DEFENDING THE AMERICAN HOMELAND
1993-2003

by

Randall J. Larsen
Patrick D. Ellis

The Counterproliferation Papers
Future Warfare Series No. 20
USAF Counterproliferation Center

Air University
Maxwell Air Force Base, Alabama

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
NOV 2003		**00-11-2003 to 00-11-2003**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Defending the American Homeland 1993-2003	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air University,USAF Counterproliferation Center,Maxwell AFB,AL,36112-6427**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**56**	

Defending the American Homeland
1993-2003

Randall J. Larsen
Patrick D. Ellis

November 2003

The Counterproliferation Papers Series was established by the USAF Counterproliferation Center to provide information and analysis to assist the understanding of the U.S. national security policy-makers and USAF officers to help them better prepare to counter the threat from weapons of mass destruction. Copies of No. 20 and previous papers in this series are available from the USAF Counterproliferation Center, 325 Chennault Circle, Maxwell AFB AL 36112-6427. The fax number is (334) 953-7530; phone (334) 953-7538.

Counterproliferation Paper No. 20

USAF Counterproliferation Center

Air University

Maxwell Air Force Base, Alabama 36112-6427

The Internet address for the USAF Counterproliferation Center is:

http://www.au.af.mil/au/awc/awcgate/awc-cps.htm

Contents

Disclaimer

The views expressed in this publication are those of the author and do not reflect the official policy or position of the U.S. Government, Department of Defense, or the USAF Counterproliferation Center.

The Authors

Randy J. Larsen is the Director of the Institute for Homeland Security as well as a Vice President for ANSER Institute for Homeland Security. He has a Master of Arts degree in National Security Studies from the Naval Post Graduate School. He is a member of the Defense Science Board, and serves on the editorial board for Johns Hopkins University's quarterly journal, *Bioterrorism and Biosecurity: Biodefense Strategy, Practice, and Science*. Since 9-11, numerous senior government officials, including Vice President Cheney and Governor Ridge, have sought his advice and counsel. He has served as an expert witness in hearings held by the Senate and the House of Representatives and provided informational briefings to numerous Members of Congress, the military, the Intelligence Community, and business audiences. He is a co-author of The *Executive's Desk Book on Corporate Risks and Response for Homeland Security*, published in March 2003. He develops and teaches graduate courses in homeland security at George Washington University, Johns Hopkins University, and the National War College. During the past eight years, he has written and lectured extensively on the subjects of asymmetric and biological warfare and the 21st-century challenges of homeland security. He has a co-developer of the nationally acclaimed DARK WINTER exercise. In June 2000, Colonel Larsen retired following 32-years of military service in the Army and Air Force.

Patrick D. Ellis, WMD/Homeland Security Analyst to the USAF Counterproliferation Center, specializes in WMD Terrorism, Homeland Security, and Disaster/Emergency Management issues. He has lived, traveled, and worked extensively in the United States, Europe and Asia. He holds a Bachelor of Arts Degree from the University of Maryland in Asian Studies/Government and Politics and a Master of Public Administration degree from the University of Oklahoma. He completed specialized courses at the Defense Nuclear Weapons School, U.S. Army Chemical School, and USAF Special Operations School. His non-military WMD experience includes Department of Justice sponsored training from Louisiana State University, Texas A&M, the Department of Homeland Security's Center for Domestic Preparedness, and Bechtel Nevada's

Counter Terrorism Operations Support. Other education and training accomplishments include a University of Maryland Certificate in Korean Studies; the Air University's Academic Instructor School; and the College of Aerospace Doctrine, Research, and Education's *Contingency Wartime Planners* and *Information Warfare Applications* Courses. Mr. Ellis participated in WMD exercises such as Consequence Island 2001 (Puerto Rico), Consequence Management 2000, and Launch Relief 2000. In addition, he planned and participated in various field study trips to Federal, State and local Counterproliferation and WMD response organizations. Mr. Ellis developed and taught WMD- related lessons for the Air Force Institute of Technology, the Air War College, and the Ira C. Eaker College for Professional Development's USAF On-Scene Commanders course. He is currently working on a monograph addressing Response to CBRNE Terrorism issues.

Defending the American Homeland
1993-2003

Randall J. Larsen
Patrick D. Ellis

I. Introduction

> *Defending our Nation against its enemies is the first and fundamental commitment of the Federal government. Today, that task has changed dramatically. Enemies in the past needed great armies and great industrial capabilities to endanger America. Now, shadowy networks of individuals can bring great chaos and suffering to our shores for less than it costs to purchase a tank. Terrorists are organized to penetrate open societies and to turn the power of modern technologies against us.*
>
> President George W. Bush
> The National Security Strategy of the United States
> September 20, 2002

On September 20, 2001, the developers of the nationally acclaimed DARK WINTER exercise met with Vice President Cheney and his staff to discuss the lessons learned from this simulated smallpox attack on America.[1] The Vice President asked, "What does a biological weapon look like?" One of the briefers reached into his pocket and pulled out a small test tube filled with a white powder. "Sir," he said as he eyed the two Secret Service agents standing by the door, "It looks like this…and by the way…I did just carry this into your office."

The powder was weaponized *Bacillus globigii*. Genetically, it is nearly identical to *Bacillus anthracis*—the bacteria that causes anthrax. However, *Bacillus globigii* is frequently used as a simulant. Most nations that have weaponized anthrax, including the United States, the Soviet

Union, and Iraq, first weaponized *Bacillus globigii* to test their production and delivery processes. Being weaponized means it has been produced at the three to five micron size, perfect for release in the air (a human hair is about 100-microns wide).

"Three decades ago," the briefer continued, "only large industrial nations had the technical capability to produce such a weapon. However, due to the revolution in biotechnology, this sample was produced with equipment bought on the Internet for less than $250,000." [2]

Three-weeks following this conversation, Robert Stevens, a photojournalist for American Media, Inc., in Boca Raton, Florida, died from inhalational anthrax. Other U.S. deaths from anthrax-laced mail followed. During the next several weeks, citizens across the nation began to question their security. Major newspapers stopped accepting letters to the editor, farmers in Iowa wondered if it was safe to open their mail, and most Americans began to appreciate how technology had changed the international security equation.

In 1828, a young Abraham Lincoln said, "No European or Asian power, even with a Bonaparte in command, could march across this continent and take a drink of water from the Ohio or make a track on the Appalachian Trail."[3] This is still true, but today it is irrelevant. America's enemies no longer need to put an army on our soil or missiles in our skies to threaten our homeland. A secure homeland is no longer an American birthright. It now must be earned, and it is a challenge that will neither be cheap nor easy.

Homeland security is the most complex endeavor this nation has ever faced. Some see this new mission as just an evolutionary step in the national security process. This is not the case—it is a change in kind, not degree. For most of our history, national security took place in Washington, D.C. and overseas. The key players were all in the federal government, most notably, the Departments of Defense, State, and the Intelligence Community.

Today there are 57 federal agencies, 50 states, 8 territories, and 3,066 counties involved in U.S. homeland security. In fact, there are 87,000 different governmental jurisdictions that will play roles in homeland security.[4] Furthermore, the private sector will play a major role in homeland security, and this role will not be limited to logistical support.

Corporate America will be required to play a major operational role in homeland security.

The changes that have and will continue to occur make it difficult to even decide which questions to ask, much less, how to answer them. Perhaps the first step will be to change how we think about security in the twenty-first century.

A young reporter once asked Albert Einstein what his theory of relativity had changed. He thought about it for a moment and then said, "Everything…everything except the way people think." If we are to secure the American homeland from 21st century threats, we must learn to do something that is very difficult…we must change the way we think. Therefore, the purpose of this paper is to help the readers change the way they think about homeland security, no easy task.

II. Homeland Security in the 1990s

The current concepts of homeland security, protecting the homeland from large-scale attacks where small nation states or well-financed terrorists organizations would use weapons of mass destruction, began in late 1990 as America began preparing for a war with Iraq. This was the first war in at least 50 years where America seriously considered the possibilities of attacks on the homeland. New security procedures were introduced at airports, increased surveillance was conducted at border crossing points, and the Federal Bureau of Investigation (FBI) monitored the activities of Iraqis in the United States.

For most Americans, homeland security entered the common lexicon on September 11, 2001. However, American historians will likely say the modern era of homeland security began in 1993. Throughout the later half of the 20th century, terrorists had used small-scale attacks to bring attention to their causes. Some have described this as, "blow up something to get a seat at the table." In the 1990s, a new age of terrorism began to emerge. The attackers chose to remain anonymous, they had no specific demands, and their primary goal appeared to be the killing of large numbers of people. Some terrorists no longer wanted a seat at the table; they just wanted to "blow up the table." This new style of terrorism came to the American homeland on February 26, 1993.

World Trade Center Bombing 1993

On February 26, at 12:18 p.m., a large explosion ripped through the B-2 level of the basement under the World Trade Center, creating an L-shaped crater measuring 130 by 150 feet across and approximately seven stories deep. Almost unbelievably, the blast and subsequent debris killed only 6, but injured more than 1,000 people. The explosion created acrid smoke, which rose up to the 46th floor. The bomb, 1,200 pounds of nitro-urea supplemented by hydrogen cylinders, created over 6,000 tons of rubble. Total property damaged was estimated at $300 million.[5] Four men led by Ramzi Yousef planned this operation some two months before the actual attack. The plan was to topple both of the twin towers.

Tokyo Subway 1995

For the next two years, the world was quiet in respect to major terrorist events. Then, on June 27, 1994, several terrorists released sarin nerve gas in an apartment complex in Matsumoto, Japan killing seven and sending over 200 residents to the hospital.[6] This was an indicator of things to come. A few months later, during the morning rush hour on March 20, 1995, this same Japanese domestic terrorist organization, Aum Shinryko (Aum Supreme Truth) released a crude form of sarin gas (GB) in the Tokyo subway.

The sarin attack on the Tokyo subway system killed twelve, injured several hundred, and traumatized thousands. The residents of Tokyo were fortunate the numbers were not higher. Aum's chemical team had been testing several chemical agents at a large ranch they owned in Australia. The quality of the sarin used in this attack was very poor because it came from a batch that had been hastily prepared the weekend before, after senior leaders in the Aum received a tip that their headquarters was going to be raided the next Monday by Tokyo police. Furthermore, the delivery system was primitive. Plastic bags filled with the poor quality sarin were placed on subway cars and punctured with umbrella tips. Had this been a high quality sarin delivered in a more sophisticated manner, casualties could have been in the hundreds or even thousands.

This attack initially appeared to be the first terrorist use of a weapon of mass destruction. However, documents presented during the criminal trials of senior Aum leaders painted a completely different picture. Between 1990 and 1995, the cult conducted at least 20 attacks using biological and chemical agents, 10 with chemicals and 10 with biological.[7] The cult had been experimenting with chemical nerve agents such as sarin, tabun, soman, VX, and other agents such as hydrogen cyanide, phosgene, and mustard blister agents. Their interest in biological agents included such agents as anthrax, Q fever, and hemorrhagic fevers such as Ebola. In the end, none of their biological attacks were effective, but they did have limited success in their chemical program. The Cult also had shopped for nuclear weapons components in the former Soviet Union, although little progress was made toward acquiring nuclear weapons.

Aum's subway attack released a floodgate of information on the Aum's extensive chemical and biological weapons development

programs—all undetected by the intelligence and law enforcement communities. It sent shock waves through the law enforcement, intelligence, and domestic and international law enforcement, intelligence, and first-responder communities, which first were shocked to realize the types of weapons that were being prepared and second, were surprised to discover the stated purpose of such attacks—the creation of mass casualty events for the purpose of toppling the government.

Despite the obvious differences between Aum Shinryko and Al-Qaeda in terms of culture, religion, and organization, their goals are nevertheless similar: to completely upset political and social order through the use of massively destructive weapons.

Murrah Federal Office Building, 1995

It has been said that whatever was left of America's innocence, in reference to terrorism, was lost on April 19, 1995, at 9:02 a.m. For the senior leadership in the Clinton Administration and Congress, the first responder community, and virtually all Americans who stared at TV screens that day, the nightmare had become reality. Catastrophic terrorism had come to the American heartland.

Initially, many assumed the attack came from Islamic fundamentalists, but in less than 24 hours an even more disturbing story emerged. Just like the Japanese had difficulty believing that some of their "own" could launch such a murderous attack on the Japanese homeland, Americans now had to deal with the cognitive dissonance of a homegrown catastrophic terrorist—a Gulf War veteran who intentionally parked a large truck bomb in front of a childcare center. Shock, horror, grief, and anger were the emotions of the day.

Timothy McVeigh and his accomplice Terry Nichols had built a 4,000-pound ammonium nitrate fuel oil (ANFO) bomb and placed it into a Ryder rental truck. McVeigh then drove it to the Murrah Federal Office Building. The front of the building was destroyed leaving 167 people dead and more than 500 injured. The eventual crime scene stretched over some 200-city blocks and the sheer magnitude of response agencies overwhelmed existing communications systems. Besides high physical and personal costs, mental health costs were $4.1 million during the following year and continues yet today.

While there are few similarities between the Al-Qaeda terrorist atrocities and Timothy McVeigh's Oklahoma City bombing, one commonality is apparent. None of the instigators had any hesitation or regret at killing innocents.

Nothing is more disturbing than to hear pundits and apologists for terrorists say, "One man's terrorist is another man's freedom fighter." There is a major difference between attacks on child-care centers, pizza parlors or high-rise office buildings and legitimate military targets. When the Marine barracks in Beirut was attacked with a truck bomb—some called it terrorism. It was not. A U.S. Navy battleship was sitting off the coast firing 1600-pound shells at military targets in Beirut. In response, an attack was launched on a U.S. military unit. Call it asymmetric warfare or guerilla warfare, but do not confuse it with those who intentionally bomb office buildings in New York City, subways in Tokyo, and childcare centers in Oklahoma.

Some looked at the 1993 attack on the WTC, the 1995 attacks on the Tokyo subway and the Federal Office Building in Oklahoma City as random events. Others realized that a new international security environment was about to emerge. One of those individuals representative of this new environment was arrested in Pakistan and returned to the United States for trial. His name was Ramzi Yousef.

The head of the FBI in New York, Bill Gavin, was escorting Yousef to New York City for arraignment. As the FBI helicopter flew up the Hudson River, Gavin eased the blindfold from Yousef's eyes, "Look down there,' …gesturing toward the twin towers. 'They're still standing.' Yousef squinted and looked out of the window. 'They wouldn't be, if I had had enough money and explosives,' he replied defiantly."[8]

III. The Role of the Commissions

The terrorist attacks in New York City, Tokyo, and Oklahoma City led to the appointment of several high-level commissions that would examine both the threat and America's state of readiness for this new type of catastrophic terrorism.

The first mention of the term *homeland security*, in a post Cold War government report, appeared in *Report of the National Defense Panel* (NDP) in December 1997. (Actually, it used the term *homeland defense* which was used interchangeably with homeland security for several years.) The NDP Report contained one paragraph on homeland defense:

Protecting the territory of the United States and its citizens from "all enemies both foreign and domestic" is the principal task of government. The primary reason for the increased emphasis on homeland defense is the change, both in type and degree, in the threats to the United States. Besides the enduring need to deter a strategic nuclear attack, the United States must defend against terrorism, information warfare, weapons of mass destruction, ballistic and cruise missiles, and other transnational threats to the sovereign territory of the nation. In many of these mission areas, the military will necessarily play the leading role; however, many other threats exist which will require Defense to support local law enforcement agencies, as well as a host of other federal, state, and local entities.

President Clinton signed Executive Order 13010 establishing *President's Commission on Critical Infrastructure Protection* (PCCIP). The report was released in October 1997. This was the first of several key commissions that laid the groundwork for how we understand homeland security today.

The initial charter of the commission was to look at all aspects of critical infrastructure protection, but the final report was almost exclusively focused on the cyber threat to infrastructure. According to Phil Lacombe, the Executive Director of The President's Commission on Critical Infrastructure Protection, the commission narrowed its focus because considerable work had already been accomplished on the physical vulnerabilities of critical infrastructure, but little had been done on the cyber threats. Four key infrastructures were initially identified: information and communications, banking and finance, energy (including electrical power,

oil and gas) physical distribution, and vital human services. The one element these infrastructures had in common was that they were each highly vulnerable to cyber attacks. In demonstration after demonstration, the commissioners were shocked to learn how easy it was to hack into systems. The report noted, "A personal computer and a simple telephone connection to an Internet Service Provider anywhere in the world are enough to cause a great deal of harm."

Highlights of the report included:

- Deregulation in the energy industry had driven corporations to look for ways to trim costs. This meant less redundancy. Energy systems were operating at near maximum capacity, so that even a minor event could cause a cascading effect. The report noted, "Because of the complexity, some of these dependencies may be unrecognized until a major failure occurs."

- The threats examined ranged from natural events and accidents to disgruntled employees, recreational hackers, criminal activity, and terrorism. The commission noted that most things entering the U.S. must go through some sort of screening: the Immigration and Naturalization Service (INS) screened people, the Postal Service examined the mail, airplanes pass through an air defense identification zone, trucks and containers are checked by border patrol and customs, food stuffs are inspected by Food and Drug Administration (FDA) and United States Department of Agriculture (USDA), but electrons, coming on the Internet enter this country every moment of every day, and nobody was checking.

- The commission also highlighted how outdated America's concepts of defense and prevention had become. They asked, "Who would be responsible for investigating a cyber attack?" According to the commission report, "With the existing rules, you may have to solve the crime before you can decide who has the authority to investigate."

The commission's number one recommendation (a recommendation that should be a top priority for all homeland security issues) was to develop a program of awareness and education. Additionally, they recommended a partnership with industry including the creation of the Infrastructure Sharing

and Analysis Centers (ISACs). ISACs would allow industry and government to share critical security information in an environment that would protect the proprietary interests of industry and the government from the Federal Advisory Commission Act restrictions.[9] Eight ISACs would eventually be created to bring together industry and government.

The **National Commission on Terrorism** was created by the 105th Congress and led by Ambassador L. Paul Bremer III.[10] The commission report, released in June 2000, concluded that international terrorists would impose an increasingly dangerous and difficult threat to the American homeland. The commission said that today's terrorists seek to inflict mass casualties, are less dependent on state sponsorship, and are forming loose transnational affiliations, making terrorists attacks more difficult to detect and prevent. They stated that this new type of threat would require significantly enhanced efforts by the U.S. Government.

The commission provided several recommendations; three of these would receive considerable attention after September 11th: (1) increased integration of law enforcement and intelligence communities, (2) creation of a cadre of FBI officers who would distill and disseminate terrorists information once it is collected, and (3) ensure that the U.S. firmly target intelligence collection on all states that support terrorists.

The commission also noted that terrorist attacks involving a biological agent or nuclear material, even if only partially successful, can profoundly affect the entire nation. Many in the press misinterpreted one recommendation. The report stated, "the Department of Defense must have detailed plans for its role in the event of a catastrophic terrorist attack, including criterion for transfer of command authority to DoD in extraordinary circumstances." Several major newspapers interpreted this to mean that DoD should have the lead role in consequence management. That was neither the intention of the commission, nor what the report said. Had the reporters read more than the executive summary they would have understood that this statement referred to a situation in which state and local authorities were completely overwhelmed and unable to respond to an incident, which was considered to be the extreme exception, not the rule.

The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, also known as the Gilmore Commission, named after its chairman, Governor James Gilmore

III of Virginia. This commission released its first report in December 1999, and issued its fifth and final report on December 15, 2003.[11]

The legislation creating this commission directed them to assess Federal efforts to enhance domestic preparedness and highlight deficiencies in federal programs for response to terrorist incidents using weapons of mass destruction. The first report introduced the debate: whether to focus on preventing and dealing with *high probability/low consequence* versus *low probability/high consequence* scenarios. The initial report from the Gilmore Commission acknowledged that the low probability/high consequence could happen, but chose to focus on high probability/low consequence. The report stated,

> Conventional explosives, traditionally a favorite tool of the terrorists, will likely remain the weapon of choice in near term as well…increasing attention must now also be paid to the historically more frequent, more probable, lesser consequence attack, especially in terms of policy implications for budget priorities or allocation of other resources, to optimize local response capabilities.

The report went to great length describing the current difficulties in acquiring and developing mass casualty weapons. They used the example of Aum Shinryko, a terrorist organization with several hundred million dollars in assets and "highly-educated scientists," who failed after numerous attempts to produce a successful biological weapons program. Information that was not available to the commission at that time, later explained why the Aum's biowarfare program failed. Court testimony revealed that the graduate student, who was directed to acquire the sample of *Bacillus anthracis* (anthrax) from a laboratory, got cold feet and instead provided a sample of anthrax vaccine.[12] Fortunately, it was the non-lethal vaccine strain that was mass-produced and released in 10 different attacks in Japan rather than lethal strains. The Gilmore report also stated many well-trained scientists worked on this program, when in fact, it was mainly chemists and physicians working on the bioweapons program. Not a single PhD level microbiologist participated in the program.

Nevertheless, the Gilmore Commission did provide several useful recommendations, primarily emphasizing the need for better cooperation and coordination of federal, state, and local governments, and a

reorganization of Congress to insure proper policies and funding were coordinated for homeland security. The commission also stated that more cooperation was needed to obtain and share information on terrorist threats at all levels of government.

Later Gilmore commission reports, released after the September 11th attacks, had a significantly changed attitude about weapons of mass destruction and became more in line with the recommendations of the initial Hart-Rudman report of September 1999.

The U.S. Commission on National Security/21st Century, also known as the Hart-Rudman Commission after its co-chairmen, Senators Gary Hart and Warren Rudman concluded that America will become increasingly vulnerable to hostile attacks, and that Americas will die in their homeland, perhaps in large numbers.[13] The two new threats they were most concerned about were the result of rapid advances in information and biotechnology. They said that terrorist organizations would attack not only humans but also the economic infrastructure of nations. They expressed concern about the porous nature of borders and also addressed numerous other challenges America will face in the 21st century not directly associated with homeland security, such as education and problems with the civil service system.

One of the most notable features of the third Hart-Rudman Report, released in February 2001, was the recommendation calling for the creation of the Department of Homeland Security. The vast majority of organizations consolidated into the new Department of Homeland Security in March 2003, were the same ones recommended two years earlier in the release of this report. In the summer of 2001, Representative Mac Thornberry (R-TX) used the commission report as the basis for the bill he introduced in the House of Representatives. This bill served as the blueprint for the legislation that eventually created the new department.

All high level commissions that studied the issue of homeland security came to similar recommendations, some more prescient than others. These commission reports, combined with the open testimony of the director of the CIA, George Tenet forewarned America of what was to come on 9-11. These reports were produced in a bipartisan manner by some of the most experienced national security leaders in the nation. Sadly, very few Americans listened.

IV. An Analytic Framework for Homeland Security

Homeland security in the 21st century presents America with an incredibly complex challenge. Despite the fact that a few high-level commissions, think tanks, and military schools had been examining the concept of homeland security since 1997, the vast majority of Americans first heard the term only after the attacks of September 11, 2001.

Following these attacks, a wide range of journal articles, congressional hearings and press reports began to examine this new security challenge. Traditional national security scholars and pundits soon learned that the analytical frameworks of the Cold War were inadequate for examining homeland security.

While some elements of the Cold War model remain relevant, such as deterrence, prevention, and retaliation, new elements such as crisis management, consequence management, attribution, and prosecution emerged. Furthermore, the national security framework of the Cold War was exclusively focused on activities of the federal government, primarily the Departments of State and Defense and the Intelligence Community. However, a complete analytic model of homeland security must be suitable for use by federal, state, and local government organizations, (ranging from defense and law enforcement, to public health, food security, immigration, and border control), plus the private sector.

The following framework was originally developed for a homeland security course at the National War College, and has evolved through several iterations during the past four years.[14] The most recent model, which is also known as the Strategic Cycle of Homeland Security, consists of six elements: deterrence, prevention, preemption, incident management, attribution, and response.

Deterrence must be a central element of any homeland security framework. The consequences of attacks on the homeland made possible with 21st century technology can be devastating. In some cases, modern technology could enable a small nation, or perhaps even a well-financed terrorist organization to bring a superpower to its knees. Therefore, our nation must have policies and postures that deter our enemies from attacking our homeland.

Classical deterrence is based on two elements: punishment and denial. The threat from both nation-state and non-state actors, who might employ nuclear and bio-weapons, demand a shift in how we practice deterrence. Throughout the Cold War, deterrence was based on mutual assured destruction—the ability to deliver incalculable punishment under any circumstance. Given the nature of modern homeland security threats, we must increase our ability to deter enemies by denying them the effects they seek. In some cases, this will be accomplished through methods, institutions, and programs that have not been considered elements of deterrence. In the past for example, a robust public health system that would significantly mitigate the effects of a biological attack, may act as a deterrent to biological terrorism. Would a nation-state or terrorist organization risk massive retaliation if it knew that America had the unquestioned ability to identify the perpetrator and significantly mitigate the affects of a biological attack? In the Cold War, civil defense was not a deterrent factor. This is not the case in the 21st century. Resource allocation should reflect this new reality. There will be times when our deterrence efforts fail, perhaps if only for the fact that some of our enemies may be undetterable. In those cases, the United States will have to rely on prevention capabilities.

Prevention incorporates a wide group of active and passive measures that can stop an attack. Our nation's prevention activities are defensive in nature and range from arms control treaties to aerospace, maritime, and land defenses to border control and other law enforcement measures. A former speaker of the U.S. House of Representatives stated that foreign aid such as "a Marshall plan for the Arab world" could help prevent terrorism.[15] Others say that searches for "root causes" are exactly the wrong strategy when responding to terrorist acts because it serves to legitimize the acts.[16] Because some modern attacks could take our nation beyond the point of recovery, our nation must also possess the capabilities and associated policies that allow us to preempt attacks on our homeland.

Preemption is the policy that is fraught with political and military risks. In the Cold War, preemption would have meant first use of nuclear weapons, possibly resulting in a global nuclear war. Further, aggressors have frequently cloaked their initiation of war with claims that they were only preempting an attack on their homeland. Preemption in the homeland security context does not have to call for the initiation of nuclear war or

occupation of another nation's territory. It will require the selective use of all elements of national power, to include military force and law enforcement to preempt terrorists before they launch their attacks. Preemption options can span the range from a precision-guided 2,000-pound bomb delivered by a B-2 bomber to an arrest by a U.S. law enforcement official working with allies in overseas nations.

Incident management combines two concepts that initially began in the Clinton administration under Presidential Decision Directive 39. PDD-39 coined the terms *crisis management* and *consequence management*. Crisis management begins the moment that intelligence information suggested an attack might occur and then until an actual attack occurred. The FBI was the lead agency for crisis management. In PDD-39, consequence management was defined as the effort to provide emergency services to government, business, and individuals to restore public health, safety, and the economy after an attack. For example, the direct economic impact of the 9-11 attacks on New York City was still clearly visible in the spring of 2003. According to the New York Times, more than 12,000 restaurant workers had been laid off due to a major downturn in tourism. Economic analysts have linked this to public concern over future terrorist attacks. The Federal Emergency Management Agency (FEMA) was the lead federal agency for consequence management.

There are several reasons the Bush administration chose to combine these two elements (crisis and consequence management) and refer to it as *incident management.* This aligns the terminology used by the President with the terminology that has been used many years by state and local first responders. These two elements also were combined because in some attacks, such as biological and cyber, there is significant overlap between the crisis and consequence management phases.

Attribution occupies a critical place in the homeland security strategic cycle. Our nation's enemies are likely to disguise their identity to avoid retaliation. The 1990's witnessed a new trend in terrorist activities. These were attacks wherein the attacker chose to remain anonymous, i.e., the Pan Am 103 bombing, World Trade Center bombing in 1993, bombing of the Khobar towers in 1996, the USS *Cole* in 2000, and the anthrax letters of 2001. Improving our nation's attribution capabilities will demand more creative scientific methods and technologies as well as greater integration of the relevant law enforcement and intelligence efforts. The responsibility for

attribution clearly resides with the Department of Justice; however, the Department of Justice has neither the scientific capability nor the budget to successfully complete this mission. The Department of Health and Human Services and the Department of Defense laboratories, as well as the private sector will be required to play significant roles in attribution. Without attribution, there can be no response.

Response has two roles in the homeland security cycle. The first is to eliminate the capability of the attacker to cause further harm. This might be achieved through arrest and prosecution, the use of military force, or covert actions. Certainly, the nature of response would depend on a range of factors, not the least being whether the attacker is a domestic or international actor. The Bush administration's actions after 9-11 illustrate the potential range of response options. Second, the ultimate goal of any response must be the reestablishment of deterrence. For America, the purpose of war is to establish a "better peace." In the homeland security strategic cycle, the purpose of response is to eliminate the attacker's offensive capability and to reestablish deterrence by sending a very clear message to all who wish America harm. Both elements of response were transmitted loud and clear in Afghanistan following the 9-11 attacks. The regime that supported Al-Qaeda was removed from power, and Al-Qaeda's command and control, logistical, financial, and training functions were severely disrupted. Additionally, terrorists and tyrants across the globe took notice of America's decisive action and global reach. As the President said, "Whether we bring our enemies to justice, or bring justice to our enemies, justice will be done."[17]

There are, of course, cases in which there is overlap within this framework, and at times, certain actions could fit in more than one category. Following the attacks on American embassies in Kenya and Tanzania, the cruise missile attacks on Al-Qaeda were called preemptive by the Clinton Administration, but one could also argue they were a response.

All models have limitations. In fact, there is an old saying in the Defense community that *all models are wrong, but some are useful*. Many within the homeland security community find this model useful. In fact, many have endorsed it because it provides an intellectual framework for short-term plans, long-range strategies, policies, and resource allocations. The Bush Administration's National Strategy to Combat Weapons of Mass

Destruction, released in December 2002, used the Homeland Security Strategic Framework, nearly verbatim.

V. "Weapons of Mass Destruction:" Description or Distraction?

The term, *weapons of mass destruction* (WMD) is one of the most misunderstood concepts in the homeland security and national security lexicons. Some have suggested that the best description of WMD is "worthless meaningless description."[18] According to the Department of Defense Dictionary of Military and Associated Terms, Joint chief of Staff (JCS Pub 1-02), WMD includes nuclear, chemical, and biological weapons. However, according to U.S. Code Title 18 (the Federal Criminal Statues), it includes all of the DoD mentioned weapons, but can also include explosives even as small as one quarter stick of dynamite. This is typical of definitional problems within the interagency and intergovernmental communities.

A far better term, and one that has gained widespread acceptance within the homeland security community is **CBRNE**, which stands for, *chemical, biological, radiological, nuclear* and *enhanced conventional explosions* (such as delivering 30,000 gallons of jet fuel to the 80th floor of a skyscraper). For the most part, each of these weapons are different in how they are produced, delivered, create damage and destruction, and the type of response and recovery required. A chemical attack is psychologically terrifying, but in most instances, will only affect a relatively small area. A biological attack, using a contagious pathogen, such as smallpox could quickly spread across an entire nation. A radiological dispersal device, also known as a "dirty bomb," would cause little destruction and casualties (only the blast from the conventional weapon) but could pose enormous cleanup problems and may even require the destruction of contaminated buildings.

JCS Pub 1-02 states, "Do not use the term total war." This is because it is too abstract. Does it mean one fights to an unconditional surrender as the U.S. did against Japan and Germany in World War II? Does it mean the war ends like the Third Punic War when the Romans completely ended the Carthaginian civilization? Or does it mean an entire nation is mobilized in the fight? Nobody knows. Which is why PCS Pub 1-02 says, "Not to be used."[19] Likewise, one should avoid the use of the term *weapons of mass destruction* and instead use the term that has gained widespread recognition within the homeland security community, CBRNE.

VI. The 2001 Attacks on the American Homeland

> If…on the morning of September 11, 2001,…the U.S. government had a fully integrated intelligence and law enforcement organization…equipped with state-of-the-art data mining capabilities…law enforcement officials would have been notified that Mohamed Atta and his roommate (both on terrorist watch lists) had just checked in for flights at Boston Logan Airport. Seconds later they would have detected that four other passengers checking in for other flights had listed the same home address as Atta, that three others checking in for flights had made numerous calls during the past month to a telephone at that same address, and two others checking in for flights had used Atta's frequent flier number just one month earlier.[20]

It is impossible to say if such a system could have prevented the attacks of September 11th. What is clear is that there was little or no chance of preventing the attacks with the system that existed in 2001. Laws, regulations, policies, cultural barriers, and bureaucratic stovepipes were ill suited for the security challenges of the 21st century. Al-Qaeda had studied their enemy well. Like a great quarterback, it knew how to find the seams in our defense.

In his book, On Guerrilla Warfare, Mao Zedong states, "many people think it impossible for guerrillas to exist for long in the enemy's rear. Such a belief reveals lack of comprehension of the relationship that should exist between the people and the troops. The former may be likened to water and the latter to the fish who inhabit it."[21] Mao may have been talking about the ability of guerrillas to operate in 1940s occupied China, but the 9-11 hijackers followed the same concept in their ability to move freely inside and outside the United States unnoticed. They wore no beards or Muslim clothing and did nothing to draw attention to themselves. Only in hindsight did the abnormalities become obvious. As the Director of the FBI, Robert Mueller likes to say, "They lived among us…they shopped at Wal-Mart, ate at Pizza Hut, and bought their command and control system from our convenience stores."[22] The 19

hijackers primarily used high tech "cyber cafes" and cell phones to coordinate their plans formulated by their leader, Osama bin Laden.

Bin Laden's role in the attacks was revealed in a series of videotapes captured in Afghanistan. The videos were made in mid-November 2001. No doubt as Bin Laden and other senior Al-Qaeda leaders were watching CNN or other international coverage of the unfolding attacks, they must have been ecstatic to learn that the attacks were more successful than they had anticipated.

> "We calculated in advance the number of casualties from the enemy who would be killed based on the position of the tower…We calculated that the floors it would hit would be three or four floors. I was most optimistic of them all…[D]ue to my experience in this field, I was thinking that the fire from the gas in the plane would melt the iron structure of the building and collapse the area where the plane hit and all the floors above it only. This is all that we had hoped for."[23]

The tapes also revealed information on Al-Qaeda's operations and communications security procedures. Bin Laden commented on those who conducted the operations: "All they knew was that they have a martyrdom operation and we asked each of them to go to America, but they didn't know anything about the operation, not even one letter."[24] These were not amateurs, like Ramzi Yousef's assistant who tried to get back his deposit on the rental truck after bombing the World Trade Center in 1993. These were seasoned professionals.

Their planning was extensive, spanning two years and several continents. To ensure the attacks were successful, Mohamed Atta selected airline flights carrying large quantities of fuel. They made test flights on those routes to study the patterns of flight attendants, pilots, and other airline personnel. By September 11, 2001, they were ready.

American Airlines Flight 11 took off at 7:45 a.m. from Boston Logan Airport for a long flight to Los Angeles' LAX Airport. On board were Mohamed Atta and the four other men. With box cutters and knives in hand they commandeered the big Boeing 767 and flew towards New York City. One hour later, the aircraft crashed into the North Tower (WTC 1) of World Trade Center complex between the 80th and 90th floor. The

resulting fire burned between 1500–2000 degrees Fahrenheit and burned for some 102 minutes. Due to the impact and extreme heat produced by burning aviation fuel, the top thirty floors collapsed onto the eighty floors below, bringing down the entire structure.

United Airlines Flight 175, a Boeing 767, also took off from Boston Logan airport roughly 13 minutes after AA Flight 11 at 7:58 a.m. with a long morning flight to Los Angeles. On board at the planned time, five hijackers took over the flight. As flight 175 approached New York City, the Al-Qaeda pilots could have surely seen the smoke coming from the North tower. At 9:05 a.m., as the world was watching, UA Flight 175 slammed into the South Tower (WTC 2), above the 90th floor, on one side with a brilliant, almost unbelievable flame coming out of the other. For the millions who watched this scene live on TV, it seemed more like something from Hollywood. The fire burned for 56 minutes before the top 20 floors would collapse on the remaining 90 below in 8 seconds.[25] The great buildings that Minoru Yamasaki had designed and that had taken seven years to build, collapsed in seconds.[26]

It is estimated that each jet carried approximately 60,000 pounds of jet fuel and was traveling in excess of 300 miles per hour when they crashed into each building.[27] Both towers were the first super-tall buildings designed without any masonry, with a uniquely designed central core and elevator system that allowed for more space on each floor. While originally designed to withstand an impact of a Boeing 707, the much larger 767s provided significantly more kinetic energy and fuel. The initial impact of the planes appeared to have created a lot of damage, but not enough to cause the building to collapse; however, the intense fires from the burning aircraft fuel combined with the damage began to weaken the undamaged metal support structures. Once the upper floors began to collapse, the downward momentum could not be stopped.[28]

World Trade Center towers 1, 2, and 7 collapsed, leaving more than one million tons of debris at what became known as Ground Zero. About 400 structures across a 16-acre area were damaged.[29] Over 13,000 customers lost electrical power.[30] In a matter of minutes, 2,752 people were killed.[31] Before the day was over, 440 first responders were killed (23 New York Police Department (NYPD), 343 Fire Department of New York (FDNY), and 74 Port Authority of New York and New Jersey).

Over 320 other emergency responders were treated for injuries or illnesses.[32]

On that same morning, United Airlines Flight 93 took off at 8:01 a.m. from Newark for a long flight to San Francisco. As the plane was being commandeered and flown back towards the East Coast, cell phone calls informed passengers onboard of what had happened at the World Trade Center. Taking the initiative into their hands with the words "let's roll," passengers engaged the hijackers, causing the plane to crash in a field near Stony Creek Township, Pennsylvania. All 45 people onboard were killed, leaving the intended target a mystery.

American Airline flight 77, a Boeing 757, took off at 8:10 a.m. from Washington Dulles Airport to Los Angeles. Along the route, five hijackers took over the plane and flew it towards the Potomac River. At 9:40 a.m., the plane slammed into the newly renovated and empty section of the Pentagon killing 189 people (125 people on the ground, and 64 on the aircraft). The crash damaged or destroyed three of the five interior concentric "rings" of the Pentagon building.[33]

By the time most Americans went to bed that night, they realized the world had forever changed. If there were any doubters left, the first two weeks of October 2001 likely changed their minds.

On October 1, 2001, Robert Stevens, an employee of American Media (AMI), was admitted to a Boca Raton, Florida hospital in a near death condition. Five days later he was dead. Within a few days, anthrax had become a 24/7 news event.

On the day Stevens died, letters claiming to contain anthrax were received at the New York Times and St. Petersburg Times, both later turned out to be hoaxes. On the next day, anthrax spores were found on another AMI employee, a mailroom worker, and on Stevens' computer. Later, this second worker was confirmed to have inhalation anthrax. On October 10, a third AMI mailroom worker tested positive for anthrax, and led FBI investigators to suspect that anthrax was being disseminated through letters in the postal system.

On October 12, one of Tom Brokaw's assistants at NBC reported a case of cutaneous anthrax. Five days later an envelope containing anthrax powder was opened in Senator Tom Daschle's office. Until this point, there was no evidence as to the quality of the pathogen, but tests of the material from Senator Daschle's office proved most disturbing. The fine

powder was some of the best quality ever seen by U.S. military personnel. America was under attack with a sophisticated pathogen.

Many now refer to the second attack of 2001 as 5-11…5 deaths due to inhalation anthrax and 11 infected with inhalation anthrax. In many respects, the 5-11 had far more ramifications than did the attacks of 9-11. These five deaths and the botched response by federal, state, and local officials demonstrated that America was woefully unprepared to respond to even a small-scale biological attack. In response, billion dollar programs in research and development and public health would soon receive funding from Congress.

VII. The Office of Homeland Security

On September 12, 2001, the former coach of the Georgetown University basketball team, John Thompson, was preparing for his afternoon radio talk show. He knew that his audience would not be interested in hearing about sports, so he asked the Director of the ANSER Institute for Homeland Security to be his guest. His first question was straight to the point, "Is America ready for homeland security?"

Considering the audience, the Director responded with a sports analogy, "We don't have a coach, we don't have a game plan, and we aren't practicing. How do you think we will do in a big game?"[34]

On October 8, 2001, President Bush gave the nation a coach, Governor Tom Ridge. Some in Congress were calling for the creation of a new department, but the President chose to create a new office within the White House, the Office of Homeland Security. The critics complained that Governor Ridge had neither operational nor budgetary authority in this position. His staff was only 35 with another 150 detailed from other agencies scheduled to come onboard. How could a leader without authority and with such a tiny staff handle what many were calling the most difficult and complex security challenge America had ever faced?

What the critics failed to realize was that the Office of Homeland Security was just the first step of a much larger plan. Following the attacks of 9-11, the President had to take action to better prepare the nation, but there was great concern that creating a new department overnight would have been a "bridge too far." The Bush Administration found wise counsel in the first rule of medicine, "First, do no harm."

The Office of Homeland Security was the first step in a long-term plan. It provided the team that would develop the National Strategy for Homeland Security (a game plan) and draft the legislative proposal for the creation of a new department. This proposal was based on commission recommendations, particularly Hart-Rudman, and other bills introduced in the House and Senate, but had several unique elements, such as the inclusion of the Secret Service and elements of the Departments of Agriculture, Health and Human Services, and the DOE National Labs.

VIII. A Homeland Security Strategy

On July 15, 2002, President George W. Bush released the first National Strategy for Homeland Security. Despite the name, the document did not provide a strategy, but did provide the first national plan for homeland security. The plan explained how the nation will reduce its vulnerabilities and marshal its resources, but not how they will be applied against any specific enemy.[35]

As recommended in the first Gilmore commission report, this document provided standard definitions for the nation.

> *Terrorism* – any premeditated, unlawful act dangerous to human life or public welfare that is intended to intimidate civilian populations or government.
>
> *Homeland Security* – a concerted national effort to prevent terrorist acts within the U.S., reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.
>
> *Critical Infrastructure* – the assets, systems, and functions vital to our national security, governance, public health and safety, the economy, and national moral.

There were four key themes emphasized in the national strategy document.[36] The first was **federalism**, "the idea that the federal government shares authority, responsibility, the mandate for action and the struggle for resources with states, local governments and private actors."[37]

Whereas national security had primarily been the realm of the executive branch of the federal government, specifically the Department of Defense, State and the Intelligence Community, homeland security involves more than 87,000 governmental jurisdictions. Furthermore, as was highlighted in the President's Commission on Critical Infrastructure Protection (PCCIP) report, 85 percent of critical infrastructure is owned by the private sector. In many scenarios, the federal and state executives will not own the assets needed for response. This has been demonstrated in many exercises, but none better than DARK WINTER. The primary response capability to a large-scale biological attack resides in the private sector – medical care facilities and personnel.

The second theme was **accountability**. "The path to homeland security requires clear organizations, consolidation of authority, and then holding some responsible for performance."[38] Nowhere was the theme better demonstrated than at the U.S. borders. In the past, when a large ship came to a U.S. port, the U.S. Coast Guard, Customs, Immigration, and (if agricultural products were on board) the Department of Agriculture met the ship. In other words, representatives from four different organizations, under four different Department Secretaries with differing priorities met the ship. Following the creation of the Department of Homeland Security on March 1, 2003, all four of these organizations now work for a single department secretary, and all have the same top priority, defending America.

The third theme was **fiscal responsibility**. In other words, "We have to accept some level of terrorist risk as a permanent condition."[39] If we do not, then the greatest threat to American security will be uncontrolled spending. The third theme is closely linked to the last one, **prioritization**.

During his first month in office as the Director of the Office of Homeland Security, Governor Ridge identified four priorities: (1) first responders, (2) borders, (3) bio-terrorism, and (4) improved intelligence and information flow.[40] These priorities have remained and are clearly stated throughout the strategy document and spending programs.

The strategy also identifies six "critical mission areas:" (1) Intelligence and warning, (2) border and transportation security, (3) domestic counterterrorism, (4) protecting critical infrastructure and key assets, (5) defending against catastrophic threats, and (6) emergency preparedness and response.

IX. The Department of Homeland Security

On March 1, 2003, the Department of Homeland Security became the federal government's third largest bureaucracy. Secretary Tom Ridge assumed control of a new department consisting of 22 agencies, 170,000 plus employees, and a budget of $37.4 billion dollars. It was the largest reorganization of the federal government since 1947.

Prior to this reorganization, a think tank had produced a chart that attempted to demonstrate the complex organizational structure of homeland security organizations within the federal government. One observer commented that it looked like a combination of a plate of spaghetti and an eye chart. (Of course, a complete diagram would have been far more complex, and confusing, since it would have required federal, state, and local government entities plus many private sector organizations.)

To resolve this, President Bush signed the Homeland Security Act of 2002 on November 25, 2002, in effect creating the Department of Homeland Security. Two months later on January 24, 2003, the new Department became part of the U.S. government. By March 1, 2003, all the component parts moved to the new Department. The idea was not to create new organizations on top of the existing structure, but to take existing independent agencies and realign them under one chain-of-command and department, thus streamlining and removing interdepartmental fighting over the sparse monetary "rice bowls" and personnel. Its major goal was to "transform and realign the current confusing patchwork of government activities into a single department."[41]

President Bush assigned the new Department three missions:

- Prevent terrorist attacks within the United States,
- Reduce the vulnerability of the United States to terrorism, and
- Minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States.[42]

One only needs to look at the new directorates to understand the depth of 9-11's impact on the United States government. The removal of agencies or functions from other departments, once unthinkable, was now fact. DHS organized into five major divisions or "Directorates." One directorate is purely for management of the department. However, the

other four are the key parts to making DHS a success. The Secret Service and the Coast Guard remains intact and reports directly to the DHS secretary.

The **Border and Transportation Security Directorate**, by far the largest, consists of the U.S. Customs Service, Immigration and Naturalization Service, the Federal Protection Service, the Transportation Security Administration, Animal and Plant Health Inspection Service, and other agencies. Many of these have been moved from the Departments of Justice, Agriculture, Treasury, and Transportation.

The **Emergency Preparedness and Response Directorate** prepares the nation for terrorist attacks and natural disasters, and the ability to recover from such events. The directorate oversees domestic preparedness training and coordinates government disaster response. It consists of the Federal Emergency Management Agency, Strategic National Stockpile and the National Disaster Medical System, Nuclear Incident Response Team, Domestic Emergency Support Teams, and the National Domestic Preparedness Office. These agencies moved from the Department's of Justice, Health and Human Services, Energy, and the FBI.

The **Science and Technology Directorate** takes advantage of all emerging technologies and science to secure the homeland. Merged into this high tech directorate will be DoD's National Biological Warfare (BW) Defense Analysis Center; and the Agriculture Department's Plum Island Animal Disease Center; and two programs from the Department of Energy: CBRN Countermeasures Programs, and Environmental Laboratory.

The **Information Analysis and Infrastructure Protection Directorate** will "analyze intelligence and information from other agencies (including the CIA, FBI, DIA, and NSA) involving threats to homeland security and evaluate vulnerabilities in the nation's infrastructure."[43] Originally, this directorate was considered to be the leading candidate to house a national law enforcement and intelligence fusion center. However, the creation of the Terrorism Threat Intelligence Center (under control of the CIA) was announced in the President's State of the Union address.

Many ask how long it will take for the new department to become effective. Defining "effective" is a challenge, but when one considers that it took the Department of Defense 40-years to "get it right" (Goldwater-Nichols Act of 1987), one hopes success in the Department of Homeland Security will come much quicker.

X. Key Issues

Despite the complaints of political pundits that it took 18 long months to create the Department of Homeland Security, it should be noted that this is the most significant reorganization of the federal government since 1947 – no small feat. On the other hand, many critical issues remain to be debated by the Administration, the Congress, the courts and the American people.

Intelligence and Law Enforcement Integration. When President Truman created the Central Intelligence Agency in 1947, he made it abundantly clear that it would serve as a foreign intelligence service, not a Gestapo-like organization that would infringe on the civil liberties of American citizens. Ultra-secret government organizations seem almost an anathema to many Americans, yet the threat of international communism made it a necessary element in America's Cold War defenses. The excesses of covert actions abroad in the 1950s, and domestic spying here at home in the 1960s, resulted in a two-decade long backlash that prohibited the Intelligence Community from operations inside U.S. borders and even limited capabilities overseas.

The failure to prevent the attacks of 9-11, even though significant amounts of information was available, but not properly collected and analyzed, led many to call for the creation of a domestic intelligence service, similar perhaps to the United Kingdom's MI-5.[44] The firewall that had been constructed between law enforcement and intelligence prevented the collection of certain information and the sharing of considerable critical information. For instance, in August 2001, the FBI began a frantic search for two terrorists believed to be inside the U.S. and planning a major attack. The FBI readily admits it faced a near impossible challenge of finding them, even though these two individuals used credit cards to purchase their 9-11 airline tickets. These cards had exactly the same names as was on the watch lists, but the FBI was prohibited from accessing this data base—a data base that corporations and private citizens can access for a small fee.

In response to the 9-11 attacks, Congress passed the USA PATRIOT Act. Some new authorities granted to the Department of Justice and FBI in this act were clearly needed. Many of the procedures for gathering

evidence and information were of the pre-Internet and pre-digital era. On the other hand, this 342-page bill, which changed seventeen laws, was passed by Congress in just two weeks. One wonders how many of the 535 members actually read this legislation. Clearly, the debate over domestic intelligence has yet to begin. It is one of the most important issues yet to be resolved. It is one of the key issues examined by the National Commission on Terrorist Attacks Upon the United States (9-11 Commission).[45]

Role of the Department of Defense and U.S. Northern Command. While there will be considerable debate on this subject, one thing is clear. In the vast majority of cases DoD will not be in charge, but will merely provide support to the lead Federal agency which could be the Department of Homeland Security, the Department of Health and Human Services or the Department of Agriculture, depending on the nature of the crisis.

DoD has divided homeland security into two general categories: *homeland defense* and *civil support*. Homeland defense includes aerospace and maritime missions plus the protection of key DoD facilities and infrastructures. Civil support includes missions ranging from traditional domestic support roles of disaster relief and counter drug operations to specialized technical support that would be required following an attack using CBRNE weapons. Specialized National Guard units, called Weapons of Mass Destruction-Civil Support Teams (initially called RAID Teams) are currently operational in more than 30 states. Eventually, each state will have at least one of these teams that are organized, trained, and equipped to be DoD's first responders to a CBRNE incident.

Additionally, DoD has identified three types of homeland security missions: *extraordinary*, *emergency*, and *limited scope and duration*. Extraordinary are those missions when DoD would likely be the lead federal agency: aerospace defense, maritime defense and when normal measures are insufficient to carry out federal functions (as was mentioned in the Bremer Commission Report). Emergency missions are those carried out in response to natural or man-made disasters. Limited scope and duration missions were conducted in support of the 2002 Olympics and the 2002 Super Bowl. In both emergency and limited scope and duration missions, DoD provides support to the lead federal agency.

***Posse Comitatus*.** This 19th century, one-sentence law, is one of the most misunderstood issues in homeland security. Many military officers, including some very senior officers do not understand *posse comitatus*. First of all, there is no Constitutional prohibition against military personnel enforcing civil law. *Posse comitatus* is Latin for, "power of the county." This legislation was passed after the American Civil War and during the Reconstruction to prevent southern sheriffs from deputizing Federal troops. No one has ever been successfully prosecuted under this law. At one time there was a significant difference in the ability of National Guard troops to conduct law enforcement activities, when operating under U.S. Code Title 32 (under the command of state governors), and Federal troops who always operate under U.S. Code Title 10. National Guard troops operating in Title 10 status (federalized) lose their Title 32 status and come under the same restrictions as federal troops—unless a Presidentially declared state of emergency exists.

However, Congress has passed considerable legislation in the past 10-years that has significantly blurred this distinction.[46] Because it is often misinterpreted and much of it is without legal precedence, *posse comitatus* is long due for legal reform.

Today, *posse comitatus* is used by DoD officials to avoid missions they do not want to do. Federal troops are not organized, trained, and equipped or funded for law enforcement activities. Furthermore, despite the change in the letter of the law, there remains a significant cultural prohibition against such activities. The requirement and likelihood of Federal troops (or National Guard troops operating under Title 10) providing law enforcement is limited and unlikely. There are, of course, exceptions, such as the Rodney King riots in 1992**,** when President George H. W. Bush invoked the Insurrection Act and deployed troops from the 7th Infantry Division at Fort Ord, California, to quell the riots in Los Angeles.[47]

Unfortunately, several key senior DoD leaders did not fully comprehend the full meaning of this Constitutional mission. All military officers and senior NCOs should receive appropriate education on *posse comitatus* so they are prepared to respond in a domestic crisis if required.[48]

Integration of Federal, state, and local government efforts. Few challenges of homeland security will pose more difficulty than the

integration of efforts of 87,000 different government entities. Nowhere is this better demonstrated than in the public health sector.

One of the greatest threats America will face in the coming decades is a sophisticated attack with biological pathogens. America is not prepared to respond to such an attack today. Unfortunately, this is not a problem that can be solved by just "throwing money at it." America's public health system is in such a state of disrepair that money alone will not lead to better preparedness.

The problem is one of organization or lack thereof. To best understand the problem, imagine if America's military was not a centralized organization. Imagine a military where each county had a tank, a platoon and an airplane. Imagine a military where promotion was not based on competency, but political connections. Imagine a military where there was little or no standardization. Imagine a military where some funding came from the federal level and some from state and local and few of the funding programs were coordinated. Sound ridiculous? Well…that is pretty much an accurate description of America's public health infrastructure today.

Prior to the 1960s, environmental issues were seen primarily as a state and local issue. Eventually, the nation learned that environmental policy would only be effective if coordinated at a national level. The same will be true for public health. At some point in the future, America's public health system will require a national organization, not more than 3,000 independent, uncoordinated departments. For example, the state of New Jersey alone has 116 independent public health departments.[49]

General Eisenhower said, "The right organization will not guarantee success, but the wrong organization will guarantee failure."[50]

Not all elements of the federal, state, and local government teams will require such radical changes. Many improvements can be made with enhanced planning efforts and exercise programs. This will avoid the situation we have seen many times in the past, where the first step in responding to a crisis was "exchanging business cards."

Furthermore, the most cost-effective means of preparing for incident management is to do it on a regional basis. Not every community needs to have every piece of equipment and every specialty. Regional capabilities and integrated Federal, state, and local teams will make homeland security affordable. Otherwise, the greatest threat to America will be uncontrolled spending.

XI. Summary

Just prior to his retirement from active military service, General Colin Powell stated that it would take a decade to figure out the international security environment that was replacing the Cold War. Some began to recognize this new environment by the mid 1990s. For most Americans it began on a Tuesday morning in September of 2001.

Scholars are still searching for the correct name for this new national security era, but they understand the elements: international terrorism, asymmetric warfare made possible through the technological revolution, and homeland security. This new era will not end with the death of Osama bin Laden or Saddam Hussein. In fact, a world that is fueled with centuries-old hatred and armed with 21st century technology is here to stay. Perhaps historians will say that what followed the Cold War was the War on Terrorism—an era that could last far longer than the Cold War.

Two wide oceans and two friendly neighbors have little meaning in the 21st century security. Today, a cell phone bought in a convenience store can serve as a global command and control system. A terrorist can sit in an outdoor café in Paris and launch a cyber attack on the Pentagon and Wall Street, and a test tube can hold a weapon that could threaten an entire nation.

The good news is that much has been accomplished since September 11th. Today, America has a coach, a game plan, and we are practicing. Secretary Ridge is the coach, and he is implementing the President's game plan, the Homeland Security Strategy. In May of 2003, the second of two national-level homeland security exercises (TOPOFF II) was completed. Additionally, hundreds of other exercises at the state and local level have been and will be conducted. A database from these exercises is being developed to identify "best practices" and leverage the investment and success.[51]

Of all the threats America faces, none will be of greater threat than uncontrolled spending. We cannot defend against all threats. We cannot deter, prevent, or preempt every truck bomber or sniper. We cannot provide every fire, police, and emergency services department in the country with every piece of emergency equipment on their wish list. We must establish priorities.

This will require continuation of a comprehensive and aggressive counterproliferation program. We must focus our efforts on deterring, preventing and preempting the high consequence events, and we must realize that they will not always be successful in these endeavors. Therefore, they must take actions to mitigate the effects of these high consequence events, determine the identity of the perpetrators, have the capability to respond in a manner that will eliminate the attackers offensive capability, and send a clear signal to all terrorists and tyrants that will re-establish deterrence.

Our leaders must learn to say, "No." We cannot afford every "good idea." Some are calling for vast amounts of spending to secure our borders. This may very well provide nothing more than a 21st century Maginot Line – and just like the French discovered in 1941, it provided no security. Ramzi Yousef and Timothy McVeigh built their bombs inside the United States. Radiological dispersal devices, chemical weapons and highly sophisticated biological weapons could just as easily be built within our borders.

Our enemies will continue to use America's strengths against us. Americans greatly value privacy, protection of individual liberties and rights of the accused, freedom of movement and access, and open borders. Americans see these values as strengths. The enemy sees them as seams in our defense, just as a National Football League quarterback exploits the seams in a zone defense. Defending the American homeland in the 21st century will be the most difficult challenge this nation has ever faced. It will likely cause us to reexamine how we think about the military, the intelligence community, privacy, civil liberties, federalism, immigration, international commerce, borders, and the role of corporate America.

A wrongly conceived counter-terrorist program could create a dilemma – forcing a society to choose between freedom and security. This fight will be neither cheap nor easy, but if we respond wisely, we will make this a false dilemma, and with wisdom and a strong effort, America will remain free and secure. We should not have to choose between freedom and security. Americans demand both.

Notes

1. DARK WINTER was an effort led by Dr. John Hamre at the Center for Strategic and International Studies. Dr. Tara O'Toole and Dr. Tom Ingelsby of the Johns Hopkins Center developed the executive simulation for Civilian Biodefense Strategies and Col Randy Larsen, USAF (Ret), and Mark DeMier of the ANSER Institute for Homeland Security. The McCormick-Tribune Foundation and the Oklahoma City Memorial Institute provided funding for the Prevention of Terrorism. Senior national security leaders, including Senator Sam Nunn, former CIA Director Jim Woolsey, former FBI Director William Session, Governor Frank Keating (R-OK), and David Gergen participated in this two-day event.

2. Comments made to Vice President Cheney by Col Randall Larsen on September 20, 2001.

3. Lincoln, Abraham, "Perpetuation of our Political Institutions: Address Before the Young Men's Lyceum of Springfield, Illinois," January 27, 1838.

4. *National Strategy for Homeland Security*, July 15, 2002.

5. Parachini, John V. "The World Trade Center Bombers," (1993), Chapter 11, page 191. From the book *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*, Jonathan B. Tucker, Editor, Monterey Institute, MIT Press, Cambridge, Massachusetts, 2000.

6. David Kaplan and Andrew Marshall, *The Cult From The End of the World* (New York: Crown Publishers), 1996, 140-146.

7. For a detailed description of this event and other Aum activities, see: Kaplan, David E. and Marshall, Andrew, *The Cult at the End of the World: The Terrifying Story of the Aum Doomsday Cult*, New York, Crown, 1996.

8. Simon Reeve, *The New Jackals*, (Boston: Northeastern University Press, 1999), 109; and Murray Weiss, *The man who warned America: the life and death of John O'Neill*, (New York: Regan Books, 2003), 89.

9. FACA, sometimes referred to as the Sunshine Law requires that meetings between federal government officials and private industry must be open to the public and press. Both public and private officials have expressed concerns that information regarding industry vulnerabilities could provide targeting information to terrorists. Legislation that created the Department of Homeland Security has allowed for some exceptions to FACA.

10. "Countering the Changing Threat of International Terrorism," *National Commission on Terrorism*, 7 June 2000, 64, on-line, Internet, 17 November 2003, available from http://w3.access.gpo.gov/nct/.

11. All Gilmore Commission reports can be viewed on-line, Internet, available from http://www.rand.org/nsrd/terrpanel/charter.html, current as of 17 November 2003.

12. Onion, Amanda, "A Lesson in Biology," *ABC News.com*, on-line, Internet, 5 October 2003, available from http://abcnews.go.com/sections/scitech/DailyNews/wtc_biologylesson011001.html.

13. "New World Coming: American Security in the 21st Century: Major Themes and Implications." *The United States Commission on National Security/21st Century.* (The Phase I Report on the Emerging Global Security Environment), 15 September 1999, 8, on-line, Internet, 17 November 2003, available from http://www.nssg.gov/Reports/NWC.pdf. 4. All the reports are available from http://www.nssg.gov/Reports/reports.htm.

14. Colonel Randall Larsen, the Chairman of the Department of Military Strategy and Operations at the National War College originally designed the model in October 1999. It consisted of: deterrence, prevention, preemption, crisis management, consequence management, and retaliation. In January 2000, attribution was added at the suggestion of Dr. Ruth David, the former Deputy Director of Science and Technology at CIA. In the spring of 2001, retaliation was replaced with response. Response includes both prosecution and retaliation. In April of 2003, crisis management and consequence management (terms from PDD-39 in the Clinton Administration) were replaced with incident management to align with the policies of the Bush Administration.

15. Discussion between Col. Randall Larsen and former Representative and Speaker of the House Tom Foley, October 2001.

16. Dershowitz, Alan, *Why Terrorism Works*, Yale University Press, 2002.

17. President Bush's Address to Congress and the American People; Thursday, September 20, 2001. On-line, Internet, available from http://www.newsmax.com/archives/articles/2001/9/21/02114.shtml.

18. Dr. Ruth David, President and CEO of ANSER uses this term frequently.

19. JCS Pub 1-02, 460.

20. Testimony of Randall Larsen, 9-11 Commission, New York City, April 1, 2003.

21. Mao, Tse-Tung. *On Guerrilla Warfare*. University of Illinois Press: Urbana and Chicago, 1961, First Illinois paperback 2000, 92-93.

22. Robert Mueller, Director of the FBI in a Speech to the National Legal Center, Department of Justice, Washington DC, November 19, 2002.

23. Garamone, Jim. *Defense Link, American Forces Information Service, News Article*. "Tape Proves Bin Laden's Complicity in September 11 Attacks," Washington D.C., 13 December 2001, on-line, Internet, available from http://www.defenselink.mil/news/Dec2001/n12132001_200112134.html.

24. Ibid.

25. Deputy Chief Vincent Dunn, ret. "Why the World Trade Center Buildings Collapsed: A Fire Chief's Assessment," 19 April 2003. *n.p.*, on-line, Internet, 19 April 2002, available from http://vincentdunn.com/wtc.html.

26. Ibid.

27. Department of State. *2001 Patterns of Global Terrorism*, 3.

28. The University of Sydney. "World Trade Center – Some Engineering Aspects," *Department of Civil Engineering, n.p.*, on-line, Internet, 17 November 2003, available from http://www.civil.usyd.edu.au/latest/wtc.php#system.

29. United States General Accounting Office (GAO). *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants, GAO-03-414*. GAO. February 2003, 9.

30. Ibid., 9.

31. Associated Press, "Official WTC death toll is 2,752," *The Salt Lake Tribune*, 30 October 2003, *n.p.*, on-line, Internet, 17 November 2003, available from http://www.sltrib.com/2003/Oct/10302003/nation_w/106763.asp.

32. Jackson, Brian A., Peterson, D.J., and others, *Protecting Emergency Responders: Lessons Learned from Terrorist Attacks*. RAND Science and Technology Policy Institute, Conference Proceedings, 2002, 6.

33. Garamone, Jim. *Defense Link, American Forces Information Service, News Articles*. "Tape Proves Bin Laden's Complicity in September 11 Attacks." Washington D.C., 13 December 2001; on-line, Internet, available from http//www.defenselink.mil/news/Dec2001/n12132001_200112134.html.

34. Randall Larsen, Director ANSER Institute for Homeland Security in radio interview with John Thompson, September 12, 2001.

35. Dr. David McIntyre, "Understanding the New National Security Strategy of the United States," *ANSER Institute for HOMELAND Security,* (Institute Analysis 009), September 2002, *n.p.,* on-line, Internet, 17 November 2003, available from www.homelandsecurity.org/hlsanalysis/hlsstrategyanalysis.htm.

36. These themes are found in Dave McIntyre's Commentary "The National Strategy for Homeland Security: Finding the Path Among the Trees."

37. David McIntyre, "The National Strategy for Homeland Security: Finding the Path Among the Trees," *ANSER Institute for HOMELAND Security*, 23 July 2002, 12, on-line, Internet, 17 November 2003, available from http://www.homelandsecurity.org /HLSAnalysis/20020723.htm, 3.

38. Ibid., 4.

39. Ibid., 5. Also found in Office of Homeland Security's *National Strategy for Homeland Security,* July 2002, p. 2.

40. Ibid., 6.

41. "What is the Mission of the New Department of Homeland Security?" *Department of Homeland Security Website,* (DHS Organization Section), *n.p.*, on-line, Internet, 17 November 2003, available from http://www.dhs.gov/dhspublic/ display?theme=10&content=429.

42. "Homeland Security Act of 2002," *The Whitehouse Website*, 17 November 2003; on-line, Internet, available from http://www.whitehouse.gov/deptofhomeland/bill/title1.html or http://www.whitehouse.gov/deptofhomeland/bill/hsl-bill.pdf.

43. "Who Will Be Part of the New Department?" *Department of Homeland Security Website,* (DHS Organization Section), *n.p.*, on-line, Internet, 17 November 2003, available from http://www.dhs.gov/dhspublic/display?theme=13.

44. Senator John Edwards, "Senator Edwards Proposes Homeland Intelligence Agency," *News from Senator John Edwards North Carolina for Immediate Release-Press Website,* 13 February 2003, *n.p.,* on-line, Internet, 17 November 2003, available from http://edwards.senate.gov/press/2003/0213-pr.html#.

45. From the oral statement by Randall Larsen to The National Commission on Terrorist Attacks Upon the United States (9-11 Commission) in New York City on April 1, 2003.

46. For more information on *posse comitatus* go to the following websites (current as of 17 November 2003): http://www.northcom.mil/index.cfm?fuseaction=news.fact sheets&factsheet=5, or http://www.homelandsecurity.org/journal/articles/displayArticle.

asp?article=11, or http://www.homelandsecurity.org/journal/articles/displayArticle.asp?article=30.

47. The Insurrection Act (Title 10 USC Sections 331-334). This act allows the President to use U.S. military personnel at the request of the State Legislature or Governor to suppress insurrections. It also allows the President to use federal troops to enforce federal laws when rebellion against the authority of the United States makes it impracticable to enforce the laws of the U.S.

48. Because if it is required, it means that a serious breach in security has occurred, and DoD must not fail in its mission.

49. Interview with Dr. Elin Gursky, former Deputy Health Commissioner for the State of New Jersey, May 30, 2003.

50. This quote is found in Senator Graham's statement during the proceedings: "I conclude by reading a quote from Dwight David Eisenhower. I think it is very appropriate as we debate the Homeland Security Department and its structure. Ike said: 'the right organization will not guarantee success, but the wrong organization will guarantee failure.'" U.S. Senate Proceedings, "091902 Homeland Security.txt, Homeland Security Act of 2002," *United States Coast Guard Legal Website*, (Homeland Security Act of 2002 - Legislative History & Documents- Text Files Listing), 19 September 2002, on-line, Internet, 18 November 2003, available on http://www.uscg.mil/legal/Homeland_legislation/text/091902%20homeland%20security.txt, or http://www.uscg.mil /legal/Homeland_legislation/Text/, page S8882.

51. More information is available at the National Memorial Institute for the Prevention of Terrorism (MIPT) website's Library and MIPT Databases, available from http://www.mipt.org/MIPT-Databases.asp. Current as of 17 November 2003.

USAF Counterproliferation Center

The USAF Counterproliferation Center was established in 1999 to provide education and research to the present and future leaders of the USAF, to assist them in their activities to counter the threats posed by adversaries equipped with weapons of mass destruction.

Barry R. Schneider, Director
USAF Counterproliferation Center
325 Chennault Circle
Maxwell AFB AL 36112-6427

Email: Barry.Schneider@maxwell.af.mil

Jo Ann Eddy, Associate Editor
The Counterproliferation Papers

Email: JoAnn.Eddy@maxwell.af.mil

(334) 953-7538 (DSN 493-7538)