is being made, observations from the most recent National Level Exercises and observations recorded in the 2006 *Katrina Lessons Learned Report* still reflect that mission success in consequence management takes a backseat to parochialism among departments and agencies. [4]

This essay identifies what makes the JTTF successful and applies those lessons to the planning and execution of consequence management operations. The first section of the essay addresses the Department of Justice charter for preventing terrorist attacks and the history of the JTTF as the context for its organizational arrangement and success. The second section proposes applying a structure similar to that of the JTTF to U.S. government consequence management planning and execution.

EXPLORING THE SUCCESS OF THE JOINT TERRORISM TASK FORCE

The JTTF is structured to meet mission requirements rather than managerial vision *per se*. Former President Clinton's *Presidential Decision Directive – 39* validated and reaffirmed a long-accepted view that law enforcement, in particular the FBI, leads the domestic counterterrorism mission. [5] Those responsible for accomplishing this mission, FBI special

agents in the field, recognized that they could never succeed without the help and contributions of all other stakeholders. The normal organization of the FBI was insufficient to cover the totality of their responsibilities.

The FBI accepted the interagency task force as the best mechanism for integrating all local, state, and federal stakeholders into the counterterrorism mission. The FBI first explored flexible interagency task forces in 1979 with criminal bank robbery investigations in New York City. [6] This criminal task force featured a single location with personnel from the FBI, New York State, and New York City law enforcement agencies and was a major success. In May 1980, FBI special agents decided the interagency task force organizational arrangement was the mechanism they needed to accomplish the counterterrorism mission. The New York City Task Force responded to terrorist threats by Puerto Rican separatists, the Weathermen Underground, and violent elements of the Black Panther Party that were joining together. "Out of necessity," notes Supervisory Special Agent Brad Swim of the National Joint Terrorism Task Force, "New York ventured into the Task Force concept for the JTTF."

Since that time, the JTTF has become the federal model for the counterterrorism mission. As of October 2007, 102 JTTFs operated full-time, with just over half their personnel from the FBI, 25 percent from state and local law enforcement, and 21 percent from other federal law enforcement agencies. [7] Individual JTTFs have no set staffing pattern; staffing, like counterterrorism investigation, is a franchise responsibility. State and local law enforcement agencies offer their personnel for detail to the local JTTF because of the valuable networking and investigative experience they gain. The broad acceptance of the concept and its record of terrorism prevention strongly suggest that the JTTF works.

The core principles of synergy and task orientation make the JTTF successful. Ideally, JTTF members assigned by their parent agency are full partners in every aspect of JTTF operations without regard to which federal, state, or local law enforcement agency employs them. [8] The individuals working at the JTTF who are not FBI personnel provide valuable reach back and collaboration with their parent agencies, but their daily assignments and investigative duties support only JTTF operations. This arrangement avoids supervisory conflicts. The regular cycling of employees from other law enforcement agencies to the JTTF facilitates a level of information sharing and collaboration that would be impossible in separate organizations that meet and share information only occasionally. The JTTF, representing the work of all area law enforcement in countering terrorism, exemplifies government operations that add up to more than the sum of their parts.

Applying the Success of the JTTF to Consequence Management Operations

Public and private sector studies on "matrix organizations" and "cross-functional teams" describe why the principles of the JTTF work well. According to a Government Accountability Office (GAO) report, "collaboration can be broadly defined as any joint activity that is intended to produce more public value than could be produced when organizations act alone." [9] The GAO contends this extra value is generated through a defined and articulated common outcome; mutually reinforcing or joint strategies;

leveraging common resources; agreed upon roles and responsibilities; and compatible policies and procedures among other elements. All these points are exemplified by the JTTF organization. Private sector organizational theorists Donald Cushman and Sarah King call this "cross-functional teamwork," [10] which enhances organizational efficiency by "effective removal of all the artificial barriers between functional units along the value chain of the firm." Cross-functional teamwork also facilitates "cooperation between people from different traditional organizational units," eliminating problems which plague a company or its customers as a result of a cross-functional dispute where no one entity controls the process. Finally, "cross-functional teams facilitate intraproject and interproject cooperation." These qualities, found in the JTTF, are absent from U.S. government consequence management operations where institutional boundaries are paramount over mission success.

Cushman and King identify a major reason why consequence management operations fail. They aptly, albeit pessimistically, state that "people who work in different functions [organizations] hate each other." [11] The JTTF, as a cross-functional team, makes the traditional jurisdictional disputes of law enforcement irrelevant by reorienting everyone towards the same goal on the same team. The *National Response Framework (NRF)*, the updated guidelines for U.S. government consequence management, often confuses the reader with multiple goals under several command structures in numerous offices across different locations. Rather than upsetting the traditional authorities and their corresponding budgets, the *NRF* at times seems to reinforce the primacy of institutional boundaries at the expense of the mission. The overlapping responsibilities of the National Interagency Fire Center (NIFC) and the National Response Coordination Center (NRCC) serve as an example. While the NRCC is the coordination center for all disasters in the United States, the NIFC acts as another coordination center for only fire emergencies. While both these staffs work hard to support senior leader decision makers, having two operations centers, where one could suffice, creates a needless opportunity for confusion. Firefighters and decision makers may be left perplexed about whose information is correct and who is really in charge.

Observers should not be surprised that the JTTF has enjoyed success; after all, it has gone farther than most elements of the U.S. government to institute the cross-functional team model. In *Managing the Public Organization*, Cole Graham and Steven Hays articulate the vision of cross-functional teams (also called matrix organizations):

> In matrix organizations, the various specialists are joined in a common purpose, thanks to their membership on a team that is supervised and coordinated by an individual with responsibility for achieving a defined set of project goals. Meanwhile, however, their ties to their functional departments are not entirely severed…in addition to enabling managers to coordinate specialists more effectively, matrix organizations have achieved a reputation for creating work environments that are highly motivating and productive of innovations. [12]

In his book, Richard Daft outlines three conditions that precipitate the need for matrix organizations. [13] The cross-functional team is the most desirable approach when two or

more critical sectors compete for lead responsibility in a task area; when the task environment is complex and uncertain; and when an economy of scale is required to conserve resources. No U.S. government mission reflects these three conditions more than consequence management operations. Our Federalist principles will not allow a single U.S. government entity to own all aspects of consequence management. [14] Cross-functional teams must solve the problems posed by consequence management.

The federal government should adopt a sensible process for consequence management planning and execution at the headquarters level, [15] and nominate a single cross-functional team under an individual department or agency for each step of that process. This assembly line would consist of cross-functional teams with members from all federal departments and agencies and some state, local, non-profit, and private sector entities that are owned and housed by a lead department or agency. An example process is outlined below: [16]

- *Threat Analysis* – completed by a cross-functional team under the director of National Intelligence, identifies which missions demand imminent preparation;
- *Strategic Guidance Statement* – completed by a cross-functional team owned by the White House Homeland Security Council, establishes the goals for planning;
- *Deliberate Planning Process* – completed by the Incident Management Planning Team (IMPT), a cross-functional team already in existence and owned by the Department of Homeland Security (DHS), produces the following:
    - *analysis of the mission based on the strategic guidance, with IMPT team members obtaining feedback from their parent organizations;*
    - *a concept of operations to be approved by each parent organization; and*
    - *a full deliberate plan for review and approval by the senior leaders in each representative organization;*
- *Crisis Action Plan* – completed by a cross-functional team in the DHS National Operations Center (NOC) no more than twenty-four hours after a contingency occurs, fills in the holes of the IMPT's deliberate plan with the event's details; and
- *Mission Assignments* – completed by a cross-functional team in the Federal Emergency Management Agency NRCC, gives specific orders for every actor in the crisis to conduct their missions according to the plan produced by the NOC.

This process, based on cross-functional teaming, guarantees a collaboratively-developed, collaboratively-executed consequence management operation at the federal department and agency level.

While fully reorganizing the federal government consequence management planning and execution system into cross-functional teams is revolutionary, there are some indications that such a change may be underway. DHS, created in the aftermath of 9/11, aspired to the effects of a cross-functional team but failed to institute the concept as designed. The IMPT theoretically is a cross-functional team, but so far has only a low level of representation from organizations outside DHS. The IMPT is a cross-functional team for deliberate planning, but federal department and agency headquarters also need cross-functional teams to identify threats, provide strategic guidance, and then turn deliberate plans into

crisis action plans and mission assignments. Our current piecemeal initiatives are well-meaning but miss the mark. Real success in consequence management operations will require a revolution of the bureaucracy, with cross-functional teams as the organizing principle.

CONCLUSION

Our nation's federalism guarantees that we will continue to have essential responsibilities dispersed across many organizations at the federal, state, and local levels of government as well as non-profit and private sector organizations. To avoid the inevitable confusion created by diffuse responsibilities across multiple layers of government in a crisis situation, we need to adopt cross-functional teaming on a grand scale. The JTTF has demonstrated the manifold benefits of cross-functional teams by demonstrating success in counterterrorism. The American people deserve the demonstrated success of cross-functional teaming for consequence management, the most critical future aspect of homeland security.

---

[1] Michael Drewniak, *Five Radical Islamists Charged with Planning Attack on Fort Dix Army Base in New Jersey* (U.S. Department of Justice, U.S. Attorney, District of New Jersey, Public Affairs Office, May 7, 2007) http://www.usdoj.gov/usao/nj/press/files/pdffiles/duka0508rel.pdf

[2] U.S. District Court, District of New Jersey. *Dritan Duka Complaint* (n.d.), http://www.usdoj.gov/usao/nj/press/files/pdffiles/DukaDritanComplaint.pdf

[3] James Jay Carafano, "U.S. Thwarts 19 Terrorist Attacks Against America Since 9/11," *Backgrounder* No. 2085 (Washington, DC: The Heritage Foundation, Nov 13, 2007). While Dr. Carafano does not cite JTTFs specifically, since the JTTF is not the subject of his article, the media and FBI public affairs have identified several of the attacks such as the "Lackawanna Six" (http://www.fbi.gov/page2/dec04/jttf120114.htm, accessed August 14, 2008) and the Fort Dix Plot as apprehensions led by local JTTFs. The media articles Dr. Carafano cites report many of the other plots as apprehensions by "federal terrorism investigations" or "federal terrorism probes," in which the reader may reasonably infer JTTF involvement, if not JTTF lead action.

[4] Townsend, Francis Fragos, *The Federal Response to Hurricane Katrina: Lessons Learned* (Washington, DC: Government Printing Office, February 23, 2006). Available at http://www.whitehouse.gov/reports/katrina-lessons-learned.pdf. Accessed on August 14, 2008.

[5] Department of Justice, *Unclassified Summary of Presidential Decision Directive – 39* (n.d.) http://www.ojp.usdoj.gov/odp/docs/pdd39.htm.

[6] Special thanks to Unit Chief Gregory Massa and Supervisory Special Agent Bradley Swim of the National Joint Terrorism Task Force (NJTTF). All historical and procedural information on the JTTF is from an October 3, 2007, interview with them and other members of the NJTTF.

[7] Ibid.

[8] The FBI Office of the Inspector General (OIG) released a report on improving FBI Task Force operations (including the JTTF) in June 2005 (http://www.usdoj.gov/oig/reports/plus/e0507/exec.htm, accessed August 14, 2008). The OIG notes that the JTTF still has major work to do in training JTTF members; providing a standard orientation for new members to the JTTF and its functions; incorporating members from some federal agencies (i.e. the Drug Enforcement Agency); improving the work conditions and information technology access for some JTTF members; incorporating local law enforcement in remote areas; addressing staffing shortages and leadership discontinuity; and creating outcome, rather than output, performance measures, among other issues. Significantly, the OIG does not criticize (publicly, at least) the conduct of counterterrorism investigations or information sharing and cooperation by the different law enforcement entities present in JTTFs. Very few, if any, reports by the Government Accountability Office or Federal department or agency Inspectors General will offer ringing endorsements of government programs. But in this case, the FBI OIG states, "…the task forces and councils have

aided the Department's counterterrorism efforts…" Of course, they also recognize that the FBI can still improve its JTTF operations and performance measures. The recommendations made by the OIG reinforce cross-functional teaming by the JTTF and will likely further enhance JTTF operations in the future, if implemented.

[9] Government Accountability Office, *Practices that Can Help Enhance and Sustain Interagency Collaboration Among Federal Agencies* (Washington, DC: GAO, October 2005), 4.

[10] Donald P. Cushman and Sarah Sanderson King, *Continuously Improving an Organization's Performance* (Albany, NY: State University of New York Press, 1997), 103-105.

[11] Ibid.

[12] Cole B. Graham and Steven Hays, *Managing the Public Organization* (Washington, DC: Congressional Quarterly Press, 1986), 92.

[13] Richard L. Daft, *Organization Theory and Design* (St. Paul, MN: West Publishing Company, 1983), 237.

[14] Special thanks to Dr. Chris Lamb of the National Defense University and the Project for National Security Reform at http://www.pnsr.org/. His thoughts during an interview on 1 Oct 2007 and the work of PNSR published on their website contributed greatly to my thinking on interagency collaboration. Thanks also to Mr. Clark Lystra for sharing his broad knowledge of U.S. government consequence management.

[15] The reader should note that the *National Incident Management System (NIMS)* (available in draft at http://www.regulations.gov/fdmspublic/component/main?main=DocumentDetail&o=0900006480541f5a as of August 14, 2008) proposes a cross-functional incident management system at the local level, which is the first and most important level of incident management. However, as disasters exceed the capabilities or capacity of local and even state responders, federal departments and agencies must have a NIMS corollary at the headquarters level. Local Incident Commands experience cross-functionality to the extent that their command system leverages the cross-functionality of NIMS, and the federal government should enjoy the same cross-functionality for threat assessment, strategic guidance, deliberate and crisis action planning, and mission assignment. The failure of the government in major catastrophes like Hurricane Katrina can be explained, at least in part, by the absence of a NIMS-like cross-functionality at federal department and agency headquarters, leaving Cabinet-level decision makers unaware of what actions were not being taken, what actions were being taken, by whom, and on what timeline.

[16] The process described here is based on the process described in DoD *Joint Publication 5-0*.

PROLIFERATION OF BIODEFENSE LABORATORIES AND THE NEED FOR NATIONAL BIOSECURITY

Jesse Tucker

Jesse Tucker is a recent graduate of the University of Alabama at Birmingham School of Public Health, where he obtained a master's in public health (MPH) in epidemiology. While enrolled at UAB, Jesse served as a graduate assistant at the UAB Center for Emerging Infections and Emergency Preparedness. There he contributed to research on surge capacity networks for the National Center for the Study of Preparedness and Catastrophic Event Response (PACER), a U.S. Department of Homeland Security Center of Excellence. Mr. Tucker's research interest, in addition to emergency preparedness, is the epidemiology and pathology of emerging infectious diseases. He can be contacted at layden.tucker@gmail.com.

INTRODUCTION

The anthrax mailings that followed the terrorist airline attacks on the United States in September 2001 brought the threat of biological terrorism abruptly back into the national security spotlight, as well as into the collective consciousness of the American public. Those incidents demonstrated a key vulnerability in homeland defenses, and the United States government reacted accordingly. Between 2004 and 2007, the president issued three Homeland Security Presidential Directives (HSPDs) that specifically address the threat of biological weapons. Additionally, we have seen a profound increase in the number of high-level microbiology and biomedical research laboratories in the past few years. Currently, no single federal agency has a mission to track and regulate this ever-expanding network of laboratories. This represents a key gap in our efforts to ensure the provision of national security. The purpose of this essay is to summarize the provisions relating to biodefense contained within the HSPDs, to trace the proliferation of high-level biomedical research laboratories in the twenty-first century, and to recommend actions for safeguarding those laboratories and the citizens they serve.

HOMELAND SECURITY PRESIDENTIAL DIRECTIVES

The first, HSPD-10, addressed the needs of biodefense in the twenty-first century. [1] Specifically, this directive acknowledged the launch of the Proliferative Security Initiative to curb the international trafficking of weapons of mass destruction; established the BioWatch program to detect the use of biological weapons in U.S. cities; expanded the Strategic National Stockpile; launched project BioShield; provided funds to improve state and local health system capabilities; and, most importantly in my view, increased funding for bioterrorism research within the Department of Health and Human Services. HSPD-10

also contained provisions for "the pillars of national biodefense" which include threat awareness, prevention and protection, surveillance and detection, and response and recovery.

The second directive, HSPD-18, specifically addressed the need for "focused development of agent-specific medical countermeasures" for chemical, biological, radiologic, and nuclear (CBRN) emergencies. [2] The directive proposed a multi-agency, multi-sector strategic plan for production of such countermeasures and streamlined industrial collaboration. With specific regard to biological threats, the directive also addressed the need for unique countermeasures to combat not only traditional agents such as anthrax and plague, but also enhanced agents, emerging agents, and novel/advanced pathogens.

The most recent directive, HSPD-21, built upon the provisions in HSPD-10 to enhance public health and medical preparedness for biological attacks and other disasters. [3] It identifies biosurveillance, countermeasure distribution, mass casualty care, and community resilience as "critical components" of public health and medical preparedness and offers implementation actions for those components. Most importantly, this directive recognizes the urgency of establishing the discipline of disaster health in the public health and medical communities, a field which is still in its infancy.

The directives outlined above have accomplished many goals in biodefense and public health preparedness over the last few years, and homeland security has benefited from collaborations with other federal agencies, state and local agencies, and the private sector. In my opinion, the greatest and most visible result of these collaborations is the dramatically enhanced research involving emerging infections and biodefense in the United States. This increase in research activity can best be demonstrated by comparing the number of high-level biomedical laboratories prior to the renewed interest in preventing bioterrorist threats and after.

LABORATORY PROLIFERATION

The U.S. Department of Health and Human Services defines four biosafety levels (BSL) for laboratory activities involving infectious microorganisms. [4] They are designated in ascending order by the degree of protection required to safely work with the agents. BSL-1 laboratories involve well-characterized agents not known to cause disease in healthy adults and require no additional safeguards beyond standard microbiological practices. Labs operating at the BSL-2 level involve agents that may cause human disease and therefore utilize additional precautions and protective equipment. BSL-3 laboratories contain agents that pose serious or lethal health hazards to humans and must utilize even more restrictive practices and protective equipment. The highest level, BSL-4, involves extremely transmissible and highly lethal agents for which there may not be a vaccine or standard treatment. BSL-3 and BSL-4 laboratories are most relevant to this discussion.

In October 2007, the United States Government Accountability Office (GAO) issued testimony regarding oversight of the recent wave of new BSL-3 and BSL-4 laboratories. [5] That testimony observed that the number of BSL-4 labs has increased from five before the

2001 terrorist attacks to a present number of fifteen, including at least one in planning stage. For the majority of the last few decades, there were only two facilities with such capabilities: the federal laboratories at the U.S. Army Research Institute for Infectious Diseases (USAMRIID) in Fort Detrick, Maryland, and at CDC in Atlanta, Georgia. In the 1990s, three new BSL-4 labs were built at Georgia State University, at the National Institutes of Health in Bethesda, Maryland, and at a private facility in San Antonio, Texas. The GAO report observes that since 2001, at least nine new facilities are either fully operational, in construction, or in the planning process. Due to the extreme hazards of BSL-4 agents, they must be handled by workers wearing protective space suits in complete physical, biological, and spatial isolation in negative-pressure laboratories. Obviously such labs are extremely costly to operate, which explains their relative scarcity prior to events in the early twenty-first century. The expansion of BSL-3 laboratories since 2001 has been even more rapid. The GAO testimony points out that the number of such laboratories is practically unknown, but more than 1,300 BSL-3 laboratories are currently registered with either the CDC or the USDA under the auspices of the Select Agent Program administered jointly by those agencies. In addition, at least forty-six states have one or more state public health BSL-3 facilities for diagnostic and analytical purposes in support of emergency response.

As a consequence of the HSPDs outlined above, the federal government has poured billions of dollars into improving our research capacity for defending the nation from biological weapons attacks and the continuing threat of emerging infectious diseases. The laboratory expansions described in the paragraphs above are an example of continued success in this effort. It would be unwise, however, for this rapid rate of laboratory and research expansion to continue without regulating these many facilities and ensuring the safety of their employees and surrounding communities.

Safety Regulation and Oversight

Occupational accidents, equipment failures, employee complacency, inadequate standard operating procedures, theft, environmental release of pathogens, natural disasters, and terrorist attacks are all possible hazards of existing BSL-3 and BSL-4 laboratories, and the risk grows with every new lab constructed. The GAO testimony identified multiple recent accidents at such laboratories, including failure to report to CDC exposures to select agents in 2006 at a laboratory at Texas A&M University and a power outage at a BSL-4 facility at CDC in 2007. It is worth considering that these are only a sample of the *reported* laboratory accidents and safety infractions. Due to the independent nature of many of these laboratories, lapses in containment and security may go unreported in order to avoid public embarrassment and guarantee additional government funding.

According to the GAO testimony, the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 made significant revisions to the Select Agent Program and placed restrictions on access to select agents and the facilities using them. CDC is responsible for the registration and oversight of laboratories that possess, use, or transfer select agents that pose a threat to human life, and USDA conducts similar activities for laboratories that possess, use, or transfer select agents that pose a threat to plants or

animals. However, no single federal agency has an official mission to track the number and activities of high-level research laboratories. According to a survey implemented by the GAO and discussed in the testimony cited above, a number of agencies (including the Department of Defense, OSHA, the State Department, and EPA) have a need to track the number and activities of a subset of such laboratories that directly support their missions, but none is responsible for determining the aggregate risks associated with the recent proliferation. According to the GAO testimony and federal agency officials, oversight of these BSL-3 and BSL-4 facilities is fragmented and relies primarily on self-policing.

We should be aware that lapses in biosecurity may have consequences beyond the occasional employee illness or environmental contamination. According to CDC, there is a baseline level of risk associated with any high-containment scenario. With the decentralized expansion of BSL-3 and BSL-4 laboratories these risks are sure to increase. Even labs with sophisticated security and containment procedures have experienced safety failures, such as the *Brucella* exposure incident at Texas A&M University in 2006. [6] The GAO testimony highlights that since the full extent of the recent expansion is not known, it is unclear how the federal government will create sufficient capacity to regulate the growing network of facilities.

Ensuring the long-term capacity to safeguard our network of biodefense research laboratories will not be a simple task. The long list of federal, state, and private stakeholder agencies involved in this endeavor should consider delegating the responsibility for tracking BSL-3 and BSL-4 expansion to a single agency, or perhaps creating a multi-agency clearinghouse with a specific mission to monitor these activities. Additionally, there should be a coordinated effort by these agencies to develop a national research agenda for studying select agents. This action would not only result in a more efficient and productive national biodefense research initiative, but also a safer national biodefense research initiative. Having twenty laboratories investigating anthrax virulence factors might generate more publications and disseminate knowledge more rapidly, but the distribution of so many samples of a high-priority select agent could pose an elevated aggregate risk for lapses in safety and security precautions. The responsible agencies should resolve to maximize the potential of our nation's research facilities while ensuring a maximum level of preparedness and security infrastructure.

CONCLUSION

I conclude this essay by referring to the classic example of laboratory disaster, an episode in human history that to most people is only a ghost memory. In 1979 in Sverdlovsk, Soviet Union (now Yekaterinburg, Russia), ninety-four people became infected with anthrax, sixty-four of whom died over a period of six weeks. Although the cause of this strange outbreak was denied for years by the Soviet Union, it eventually became clear that anthrax spores had accidentally been released into the air from a nearby military research facility. [7]

When research of this importance is conducted, every effort must be made to ensure the safety and security of both the research entity as well as the surrounding community. We have taken so many steps in the right direction over the last five or six years, we are bound

to take a few backwards. Given the urgency of matters related to biological terrorism and the adolescent nature of disaster preparedness in the United States, we must make sure that our gains do not make us more vulnerable.

---

[1] The White House, Biodefense for the 21st Century (2004), http://www.whitehouse.gov/homeland/20040430.html.
[2] The White House, Medical Countermeasures Against Weapons of Mass Destruction (2007), http://www.whitehouse.gov/new/releases/2007/02/20070207-2.html.
[3] The White House, Public Health and Medical Preparedness (2007), http://www.whitehouse.gov/news/releases/2007/10/20071018-10.html.
[4] J.Y. Richmond and R.W. McKinney, Biosafety in Microbiological and Biomedical Laboratories, 4th ed. (Washington, DC: U.S. Government Printing Office, 1999).
[5] K. Rhodes, High-Containment Biosafety Laboratories: Preliminary Observations on the Oversight of the Proliferation of BSL-3 and BSL-4 Laboratories in the United States, GAO Testimony Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives, October 4, 2007, GAO-08-108T. All references to "GAO Testimony" refer to this document.
[6] J. Kaiser, "Accidents Spur a Closer Look at Risk at Biodefense Labs," Science 317 (2007):1852-1854.
[7] M. Meselson, J. Guillemin, M. Hugh-Jones, A Langmuir, I. Popova, A. Shelokov, and O. Yamplolskaya, "The Sverdlovsk Anthrax Outbreak of 1979," Science 226 (1994):1202-1208.