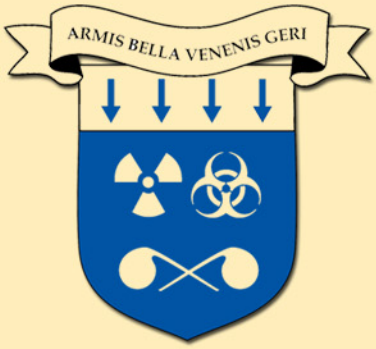
The Homeland Security Papers: Stemming the Tide of Terror

Colonel Michael W. Ritz, USAF,
Lieutenant Colonel Ralph G. Hensley, Jr, USAF, and
Major James C. “Chris” Whitmire, USAFR, eds.



US Air Force
Counterproliferation Center
Maxwell Air Force Base, Alabama

THE HOMELAND SECURITY PAPERS:
Stemming the Tide of Terror

Edited by
Michael W. Ritz
Ralph G. Hensley, Jr.
James C. “Chris” Whitmire

USAF Counterproliferation Center

325 Chennault Circle
Maxwell Air Force Base, Alabama 36112-6427

February 2004

Disclaimer

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

ISBN 0-9747403-2-2

Contents

Acknowledgments

This book is the product of many sponsors, authors, editors, and support staff of the USAF Counterproliferation Center (CPC). Special thanks are given to Dr. Barry Schneider who served as a mentor and advisor throughout the creation of this work. Also, thanks to Headquarters USAF/XONP, which funded the printing and distribution of this book. Additional appreciation is given to the Defense Threat Reduction Agency Technology Development Division (DTRA/TD) whose generosity provided funding for the CPC taught Air War College elective class, *Homeland Security: Protect, Prevent, and Recover*, which generated many of the ideas presented. We thank each of the authors whose combined scholarship we bring to you in the chapters that follow.

The editors owe a special debt of gratitude to Mrs. Jo Ann Eddy, Mrs. Abbey Plant, and the other CPC support staff who devoted many hours to this project. Additional thanks are due to Mrs. Brenda Alexander who assisted in multiple tasks required to bring this book to press. Additionally, we extend our appreciation and special thanks to one of the world's best copyeditors, Mr. Armin Reitz.

Finally, the editors are grateful for the loving support of our wives, Mixie Ritz, Diana Hensley, and Shannon Whitmire who encouraged us and gave us the freedom to devote many extra work hours to this book while they did more than their share on the home front.

Michael W. Ritz
Ralph G. Hensley, Jr.
James C. "Chris" Whitmire

Figures and Tables

Figures

Tables

Preface

The September 11, 2001, attacks on the World Trade Center and the Pentagon highlighted our national-level vulnerability to the threat posed by a formidable new enemy—focused, mass destruction terrorism. The tragic events of that day also demonstrated how determined, adaptive, and sophisticated—in both planning and execution—our terrorist adversaries have become. In this sense, the September 11th attacks were an important wake-up call for the American people, dispelling forever the false notion that the U.S. homeland is somehow immune to the violence and destructive hatred that characterize the international terrorist agenda. On the contrary, given the capability and commitment of our terrorist adversaries, we can fully expect future attacks to be even more sophisticated and destructive in terms of overall physical, economic, and psychological impact. With this reality in mind, the imperative to develop a comprehensive, creative national approach to homeland security is, indeed, most urgent.

As President Bush highlighted in the *National Strategy for Homeland Security*, protecting our Nation against future terrorist attack is our number one priority. Working together as a Nation, we have made important progress in addressing our most critical vulnerabilities, preventing terrorists from reaching our shores and border points of entry, and enhancing our mitigation and response capabilities should our protective efforts fall short of the mark. As we move further in time from the tragic events of September 11th, it is important that we maintain this critical focus and do all that we can to anticipate our adversary's next move—one that may well entail the use of weapons of mass destruction against our population and national resource base.

This book presents an important intellectual framework for contemplating the future of the terrorist threat, as well as potential solutions to the complex security dilemmas that we face in dealing with a highly dynamic and resilient enemy. As we look to the future, we must be

more creative and adaptive than our terrorist adversaries. We must seek approaches that engender cooperation and integration across government, private industry, and the public at large. We must look to innovative concepts and technologies to help leverage the most effective and efficient protective solutions, while preserving the freedoms and liberties that serve as the hallmark of this great Nation. Finally, we must all take ownership of this very complex set of challenges and partner in unified fashion to defeat those who would seek to cause us great harm. I ask that you keep these imperatives in mind as you ponder the framework herein.

ROBERT B. STEPHAN
Special Assistant to the Secretary
U.S. Department of Homeland Security

CHAPTER 1

Introduction

The notion of homeland security has always been an integral part of our nation's past. Before our nation was founded, frontier settlements and villages bore the brunt of homeland security by providing safe haven for those helping forge a new, more progressive civilization on the North American continent. Though "protected" by British forces before the American Revolution, the colonies nonetheless could raise armed militia to defend their homes, lands, towns, and first cities from outside threats to their security. And when the passionate voice of a new nation at birth was heard through the Declaration of Independence, the thirteen colonies' Minutemen were gathering arms to form the core of a Continental Army that would defend a republic that so eloquently proclaimed its freedom.

In the 1800s, our new nation boldly sought its identity with other world powers. The challenges of the War of 1812, the dynamics of the Industrial Revolution, westward expansion to the Pacific Ocean and to our southern borders with Mexico, and the increasing realities of complicated relations with ever-changing nation-states around the globe furthered our nation's need for homeland security. In 1861, our young nation faced its greatest challenge in a civil war that encompassed the entire homeland's security. Federal forces would fight Confederate forces in a conflict to ensure our nation remained both united and free from the yoke of human slavery. By 1899, our nation had furthered its national security interests by meeting the challenges of foreign dominance in Cuba and the Philippines.

The 20th century brought our nation new horizons and even greater security challenges. From 1910 to 1917, the Mexican Revolution created instability with Mexico along its borders with California, Arizona, New Mexico, and Texas. While securing those same borders, American forces would test their mettle against Mexican insurgents and regular military. Those same forces would soon be tested again in the world's first global

conflict. Our entry into World War I put our nation firmly on the world stage by emphasizing the fact that United States' national security lay not only at home, but also on the doorsteps of our allies and our enemies

On December 7, 1941, our security was again challenged when the Japanese attacked Pearl Harbor and thrust our nation into World War II. Although that global catastrophe ended in 1945, a new of kind of war brought our nation to again confront those who would threaten our homeland security. It was during that Cold War we came face to face with the calamity of total nuclear destruction. When the walls of communism came tumbling down in the late 1980s, many in our nation felt the world had finally become a much safer place. We could, perhaps, finally say to ourselves that since the founding of our republic, through peace and in war, our nation had built the world's strongest economy, a military second to none and a union of states and citizens forming the core of defending our national interests and homeland security. But that was not to be.

Terrorism has plagued mankind in one form or another throughout written history. But, in the latter part of the 20th century, terrorism had become, perhaps, the most sinister method of conflict the world had ever seen. Coupled with weapons of mass destruction, the terrorists and their organizations could wreak havoc on a virtual global scale. Those not prepared for terror would be ripe for a terrorist's methods. For the United States in the 1990s, complacency had replaced vigilance and readiness in a number of key homeland security areas. And, as we entered a new millennium, the shocking horrors of September 11, 2001, would alter our perception of the world and our homeland security.

That single event forced opportunity out of adversity. Our nation became fully aware of the formidable challenge posed by a well-funded, intellectually capable, ideologically driven enemy with asymmetric strategies and tactics. Securing our homeland became our nation's number one priority.

Today, significant steps have been taken to design and implement a strategy to secure our homeland against hostile nation-states, terrorism, natural emergencies, and accidental manmade disasters. Although much progress has been made, much more has yet to be done. Our policymakers must be good stewards of limited resources. They must develop sustainable, multi-use solutions to protect our way of life and the infrastructure that makes that life possible. Those same solutions must

help secure our nation's homeland while respecting freedom and enabling the economy to prosper. Additionally, the framework of such solutions must help our nation respond and recover when necessary to all hazards while continually striving to counter the unexpected.

It is our hope this first compilation of *THE HOMELAND SECURITY PAPERS* will help provide valuable insight and cutting-edge concepts to assist others who stand at the forefront of protecting our homeland from the dangers of a 21st century world.

MICHAEL W. RITZ
RALPH G. HENSLEY, JR.
JAMES C. "CHRIS" WHITMIRE

CHAPTER 2

What Price Security?
The USA PATRIOT Act and America's Balance Between Freedom and Security

Roger Dean Golden

Introduction

> *It is a melancholy reflection that liberty should be equally exposed to danger whether the government have too much power or too little.*
>
> —James Madison in a letter to Thomas Jefferson, October 17, 1788.[1]

On September 11, 2001, terrorists crashed jetliners into the two World Trade Center towers in New York City and the Pentagon in Washington, DC. These attacks were successful in many ways. Of course, there was the immediate devastation of some 3,000 people killed, with thousands more wounded. Billions of dollars in property damage also resulted from the attacks. In the weeks that followed, more effects were evident. Americans truly were terrorized and traumatized, realizing that they were not safe in their own homeland. While the lives of those closest to the tragedies were changed radically, virtually all Americans felt some emotional effect from the attacks. In addition, the American economy, already beginning to falter, was dealt a severe blow. Certainly, if the terrorists' goal was to punish America, their success was significant.

However, the terrorists may have accomplished an even greater long-term victory, with implications for the future of all Americans. As a reaction to the September 11th attacks, Congress rapidly passed the USA PATRIOT Act on October 24, 2001, and President Bush signed it into law

two days later.[2] This act provided broad new powers to various agencies of the federal government, particularly in the area of gathering information which might lead to arrest of terrorists or might prevent future terrorist acts. Among other issues, the USA PATRIOT Act addresses intelligence gathering related to communications, funding, and other activities of possible terrorists.

The weighty question is, to what degree does this new act infringe on the freedoms of American citizens? Does this act allow the federal government to intrude in an unacceptable manner into the private lives of Americans? Does it diminish the civil liberties that Americans hold dear? Does it represent a shift toward increasing security while taking away freedom? If this act has resulted in a loss of freedom and reduced civil liberties for Americans, then have not the terrorists accomplished an even greater long-term victory as a result of their attacks? Have we conceded a portion of victory to the terrorists by sacrificing freedom to increase security?

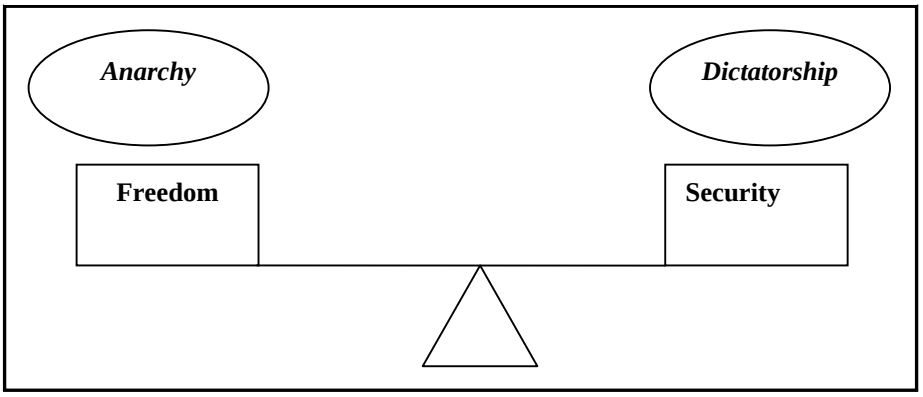
The Balance Between Security and Freedom

> *They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.*
>
> —Benjamin Franklin

Freedom and security may be viewed on a continuum, with the assumption that, as one is increased, the other may decrease. A nation that has total freedom may be characterized by anarchy, with minimum security for individuals in the state. Every person is free to do as he pleases, with no restrictions by the state. In such a nation, one person may use his freedom to the detriment of other people, resulting in anarchy. On the opposite end of the spectrum, a state may best be able to ensure maximum security only by severely limiting the freedoms of individuals. The state may seek to protect its citizens by controlling their lives. Such a state may ultimately constitute a dictatorship. This totalitarian state is the type of state pictured in George Orwell's novel *1984*.

A model of this continuum for a nation reflecting a healthy balance between security and freedom would be as follows:

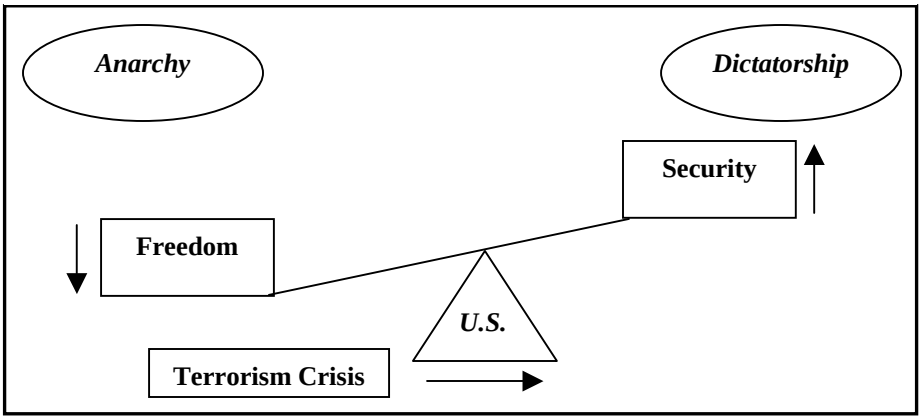
Figure 2.1 Healthy Balance Between Security and Freedom



Source: Author's model.

However, as freedom is increased, security is decreased and the nation moves toward anarchy. Conversely, as security is increased, freedom is decreased, and the nation moves toward dictatorship. Thus, one might argue that America has historically found a healthy balance between freedom and security. However, due to reactions to the recent crisis of terrorism, the fulcrum in America has moved toward security. Consequently, as security has increased, freedom has decreased, and America may be moving toward an unhealthy balance. The model would be adjusted to reflect this movement as follows:

Figure 2.2 Unhealthy Balance Between Security and Freedom



Source: Author's model.

Has America experienced an unhealthy shift in the balance between freedom and security as a result of the reactions to the terrorism of September 11, 2001? Champions of civil liberty argue that such a shift has taken place and that America is moving toward dictatorship. An examination of the USA PATRIOT Act in the light of America's historical perspective may prove useful in determining whether this fear is plausible.

The Origins of Freedom

> *Is life so dear, or peace so sweet, as to be purchased at the price of chains and slavery? Forbid it, Almighty God! I know not what course others may take; but as for me, give me liberty or give me death!*
>
> —Patrick Henry, March 23, 1775

In 1776, America's founding fathers wrote in the *Declaration of Independence* that "we hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable rights, that among these are life, liberty and the pursuit of happiness…" With this statement, the founding fathers expressed the heritage that was to be American—a heritage of liberty bestowed by the Creator himself. Infringement of this liberty was the reason given for the thirteen colonies revolting against the King of England and declaring their independence as the United States of America. The *Declaration of Independence* was enacted on July 4, 1776, and signed by representatives of the thirteen states, who pledged their lives, their fortunes, and their sacred honor to support this document and the liberty it proclaimed.

This principle of preeminent liberty was codified by the founding fathers in the governing document which they wrote to establish the basic law for America, *The United States Constitution*. The *Constitution* was completed on September 17, 1787. The preamble to the *Constitution* states:

> We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and *secure the Blessings of Liberty to*

> *ourselves and our Posterity*, do ordain and establish this Constitution for the United States of America. (*Emphasis added*).

The objective of the *Constitution* was to establish the overall system of government that would defend the security of the people and provide domestic peace and welfare. However, the greater goal of the *Constitution* was the securing of liberty. The purpose of the law was so that liberty might be protected. Thus, a healthy balance was established between security and liberty in the *Constitution*.

In order to clarify the liberties which the founding fathers believed to be the unalienable rights of all Americans, the U.S. Congress added the first ten amendments to the *Constitution*, and these amendments were ratified on December 15, 1791, just four years after the signing of the *Constitution.* The *Bill of Rights*, as these ten amendments have commonly been called, provides for specific rights and freedoms to be guaranteed to Americans. The first amendment rights include freedom of religion, freedom of speech, freedom of the press, freedom to assemble peacefully, and freedom to petition the government for redress of grievances. The second amendment provides the right to bear arms. The fourth amendment provides "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The fifth amendment provides that no person shall be "deprived of life, liberty, or property, without due process of law." Amendment nine recognizes that there are rights which even the *Constitution* may not enumerate. This amendment states: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people." Thus, the forefathers established the importance of civil liberties, with the principle that the *Constitution* and the body of law were there for the protection of the rights of the citizens.

Over the course of America's history, the body of law established by the U.S. Congress and interpreted by the courts has sought to maintain a proper balance between security and liberty. If security is threatened by a crisis, Congress may enact a law which represents a shift toward security at the cost of reduced freedom. This shift toward security may also be effectuated by a Presidential Executive order or other actions of the executive branch. However, if a law is too intrusive on liberty, it is likely that the Supreme Court will invalidate the law, moving the fulcrum back

toward freedom, even at the cost of potential reduction in security. Congress may also pass laws expanding or guaranteeing freedom, moving the balance toward freedom with possible reductions in security. Certainly, the fulcrum has shifted from time to time in one direction or the other. Historians might disagree as to the degree the fulcrum has shifted toward freedom or toward security, but examples of movement in both directions can be cited.

In 1928, writing the majority decision in *Olmstead v. U.S.*, Justice Louis Brandeis introduced the "right to privacy," which had not been specifically listed in the *Constitution*. Brandeis wrote, "To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment." Brandeis considered the right to privacy as "the right to be left alone—the most comprehensive of rights, and the right most valued by civilized men."[3] With this Supreme Court decision, the fulcrum moved toward increased freedom. Yet, the decision made it more difficult for the federal government to gather information that might ensure security. The right to privacy has subsequently been regarded to be as fundamental as the other civil liberties specifically enumerated in the *Bill of Rights.*

There are also examples of the fulcrum moving toward security at the cost of freedom. One of the most glaring examples was the treatment of Japanese-American citizens during World War II. After the Japanese attacked Pearl Harbor on December 7, 1941, the U. S. experienced great fear, particularly in the west, where citizens thought Japan would attack next. On February 14, 1942, President Roosevelt issued Executive Order 9066, which ordered Japanese residents to be taken from their homes and placed in camps supervised by the War Relocation Authority. Over 120,000 Japanese were placed in austere conditions in these camps, even though two-thirds of these Japanese people were American citizens. There was no evidence of a threat, or even disloyalty, by any of these Japanese people. Yet the Executive Order was not canceled until 1944, and the camps were not completely closed until March 1946.[4] The U.S. Supreme Court upheld these incarcerations. The fulcrum had shifted toward supposed security for Americans in general, but had resulted in a total loss of freedom for thousands of Japanese-Americans.

In January 2001, Tampa, Florida, used face-recognition cameras to scan the crowds at the Super Bowl. Faces were to be matched by computer with faces of known criminals, hopefully leading to arrest of those criminals. After the Super Bowl, the cameras were moved to the Ybor City region of Tampa, where police continued to try to identify criminals.[5] Civil libertarians protested this technique as an invasion of privacy, but the cameras were only removed after they proved ineffective in leading to apprehension of criminals. Consideration is being given to use of similar face-recognition technology in airports and seaports to try to identify terrorists attempting entry into the U.S. Opponents argue that this technology deprives Americans of the right to privacy, moving the fulcrum toward security at the cost of freedom.

American history includes many other examples of movement in one direction or the other. U.S. Representative Jerrold Nadler said that the U.S. has often limited civil rights during war time, including the 1798 Alien Sedition Act, the 1917 espionage act and Palmer raids, COINTEL during the Vietnam War, and McCarthyism during the Cold War. He also noted that America has had to apologize for each of these cases.[6] Over time, America has continued to seek a healthy balance between freedom and security. Crisis has usually been the impetus for any moves toward security. Such is the case with the USA PATRIOT Act of 2001 and other federal government actions following the September 11, 2001, terrorist attacks.

The USA PATRIOT Act

> *We're likely to experience more restrictions on personal freedom than has ever been the case in this country.*
>
> —Supreme Court Justice Sandra Day O'Connor, after a visit to Ground Zero, the site of the terrorist attacks on the World Trade Center in New York.[7]

The USA PATRIOT Act is actually 167 pages of documents, which primarily modify existing laws on a variety of subjects. The title is an acronym for "*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism."* The act's primary focus is to grant the federal government increased powers for surveillance and intelligence gathering on individuals residing in the

United States. These individuals may include both citizens and non-citizens. Other provisions of the act cover a variety of issues related to the war on terrorism.

With the anthrax scare in full swing and many lawmakers shut out of their offices, the act passed Congress with virtually no debate. According to Senator Russell Feingold, the only senator voting against the bill, most senators were very unaware of the details of the act.[8] U.S. Representative Jerrold Nadler said that the version of the bill approved by the House Judiciary Committee had been thrown out, with House Republican leaders and Attorney General John Ashcroft crafting a new version. Although only two copies of the lengthy new bill were printed at 10:00 a.m., the bill passed the House three hours later by an overwhelming majority vote of 356 to 66.[9] In fact, the bill could only be understood by comparing it to the several other laws it amended. Critics of the bill contend that the federal executive department used this opportunity to railroad through many intrusive practices Congress had refused to allow in the past. Senator Feingold said, "There is no doubt that if we lived in a police state it would be easier to catch terrorists. That would not be America."[10]

The act addresses a number of different areas in order to provide tools for the government to combat terrorism within the United States. Title I discusses antiterrorism funding and philosophical issues. Title I, Sec 102 (b) states: "It is the sense of Congress that the civil rights and civil liberties of all Americans, including Arab Americans, Muslim Americans, and Americans from South Asia, must be protected, and that every effort must be taken to preserve their safety."[11] Thus, Congress stated their intention to maintain the balance between security and freedom. However, critics of the act argue that, in spite of those stated intentions, the act severely infringes on civil liberties of all Americans.

Title II of the act provides for enhanced surveillance procedures. Authority to intercept wire, oral, and electronic communications is expanded if these communications may be related to terrorism or computer fraud and abuse. This title includes 25 separate sections, providing significant new authority for the government to monitor all forms of communication, including postal mail, e-mail, voice mail, telephone, and computer communications. Search warrants will be easier to obtain, more powerful, broader in scope, and will provide for warrants to be valid for longer periods of time. Typical language of this title is

"The…Federal Bureau of Investigation…may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities."[12]

One statute revised by the USA PATRIOT Act is the Foreign Intelligence Surveillance Act (FISA) of 1978. Congress passed FISA after learning that the Federal Bureau of Investigation (FBI) had performed extensive surveillance on American citizens during the previous two decades. FISA severely restricted domestic surveillance, establishing guidelines for when and how wiretaps could be performed on American citizens. FISA was an example of Congress moving the fulcrum toward liberty at the possible cost of security. The USA PATRIOT Act significantly loosens some of the restrictions of FISA, moving the fulcrum back toward security at the potential cost of freedom.

For example, the USA PATRIOT Act allows "roving" wiretaps that can follow a person wherever he goes, including a neighbor's computer, a library computer, his home or office computer, or any phone he may use. Critics argue that the new provision may violate the Fourth Amendment to the *Constitution*, which prohibits unreasonable searches and requires that warrants "particularly describ[e] the place to be searched, and the persons or things to be seized." Under the USA PATRIOT Act, national search warrants may be requested, whereas previously, separate warrants had to be obtained for every jurisdiction. The USA PATRIOT Act also changed the Electronic Communications Privacy Act (18 U.S.C. sec 2703) so that nationwide search warrants can be issued for voice mail and e-mail. The only probable cause that is required is a reasonable suspicion that a person may be acting for a foreign power. Search warrants are powerful, and can be enforced immediately, even against resistance.[13]

Wiretapping authority is also broadened by the USA PATRIOT Act. FISA allowed wiretaps only if a federal judge determined that the target individual had probably committed a serious crime, with those crimes specifically listed. The USA PATRIOT Act added a number of crimes related to terrorism and cyber-crime to the list justifying wiretapping. In addition, an internet service provider may be required to gather information such as web sites visited or e-mail headers.[14] Critics argue that, once such broad access is allowed to an individual's communications, there is no way to ensure that the agency only gathers information relevant

to an investigation, or that information will not be used to harm individuals who are not involved in terrorism. Therefore, the right to privacy may have been significantly lessened by the USA PATRIOT Act.

Title III of the USA PATRIOT Act addresses "International Money Laundering Abatement and Anti-Terrorist Financing." The act contends that money laundering totaling over $600 billion annually permits funding of terrorism and international crime. This portion of the act is designed to "increase the strength of…measures to prevent, detect, and prosecute international money laundering and the financing of terrorism."[15] The act includes new authority to gather information, seize funds, and levy heavy criminal penalties, including fines and prison time, for money laundering. Areas of concern for civil liberty activists include new requirements for financial institutions such as banks to gather additional information and report more information to government agencies. Securities brokers and dealers are required to report activities that they judge to be "suspicious."[16] Many of the new provisions represent changes to the "Bank Secrecy Act," removing some of the privacy Americans have historically had in their financial transactions and arrangements.

Title IV of the USA PATRIOT Act provides measures to protect the borders of the United States. The State Department and the Immigration and Naturalization Service (INS) are provided more access to the criminal records of persons attempting to enter the United States. The U.S. Attorney General is given two million dollars for an "integrated automated fingerprint identification system for ports of entry and overseas consular posts." The act includes an extensive definition of terrorism and provides for mandatory detention of any suspected terrorist. The criteria for detention is "reasonable grounds" to believe that the person "is engaged in any…activity that endangers the national security of the United States."[17]

Title V aims to remove obstacles to investigating terrorism. Section 504 provides for more coordination and sharing of information between intelligence and law enforcement officials. Section 505 provides broader authority to obtain telephone bills and records and financial records. Sections 507 and 508 give authority to collect educational records. In each case, information previously considered private can be more readily obtained by federal agencies.[18]

Title VI provides financial benefits for victims of terrorism, public safety officers, and their families and does not appear to contain any civil

liberty issues. Title VII expands information sharing between federal, state, and local law enforcement agencies. The act provides $150 million to the Bureau of Justice Assistance to establish and operate "secure information sharing systems to enhance the investigation and prosecution abilities of participating enforcement agencies in addressing multi-jurisdictional terrorist conspiracies and activities." Critics fear a "big brother"-type government gathering all kinds of information on its citizens and using this information for wrong purposes.[19]

Title VIII strengthens criminal laws against terrorism. Statutes of limitation are removed for certain terrorism offenses. Maximum penalties are increased. Domestic terrorism, cyberterrorism, bio-terrorism, terrorism conspiracies, and terrorism as racketeering are addressed. Even harboring of terrorists and providing material support for terrorists are discussed, with new penalties including fines and up to ten years in prison.[20]

Title IX discusses improved intelligence against terrorism, amending the National Security Act of 1947 to make clear the responsibilities and authorities for various federal agencies in dealing with terrorism. The Director of Central Intelligence is given broader authority to gather intelligence that possibly relates to terrorist activities. Requirements for reporting to Congress on intelligence gathering activities are softened.[21]

Title X includes a number of miscellaneous provisions, including efforts to provide some protections for civil liberties. Section 1001 says that the "Inspector General of the Department of Justice shall designate one official who shall review information and receive complaints alleging abuses of civil rights and civil liberties by employees and officials of the Department of Justice."[22] Section 1002 expresses the sense of Congress that "in the quest to identify, locate, and bring to justice the perpetrators and sponsors of the terrorist attacks…the civil rights and civil liberties of all Americans, including Sikh-Americans, should be protected."[23]

Reactions to the USA PATRIOT Act

> *I don't think the American public has even begun to grasp the kind of sacrifices we've been called to make in civil liberties in this war on terrorism.*
>
> —Vermont Law School Professor Stephen Dycus[24]

Since the USA PATRIOT Act became law, many voices have been raised in criticism of the act, alleging that Americans have suffered serious loss of civil liberties. A statement by Nancy Chang, senior litigation attorney at the Center for Constitutional Rights in New York, is representative of the level of concern. Ms. Chang said:

> To an unprecedented degree, the Act sacrifices our political freedoms in the name of national security and upsets the democratic values that define our nation by consolidating vast new powers in the executive branch of government. The Act enhances the executive's ability to conduct surveillance and gather intelligence, places an array of new tools at the disposal of the prosecution, including new crimes, enhanced penalties, and longer statutes of limitations, and grants the Immigration and Naturalization Service (INS) the authority to detain immigrants suspected of terrorism for lengthy, and in some cases indefinite, periods of time. And at the same time that the Act inflates the powers of the executive, it insulates the exercise of these powers from meaningful judicial and Congressional oversight.[25]

Ms. Chang believes that the act gives the federal government "unchecked surveillance powers" related to e-mail, Internet, and personal and financial records. She sees the act as violating both First and Fourth Amendment rights, as well as virtually dismantling the right to privacy.[26]

The Electronic Frontier Foundation (EFF) expresses similar concerns, saying, "The civil liberties of ordinary Americans have taken a tremendous blow with this law, especially the right to privacy in our on-line communications and activities." EFF says that many of the provisions are aimed at nonviolent cybercrimes that do not involve terrorism at all. Specific concerns include increased surveillance, overly broad provisions, and "spying" on Americans by the CIA and the FBI. EFF is also concerned about the lack of accountability to Congress, which may lead to misuse of the new powers.[27]

On November 18, 2002, a three judge federal panel upheld provisions of the USA PATRIOT Act allowing expanded wiretap and other information collecting and sharing by the Justice Department and U.S.

Intelligence Agencies. This decision by the panel stopped efforts of the Foreign Intelligence Surveillance Court to restrict surveillances by the FBI and the Justice Department. After the latest decision, Attorney General John Ashcroft quickly increased surveillance on terrorist suspects. Civil liberties advocates assailed the decision as allowing the government to eavesdrop on telephone conversations, read private e-mail, and search private property, even if there is no evidence of wrongdoing by the targeted individual.[28] The American Civil Liberties Union (ACLU) argued that the ruling violates rights to free speech and due process and said that the ruling would give the government free reign for "intrusive surveillance warrants."[29]

The ACLU has joined with the American Bookseller's Foundation for Free Expression, the Electronic Privacy Information Center, and the American Library Association's Freedom to Read Foundation to file suit against the Department of Justice (DOJ). These organizations allege that the DOJ refuses to release information concerning what actions it has taken under provisions of the USA PATRIOT Act. Of particular concern is the seizing of records from bookstores and libraries even when no criminal activity has been demonstrated. DOJ says it cannot release the information due to possible detriment of national security. The plaintiffs want to build a case that information is being gathered unnecessarily and used improperly.[30]

Attorney General Ashcroft has said, "I don't have the power to erode the Constitution. I wouldn't do it if I could." However, Ashcroft also said, "We don't need any leads or preliminary investigations" to send undercover agents into public meetings or public places, including churches or mosques "under the same terms and conditions of any member of the public."[31] The government only needs a "reasonable indication," rather than the previous standard of probable cause.[32] The chairman of the House Judiciary Committee, James Sensenbrenner disagreed, stating, "We can have security without throwing respect for civil liberties into the trash heap. We don't have to go back to the bad old days when the FBI was spying on people like Martin Luther King." Roger Pilon of the Cato Institute went further, stating, "This is now an executive branch that thinks it's a law unto itself."[33]

Some Congressmen are not satisfied with the Executive Branch's actions under the USA PATRIOT Act. Senator Richard Durbin said the

bill represented a "leap of faith, born of fear. This administration, this Department of Justice, has abused that faith." Senator Patrick Leahy, chairman of the Senate Judiciary Committee, has threatened subpoenas if the Justice Department does not give the requested information. House Judiciary Committee Chairman James Sensenbrenner has echoed the threat of subpoenas.[34]

Supporters of the USA PATRIOT Act contend that the expanded authorities are needed to protect the security of Americans. They are not opposed to civil liberties but, "Dead people have no civil liberties at all."[35] *The Village Voice* has quoted Attorney General Ashcroft as saying, "To those who scare peace-loving people with phantoms of lost liberty, my message is this: Your tactics only aid terrorists, for they erode our national unity and diminish our resolve. They give ammunition to America's enemies."[36] (Please see note). Associate Deputy Attorney General David Kris told the Senate Judiciary Committee, "What is at stake is nothing less than our ability to protect this country from foreign spies and terrorists."[37]

Supporters of the act point out that we are at war, and the old standards no longer apply. With the crisis surrounding U.S. security, reasonable suspicion is a more realistic standard than the probable cause standard, which refers to mere criminal activity, not terrorism. Supporters cite the case of one terrorist, Zacarias Moussaoui. The government was actually arguing over whether to search Moussaoui's computer, even though he was not even in the country legally and could certainly not be considered a U.S. person.[38]

Writing in *The American Criminal Law Review*, Jennifer M. Collins notes that the events of September 11 changed reality. Ms. Collins notes that there has been a strong separation between law enforcement and the foreign intelligence community for the fifty years of the CIA's existence. Now, however, Ms. Collins cautiously argues that the ongoing danger of terrorism justifies "lowering the wall of separation between the grand jury and other agencies of the government to improve coordination and the sharing of national security information—with the goal of safeguarding the nation's security and its citizens."[39]

One recurring theme of supporters of increased government authority is that, without adequate power, the government cannot protect the very liberty Americans hold dear. Laurence Tribe, Harvard Law School, said that, "civil liberties are not only about protecting us from our government.

They are also about protecting our lives from terrorism." Supporters also cite the example of President Abraham Lincoln's emergency actions during the Civil War. When Lincoln suspended the writ of habeas corpus, he justified the action with the statement, "Must a government, of necessity, be too strong for the liberties of its own people, or too weak to maintain its own existence?"[40] Supporters argue that, without the additional authorities given to government by the USA PATRIOT Act, the government will not have the tools of power to defend the lives, much less the freedom, of Americans.

Conclusion

> *For rulers are not a terror to good works, but to the evil. Wilt thou then not be afraid of the power? Do that which is good, and thou shalt have praise of the same: For he is the minister of God to thee for good. But if thou do that which is evil, be afraid; for he beareth not the sword in vain: for he is the minister of God, a revenger to execute wrath upon him that doeth evil.*
>
> —The Holy Bible, King James Version, Romans 13:3-4

The USA PATRIOT Act certainly represents a shift toward security even at the cost of potential loss of freedom. However, the majority of Americans appear willing to accept this shift. In a February 2002 Greenberg poll, sixty-two percent of those responding agreed, "Americans will have to accept new restrictions on their civil liberties if we are to win the war on terrorism." In late September 2001, a NBC/Wall Street Journal poll found seventy-eight percent of respondents approving surveillance of internet communications. Sixty-three percent of respondents to a Harris poll approved camera surveillance on streets and public places. In 1998, Chief Justice William Rehnquist recognized that a national crisis can shift the balance between freedom and security toward security, "in favor of the government's ability to deal with the conditions that threaten the national well-being."[41]

However, as time passes and the events of September 11, 2001, begin to diminish, the minds of the American people may change. A November 2001 Investor's Business Daily poll found 58 percent of respondents

worried about losing "certain civil liberties in light of recently passed anti-terrorism laws." By March 2002, a Time/CNN poll found 62 percent of respondents concerned that "the U.S. Government might go too far in restricting civil liberties."[42] Americans in general may be willing to accept some loss of freedom so long as the government uses the new powers to consistently target the "evil doers" of terrorism. However, if Americans believe their own personal civil liberties have been unnecessarily or overly limited, active opposition is likely to increase.

Does America still have a healthy balance between freedom and security? At this point, the fulcrum has shifted toward security with the potential loss of a degree of the freedom previously enjoyed by Americans. Whether this shift toward security will have significant permanent effect obviously remains to be seen. If America follows historical patterns, the people will force the fulcrum back toward freedom once the threat to security is perceived as sufficiently reduced. In the meantime, to the extent that any degree of freedom is lost for Americans, the terrorists will have achieved some measure of victory.

Notes

1. "The Question of a Bill of Rights," Letter to Thomas Jefferson, October 17, 1788, from James Madison. On-line. Internet, 2 December 2002. Available from http://www.constitution.org/jm/17881017_bor.htm.

2. Mary Minow, "The USA PATRIOT Act," *Library Journal*, vol. 127, October 1, 2002, 52-55.

3. "Your Right to Privacy." On-line. Internet, 25 November 2002. Available from http://www.rightoprivacy.com/.

4. Roy Webb, archivist, "Japanese-American Internment Camps During World War II." On-line. Internet, 25 November 2002. Available from http://www.lib.utah.edu/spc/photo/9066/9066.htm.

5. "Face Recognition," Electronic Privacy Information Center. On-line. Internet, 25 November 2002. Available from http://www.epic.org/privacy/facerecognition/.

6. Jane Adas, "New York Congressman Nadler Calls USA PATRIOT Act Extreme Danger to Civil Rights," *The Washington Report on Middle East Affairs*, vol. 21, August, 2002, 57-58.

7. Nick Gillespie, "What Price Safety?: Freedom for Safety," *Reason*, vol. 34, October, 2002, 24-26.

8. Minow, 52-55.

9. Adas, 57-58.

10. Alisa Solomon, "Things We Lost in the Fire," *The Village Voice*, vol. 47, September 11-September 17, 2002, 32-36.

11. *USA PATRIOT Act*, H.R. 3162, October 24, 2001, 10.

12. Ibid., 25.

13. Minow, 52-55.

14. Ibid., 52-55.

15. *USA PATRIOT Act*, 37.

16. Ibid., 71.

17. Ibid., 103-106.

18. Ibid., 119-126.

19. Ibid., 132.

20. Ibid., 132-149.

21. Ibid., 150-154.

22. Ibid., 154.

23. Ibid., 155.

24. Gina Holland, "Government Surveillance Powers Scrutinized," *The Montgomery Advertiser*, November 20, 2002, 5A.

25. Nancy Chang, "The USA PATRIOT Act: What's So Patriotic About Trampling on the Bill of Rights?" November, 2001, Center for Constitutional Rights. On-line. Internet, 26 November 2002. Available from http://www.ccr-ny.org/whatsnew/usa-patriot-act.asp.

26. Chang, accessed 26 Nov. 02.

27. "EFF Analysis of the Provisions of the USA PATRIOT Act," Electronic Frontier Foundation. On-line. Internet, 26 November 2002. Available from http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html.

28. Holland, 5A.

29. Curt Anderson, "Ruling Expands Wiretap Powers," *The Montgomery Advertiser*, November 19, 2002, 6A.

30. Steven Zeitchik, "Groups Sue over Patriot Act," *Publishers Weekly*, vol. 249, October 28, 2002, 16.

31. Nat Hentoff, "Citizens Resist War on the Bill of Rights," *Free Inquiry*, vol. 22, Fall 2002, 13-14.

32. Joe Feuerherd, "September 11: A Year Later—Congress Questions Patriot Act Policies," *National Catholic Reporter*, vol. 38, September 6, 2002, 7.

33. Hentoff, "Citizens Resist War on the Bill of Rights," 13-14.

34. Jess Bravin, "Leahy Warns Justice Department on New Powers," *The Wall Street Journal*, September 11, 2002, A4.

35. Minow, 52-55.

36. Nat Hentoff, "The Sons and Daughters of Liberty," *The Village Voice*, vol. 47, July 2, 2002, 34. *(note that this quote is reported by The Village Voice, which may be a biased source. The context of the alleged quote is not provided in The Village Voice article.)*

37. Bravin, A4.

38. Richard Lowry, "A Better Bureau," *National Review*, vol. 54, July 1, 2002, 28-30.

39. Jennifer M. Collins, "And the Walls Came Tumbling Down: Sharing Grand Jury Information with the Intelligence Community under the USA PATRIOT Act," *The American Criminal Law Review*, vol. 39, Summer, 2002, 1261-1286.

40. Mackubin Thomas Owens, "Liberty & Security: A Prudential Balance," *National Review On-line*. On-line. Internet, 01 December 2002. Available from http://www.nationalreview.com/comment/comment-owens120401.shtml.

41. Jon B. Gould, "Playing With Fire: The Civil Liberties Implications of September 11th," *Public Administration Review*, vol. 62, September, 2002, 74-79.

42. Gould, 74-79.

CHAPTER 3

The Colombian War and the Narco-Terrorist Threat

Dario E. Teicher

Introduction

The purpose of this chapter is to provide justification for regarding the narco-war in Colombia as a threat to the homeland security of the U.S. In order to support this premise, U.S. interest in Colombia will be defined in terms of geopolitical and socioeconomic impact. The warring factions will be outlined to ascertain that, in fact, defeating the FARC (*Fuerzas Armadas Revolucionarias Colombianas*) is key to winning the war in Colombia.

Another aspect to be discussed is the threat that the intrinsic relationship between the drug trade and international terrorism poses to the U.S. homeland. This chapter intends to provide evidence that international terrorism may already be involved in Colombia's war and, therefore, our robust counter-drug defenses should expand to include this additional threat. Ultimately, the analysis centers on the need to win the war in Colombia to secure America's southern border.

Background

The Strategic Importance of Colombia to the United States

Colombia has been engaged in a vicious civil war for over 40 years. With each passing year, Colombia slips further into anarchy and today may be on the verge of becoming the world's first narco-terrorist state.

Geopolitical Interests

A narco-terrorist state, not halfway around the world, but only a 3-hour flight away from Miami, Florida, should cause alarm bells for several vital reasons. For example, Colombia is the only South American country, which borders both the Atlantic and Pacific Oceans straddling the north-south sea lines of communication between the United States and Latin America. Trade in excess of $100 billion annually traverses these sea routes.[1] Also, all land routes from the rest of South America converge in Colombia before entering Central America and then North America. The North American Free Trade Agreement (NAFTA – Mexico, Canada, and the U.S.) envisions one day including the entire Western Hemisphere, thus becoming the Free Trade Area of the Americas. Hence, the war in Colombia must be won to avoid a strategic trade choke point in the Americas.[2] Additionally, Colombia borders on Panama where the Canal Zone remains strategically important and it also borders on Venezuela, the number one supplier of crude oil to the U.S.[3] Furthermore, in 1997, the U.S. National Security Strategy explained:

> The principal security concerns in the hemisphere are transnational in nature, such as drug trafficking, organized crime and money laundering, illegal immigration, and instability generated from corruption and political or social conflict.[4]

In Colombia, every one of the U.S.'s "principal security concerns" exists in epidemic proportions. Therefore, U.S. security interests in the Western Hemisphere are under assault precisely because of the narco-war in Colombia.

Socioeconomic Interests

Colombia's crime ridden society is a "clear and present danger" to the very social fabric of its hemispheric neighbors.[5] For instance, in the United States:

> 70 percent of the cocaine… originates from Colombia… with a street value of $30 billion. In addition, 75 percent of the heroin seized by U.S. authorities on the East Coast is Colombian. …Drug consumption caused 100,000 deaths in the [decade of the

> 1990s.] There are 13.9 million drug users and 3.6 million addicts in the United States. The total societal cost is estimated at $300 billion annually from lost productivity, crime, policing, incarceration, rehabilitation, insurance and hospital care.[6]

"Colombia produces 80 percent of the world's cocaine…" and the U.S. is its number one market, but not the only one.[7] The drug trade routes north are causing drug markets to develop in Central America *(the Transit Zone)* as the drug runners use a portion of their contraband to exchange with local hoods for logistics support en route to the U.S. These nations do not have the resources to fight the drug plague. They are developing democracies that could unhinge, becoming narco-states following the Colombian model.[8] Even Mexico, a large and more affluent nation, "…fears the 'Colombianization' of its own political process…"[9] The statistics are staggering and surely make Colombia's drug traffickers a threat to homeland security in the United States and throughout the region.

Defining the Enemy

The Cartels

"The cartels of the 1980s were set up…like vertically integrated corporations… Police needed to recruit only a single strategically placed informant to disrupt the entire cartel." Moreover, the cartels flaunted their power and were incredibly brutal, bombing and murdering scores of government officials and innocent by-standers. "Colombia's trigger-happy first generation of coke lords tended to be short-term scary but long-term dumb." By the 1990s, the Cali, and the even more notorious, Medellin Cartels had been rolled up. Nevertheless, like the mythical hydra monster, decapitating these two powerful cartels only led to the creation of many small technologically and socially sophisticated, and less integrated cartels. In other words, the new drug lords of Colombia blend well into high society and are not excessive in their use of violence. They gather together to pool resources for a big drug smuggling deal and quickly withdraw into the fold of society.[10]

The Leftist Guerillas

The end of the Cold War should have also meant the end for the communist guerillas of Colombia, as aid from the USSR evaporated. In fact, the Colombian leftists were never dependent on outside sources to fund their campaigns. Instead, the communist groups first survived by making raids on isolated farms to secure supplies and ambushed small military outposts to obtain hardware. Later, they moved into resource rich areas of Colombia, where they established extortion and protection rackets.

Meanwhile, by the 1980s, the small agricultural farmers *(campecinos)* were growing marijuana and coca plants for the drug lords who would protect them using their private security forces. Marijuana and coca was a more profitable cash crop. The communist guerillas, fearing they would lose their "social base," became astute learners of the capitalist ways of the drug trade.

By the 1990s, the guerillas were collecting "taxes" on the drug trade while providing security for the fields, through the transportation network, and even providing escort beyond the Colombian borders.[11] In 2000, the U.S. Drug Czar, General Barry McCaffrey (ret.), and Ambassador to Colombia, Anne Patterson, accused the FARC of "…shipping cocaine to U.S. markets…" and went so far as to accuse them of operating "…like the big cartels."[12]

The various criminal enterprises, including kidnapping-for-ransom and murder-for-hire, have given the guerillas fabulous wealth and increased their numbers. The best known and the largest group are the FARC with 15,000 – 20,000 combatants. Another group is the ELN (*Ejercito de Liberacion Nacional*) with 3,000 – 6,000 combatants. Additionally, a smaller group of a few hundred guerillas, also operating against Colombia, is the Maoist EPL (*Ejercito Popular de Liberacion*). Additionally, at least, four other groups operated in Colombia but over the long years merged with the larger groups, faded, or made peace.[13]

The Paramilitaries

The failure of the Colombian Government forces to adequately defend the country against the leftist insurgency gave rise to numerous private armed organizations. These organizations operated in areas where the government forces were scarce. In Colombia, both the wealthy and the

narco-traffickers employ the services of private security. Initially, these units were raised with the full support and encouragement of the government, but charges of human rights violations by paramilitaries, involvement in criminal enterprises, and U.S. pressure forced the Colombian Government to reverse its policy. Regardless, accusations continue to be made against the Colombian military that they are still coordinating actions with the paramilitaries.[14]

The paramilitaries had been fragmented but "…in recent years the groups have clustered under an umbrella organization, the AUC (*Autodefensas Unidas de Colombia*)" and number approximately 8,000 combatants.[15] Their intense brutality against the leftist guerillas and suspected sympathizers forced the U.S. State Department to list the AUC as a terrorist organization. Perhaps in response but certainly to obtain a political voice, on 4 September 2001, the AUC "…announced it was forming a political organization called the National Democratic Movement…"[16]

The AUC's operations are funded by private contributions from wealthy landowners. Additionally, the AUC, like other armed organizations in Colombia, finances its operations through the drug trade. For instance, the successful 1998 U.S. DEA and Colombian police roundup of the powerful Bernal Syndicate, one of the modern high-tech cartels, discovered two senior members who were also members of the paramilitaries.[17]

The Government

The Colombian Government is under siege from all sides of the political spectrum, including powerful criminal conglomerates engaged in drug smuggling, kidnapping, arms smuggling, illegal alien smuggling, money laundering, counterfeiting, etc. Analysts have made strong arguments that the Colombian economy is already a narco-economy. They point to Colombia's economic success in the 1980s despite the war. Colombia was able "…to continue to service its foreign debt, while other Latin American countries had to reschedule theirs, [because of] …the vast sums of drug money – estimated at between $5 billion and $7 billion annually – that entered the country."[18]

Arguably, the drug connection has permeated all corners of Colombia. For example, "the Colombian Government suffered a severe

loss of legitimacy… after revelations of drug network financing of the successful presidential campaign of Liberal Party candidate Ernesto Samper in 1994."[19] On September 20, 1996, President Samper was once again embarrassed when "…drug-sniffing dogs found 8 pounds of heroin on the official [Colombian Air Force] plane that Samper was to fly to New York" to speak at the United Nations on the evils of drugs.[20] Two days later, Colombian "…officials announced the arrest of 11 Colombian Air Force personnel, including several officers…"[21]

One must wonder how broad the corruption is when it can undermine the democratic process and the military charged with defending it. It is not surprising then when CNN reports "…that the FARC sometimes has access to intelligence about raids by the military before they occur."[22] The question then becomes, has the Colombian war already been lost?

The Global Drug Network

Sanctuary

Perhaps in desperation, deep in the Southern Colombian coca region an area the size of Switzerland *(La Zona de Despeje – 16,000 square miles)* was ceded to the FARC in 1999 to open a peace dialogue. Colombian President Andres Pastrana, with the support of the Clinton Administration, crafted a "land for peace" proposal. Although the FARC already controlled this vast area, the Colombian military would now be forbidden from conducting operations into the region. Initially, the proposal was to be a 90-day cease-fire but it has become part of the status quo of the Colombian war, so long as the FARC continues to "talk peace."[23]

There is every indication the FARC will "talk peace" ad infinitum, while waging war and protecting their criminal enterprises. Coincidentally, the ELN and AUC have publicly demanded similar deals. According to General McCaffrey, the *Despeje* was a mistake because "…there was little incentive for the FARC to lay down its arms…" and instead helped to secure nearly $1 billion a year in profits from the drug trade.[24]

Connection to an International Axis of Terror

Terror International has taken notice of the safe-haven in the jungles of Colombia and it may already be an important link in the terror network. The *Despeje* is already a sanctuary for the production of cocaine. The FARC then uses the cocaine shipments to exchange them for weapons and dollars.

The Crime Syndicate Connection

The FARC has plugged into crime networks from Mexico to Russia and perhaps elsewhere. Authorities have confirmed the weapons connection extends to Mexico where an alleged FARC envoy was captured attempting to make a "…cocaine-for-guns deal with Mexico's Arellano Felix Drug Cartel."[25] Even more intriguing is the FARC's connection to the Russian Mafia; where NBC reported on April 9, 2001, "Russian crime syndicates and military officers are supplying sophisticated weapons to Colombian rebels in return for huge shipments of cocaine…"[26] The report goes on to explain that the arms are transported in IL-76 cargo planes from Russia or Ukraine, with stops in third world locations such as Amman, Jordan, where authorities are bribed including promises of a part of the cocaine shipment on the return trip. The IL-76 flies directly into the *Despeje* where the FARC off-loads weapons and on-loads cocaine.[27]

The Rogue State and International Terrorist Connection

Arguably, the *Despeje* and cocaine have made the FARC a major player on the international terror scene. Perhaps most ominous is a possible Iran connection. According to ABC News, in 2000, Iran attempted to establish a meat packing plant in San Vicente del Caguan – the headquarters of the FARC in the *Despeje*. Although initially, Colombian authorities had agreed to the project, they withdrew the authorization when the U.S. became aware and advised the Colombian Government that proceeding would place a $1.35 billion emergency aid package in jeopardy. Also, ABC went on to report "…*Hezbollah* is already well established in South America," including facilities in Isla Margarita off the coast of Venezuela, along the Colombian and Paraguayan borders in Brazil, and in Argentina.[28]

In addition to suspect connections to rogue states such as Iran, and possibly terrorist groups such as Hezbollah, the FARC was linked to the IRA (*Irish Republican Army*) when Colombian authorities captured three IRA "explosives experts" shortly after they departed the *Despeje*.[29] Consequently, U.S. authorities have vowed to keep close scrutiny of the *Despeje* because the FARC has become a major player in an "axis of terror" that includes international crime syndicates, international terrorists, and rogue nations.[30]

The Narco Trade Routes

In Southern Colombia, the cartels, the guerillas, and the paramilitaries are busy harvesting the white gold (cocaine), which finances their nefarious activities. The vast majority of the cocaine is headed north to America's streets. The cocaine is moved internally to clandestine points of departure. Every means of conveyance is employed to move drugs into the U.S., e.g., personal luggage, cars, trucks, even in the stomachs of people known as "mules." Large quantities of cocaine used to move by illegal aircraft and it is still employed but the favored method is by sea where the cocaine dealer can move tons to market. The Caribbean had been the preferred sea route in the 1980s but the geography (the major Islands are natural bottlenecks) allowed successful interdiction by the U.S. and friendly countries. The smugglers have shifted to the unhindered vastness of the Eastern Pacific.[31]

The goal of the smugglers is not to reach the U.S. coast but to make it to Mexico. The Colombian drug smugglers have formed "a symbiotic relationship" with Mexican crime syndicates. In some cases, they will vary the routes and instead arrive in one of the Central American countries, where the cargo will then be moved by road after leaving a small quantity for the local market. Once in Mexico, the cargo is consolidated in smaller packages and moved by trucks to several distribution points along the nearly 2,000-mile U.S. border with Mexico. The cocaine then crosses at points in California, Arizona, New Mexico, and Texas.[32]

Business has been booming; the Colombia-Mexico connection has expanded moving heroin, methamphetamine and, of course, they have always shipped marijuana.[33] Additionally, illegal migrant smuggling also occurs along these same pipelines earning the smuggler as much as

"$70,000 per person."[34] One can surmise, the FARC "…may have become the richest Marxist guerilla faction in history…"[35]

The Decisive Phase of the Drug War

Plan Colombia

Previously, "…U.S. policy carefully delineated the boundary between counternarcotics and counterinsurgency…Mindful of the absence of support at home for counterinsurgency…"[36] Nonetheless, there is only one war in Colombia, and it is those who run drugs against those who do not. One can debate whether the leftist ideological slogans are Cold War relics; regardless, "…Colombia is no longer a battle over ideology, but a battle over… narco-dollars…"[37]

The U.S. Congress has finally faced reality, eliminating the artificiality that hindered the war on drugs, such as, a few years ago when the U.S. provided helicopters to Colombia, which could not be used for counterinsurgency.[38] The U.S., European Union, Canada, Japan, and International Institutions have bought into President Pastrana's Plan Colombia. The plan defines ten elements:

- Economic recovery through free trade agreements to encourage foreign and domestic investment to create jobs.
- Fiscal and financial reform.
- A peace strategy to achieve a negotiated settlement with the guerillas.
- Strengthening the armed forces and police to uphold the rule of law and restore security throughout the country.
- Judicial reform to ensure impartial justice.
- A counter-narcotics strategy in partnership with other countries.
- Agricultural development to provide an alternative to coca plantation.
- Popular mobilization in an anticorruption effort.

- Social programs for health, education, and alleviation of poverty.
- Mobilization of the international community to participate in the plan.[39]

One can see Plan Colombia is a set of guiding principles and not meant to be a war winning strategy. Its worst critics may even call it a 'pipe dream.' Nevertheless, the U.S. Congress authorized $1.35 billion in emergency aid to Colombia in July 2000, with additional funding to follow, and the U.S. military is moving ahead with training support for the Colombian military. Indeed, already U.S. Special Forces are in-country training Colombian troops at bases deep in guerilla territory.[40]

Warning Signs

Colombia's leftist guerillas call Plan Colombia "a declaration of war" by the U.S.[41] Commandante Raul Reyes, the third ranking leader of the FARC, attributes the plan as "…a way of interfering in the domestic affairs of Colombia."[42] The FARC has announced, "…foreign military personnel in the combat zones will be military targets."[43] This threat was aimed at the U.S. Special Forces already in Colombia.

The Seattle Times reported in September 1999 that Colombian authorities had raided a warehouse where members of the FARC were building a Russian diesel submarine to use in their transnational criminal endeavors. The *London Times* carried a story in which Colombian police seized 1.5 pounds of enriched uranium, which a self-proclaimed scientist hoped to turn into a bomb.[44] There are even allegations of the guerillas having used "a toxic gas" in an assault on a police station, which killed four.[45] One can see that the leftist guerillas are very wealthy, technologically competent, and have a very dangerous reputation.

Colombian leftist guerillas never stopped fighting the Cold War and may still believe their slogans—in which case, they remain ideological enemies of the U.S. and its way of life. The FARC and ELN must conclude that events since September 11, 2001, changed U.S. public opinion regarding U.S. support for a counterinsurgency in Colombia. In particular, they are aware that although not mentioned by name, President Bush was including them when he defined America's enemy in the war on

terror as "…every terrorist group with global reach…"[46] Therefore, the U.S. must not let its guard down as it did prior to "9/11." The U.S. must look south and not just east. The FARC or ELN could decide to strike at the center of gravity of the Colombian Armed Forces – The United States of America.

Consequences

The U.S. Defense Network

As a result of the 20-year drug war, the U.S. has created a robust command and control interagency organization to attempt to keep drugs away from America. The front line of the war effort has of course, been the Colombian security forces with support from the U.S. Drug Enforcement Administration and other U.S. Government agencies, including DOD. There are three key organizations, which make command and control possible and response effective despite coordination with many U.S. Government agencies.

The Joint Inter Agency Task Forces (JIATF)

JIATF EAST is responsible for coordinating the drug war in the Southern Command Area of Responsibility (AOR) and JIATF WEST is responsible for the drug war in the Pacific Command AOR. The JIATFs have access to all necessary intelligence being gathered against drug smugglers. They also have air and maritime assets TACON (tactical control) available to them from the theater combatant commanders who retain OPCON (operational control). The JIATFs have representatives from key government agencies including each of the DOD service branches, key members from the Justice Department such as FBI and DEA, and liaison officers from friendly countries in the AOR. U.S. Coast Guard Admirals command both JIATFs.[47]

Joint Task Force Six (JTF-6)

JTF-6 is directly involved in homeland defense against drug smugglers. They support law enforcement agencies engaged in counter-drug operations. JTF-6 is manned by personnel from all U.S. military

service branches, bringing a broad set of capabilities to the fight. For example, JTF-6 can fly a reconnaissance mission for the Border Patrol, establish a listening/observation post on the Canadian border, or provide divers to inspect the underside of a suspect vessel in the Port of Galveston, Texas.[48]

The Colombian "Pipe Dream"

The Dim Hope of Success

The unfolding of the violence in Colombia left President Pastrana and the U.S. with no other alternative but to execute a plan whose chance of success may be very limited. Politicians at various times in Colombia's history have introduced "peace strategies," anti-corruption campaigns, and even five constituent assemblies (1827, 1885, 1905, 1952, and 1957) to address the nation's tendency towards corruption and violence.[49] In the long run, they all failed. Regardless, by the beginning of the 1990s, the counterinsurgency was going poorly and the nation was once again in chaos.

> Drug dealers were responsible for the death of some fifteen hundred people between August 1989 and August 1990, including the three presidential candidates who were assassinated in the 1990 presidential election. And paramilitary groups functioned in many rural parts of the country, at times assisted by drug dealers and at others by the armed forces… Common crime was rampant, with the government itself stating that 80 percent of the crimes were not reported and of those reported, 90 percent did not lead to indictment and conviction. During the 1980s murder became the most common cause of death in the country.[50]

Plan Colombia in Execution

The U.S. and other wealthy foreign nations are giving President Pastrana every opportunity to bring his country back from the brink ($3.5 billion in foreign assistance for 2000 and more to follow.)[51] The first major element of "Plan Colombia" began in 1999 with the opening of a peace dialogue with the FARC.

Pastrana correctly concluded law and order has too many enemies in Colombia. The most powerful is the FARC but the various cartels, the ELN, and the AUC are also involved in causing great harm. Furthermore, the drug trade is the primary means of funds for these organizations. The hope then is to strengthen the military and police to destroy the drug trade. If the FARC is detached from its revenue source, then maybe they will make peace and, if they demobilize under a fair amnesty program, perhaps the much smaller ELN will follow suit. The AUC should also demobilize since the "…paramilitaries [would] have less reason for being." The war against the cartels would then become a controllable police affair.[52]

Hope Shining Brighter

As of January 2002, the FARC refuses to make peace. The conclusion could be Plan Colombia is on its way to failure or perhaps the FARC has not yet been squeezed. Despite this, events on the battlefield may be changing for the better. "As recently as 1998, the FARC beat the Colombian Army in battalion-size engagements." However, this is no longer the case.[53] Colombia's newly reinvigorated "…Rapid Deployment Force… conducted very successful operations in 2001, including *"Gato Negro"* which captured the notorious Brazilian drug lord, Fernandinho (who was trading money and arms for cocaine with the FARC), and this success seems to be the trend.[54]

Conclusions

Has the Colombian War already been Lost?

Governor Gary Johnson of New Mexico argues "drug problems are health problems, not criminal justice problems" and he goes on to add, "the war on drugs is an absolute failure."[55] One can engage in mental gymnastics with the validity of his first statement but one must hope his second statement is wrong. Otherwise, the only victors to this point are the leftist guerillas and the U.S. can ill afford such a hostile adversary so close to our shores.

The FARC has drug, personnel, and weapons smuggling pipelines that lead into the American heartland. Furthermore, they are opposed to

the American way of life and have identified the U.S. as their enemy. The leftist guerillas also keep relations with other international terrorist organizations and nations hostile to the U.S. The Green Berets in Colombia are a symbol of U.S. vigilance and resolve to turn the tide of the war.

Far from being a lost cause, the Colombian War is entering a new perhaps-decisive phase. "Remember 9/11" could be the battle cry that is bringing U.S. military support to the Colombian Armed Forces. Gone are the excessive restrictions, which sought to keep U.S. assistance away from counterinsurgency. There is a realization that the counternarcotic war can only be won if the counterinsurgency war is successful. Operation *Gato Negro* is an important indicator that the tide can be turned in favor of the forces of law and order.

In Defense of the Homeland

Defeating the FARC and other leftist guerillas in Colombia is the surest way of defending the homeland from a southern threat. The threat is more pronounced because the IRA, Al Qaeda, the PLO, Hezbollah, FARC, ELN and other terrorists share one common source of revenue; they are plugged into the global drug network. Although drug revenue is not the only source of income, it is a major portion of the financial base of international terrorism.[56] The interest shown by the IRA, Hezbollah, Iran and other criminal elements highlight the importance of the southern coca region of Colombia to international terrorism. Therefore, one can safely argue the war in Colombia is a battlefield of the global war on terror.

Monitoring and interdicting this battlefield, through the transit zone, and across U.S. borders is done by U.S. agencies involved in fighting transnational crime. They are represented at JIATF EAST and JIATF WEST, where coordination, planning, and execution of the nation's counter-drug strategy occurs. Another key organization in the homeland defense against drugs is JTF-6, which provides DOD assets for operations along any American frontier and well inside U.S. borders.

These assets can be geared towards a broader defense of the homeland. Although previously, the overarching threat was transnational crime focused on drugs, the mission statement now would include international terrorism. As the nation prepares to defend the homeland

against the next terrorist onslaught, it would be foolish not to include this robust time-tested architecture. One cannot overemphasize that the "war on drugs" is a major aspect of the "war on terror."

Notes

1. "U.S. Trade Balance with Latin America (Excluding Mexico)," *Foreign Trade Division*, 18 January 2002, U.S. Census Bureau, on-line, Internet, 8 February 2002, available from www.census.gov/foreign-trade/balance/c0009.html.

2. Marcella, G. and Schultz, D., *Colombia's Three Wars: U.S. Strategy at the Crossroads*, U.S. Army War College, Strategic Studies Institute, 5 March 1999, 5.

3. "Chapter 4, U.S. Crude Oil Imports: Growing U.S. Dependence," *Petroleum 1996: Issues and Trends*, Energy Information Administration, 1996, on-line, Internet, 8 February 2002, available from http://www.eia.doe.gov/pub/oil_gas/petroleum/analysis_publications/petroleum_issues_trends_1996/CHAPTER4.PDF, 12.

4. "A National Security Strategy for a New Century," *National Security Council*, May 1997, White House, on-line, Internet, 8 February 2002, available from http://clinton2nara.gov/WH/EOP/NCS/Strategy/#preface.

5. Clancy, T., *Clear and Present Danger*, G. P. Putnam's Sons, 1989.

6. Marcella, G. and Schultz, D., *Colombia's Three Wars*, 7.

7. Ibid., 7.

8. Johnson, K., and Teicher, D., "Fighting Narco-trafficking and the Forward Operations Location," *Frente a Frente: An interview with Eduardo Torres*, TV12, El Salvador, 14 July 2000.

9. Marcella, G. and Schulz, D., *Colombia's Three Wars*, 4.

10. Contreras, J. and Ambrus, S., "Fighting the New Drug Lords," *Newsweek International*, 21 February 2000, Cannabis News, on-line, Internet, 6 February 2002, available from www.cannabisnews.com/news/thread4738.shtml.

11. Rabasa, A. and Chalk, P., *Colombian Labyrinth: The Synergy of Drugs and Insurgency and Its Implications for Regional Stability*, Rand, 2001, 24, 26.

12. Tamayo, J. O., "U.S. Charges Raise Suspicions of Widening Role in Colombia," *The Inquirer*, 20 December 2000, Knight Ridder News Service, on-line, Internet, 6

February 2002, available from http://inq.philly.com/content/inquirer/2000/12/20/national/COLOMBIA20.htm?template-apri.

13. Rabasa, A., and Chalk, P., *Colombian Labyrinth*, 27, 31, 32.

14. Ibid., 53-54.

15. Ibid., 54.

16. "U.S. Labels AUC Terrorist," *Weekly News Update on the Americas*, 17 September 2001, Nicaragua Solidarity Network of NY, on-line, Internet, 6 February 2002, available from www.locombia.org/1000725744/index.html.

17. Contreras, J. and Ambrus, S., "The DEA's Nightmare."

18. Fleischer, L. and Lora, E., *Colombian Policy in the Mid-1990s: A Report of the CSIS Americas Program*, the Center for Strategic and International Studies, 1994, 46.

19. Rabasa, A., and Chalk, P., *Colombian Labyrinth*, 3.

20. "Colombian President Speaks at U.N., Drugs found on His Plane," *Newsbriefs*, November 1996, National Drug Strategy Network, on-line, Internet, 6 February 2002, available from http://www.ndsn.org/NOV96/COLOMBIA.html.

21. Ibid.

22. Karon, T., "Why U.S. Top Brass Fears Getting Dragged into the Colombian Drug War," *Time.Com*, 31 March 2000, Cable News Network, 2001, on-line, Internet, 6 February 2002, available from www.cnn.com/2000/WORLD/americas/0331/Colombia 3_31.a.tm.

23. Ehrenfeld, R., "U.S. Ignored Money Trail: Bush is Doomed to Fail if He doesn't Cut-off Financing of Terrorist," *Special to The Detroit News*, 30 September 2001, Center for International Integrity, on-line, Internet, 6 February 2002, available from www.public-integrity.org/publications10.htm.

24. "U.S. Drug War Chief Says Marxist Rebels Behind Colombian Cocaine Traffic," *Reuters*, 20 November 2000, Global Exchange, on-line, Internet, 6 February 2002, available from www.globalexchange.org/colombia/reuters112000.html.

25. Tamayo, J. O., "U.S. Charges Raise Suspicions of Widening Role in Colombia."

26. Lackey, S. and Moran, M., "Russian Mob trading Arms for Cocaine with Colombian Rebels," *Special Reports*, 9 April 2001, MSNBC, on-line, Internet, 6 February 2002, available from www.msnbc.com/news/391623.asp?cpl=1.

27. Ibid.

28. "U.S. Stops Iranian Project in Colombia," *abcNews.com*, ABC News Internet Ventures, on-line, Internet, 6 February 2002, available from http://my.abcnews.go.com/ PRINTERFRIENDLY?PAGE= http://abcsource.starwave.com/, 2000.

29. Marcella, G., "Plan Colombia: An Interim Assessment," *Hemisphere Focus, Vol. X, Issue 02*, 25 January 2002, The Center for Strategic & International Studies, on-line, Internet, 28 January 2002, available from Hwww.csis.org/americas/pubs/ h020125.htmH, 2001.

30. "U.S. Stops Iranian Project in Colombia," *abcNews.com.*

31. Chavez, E. J., "DEA Congressional Testimony," *Statement*, 13 April 2001, U.S. Drug Enforcement Administration, on-line, Internet, 10 February 2002, available from www.usdoj.gov/dea/pubs/cngrtest /ct041301.htm.

32. Ibid.

33. Ibid.

34. Greene, J. R., "U.S. and Multinational Coalition Disrupts Migrant Smuggling Operations," *Global Issues: Arresting Transnational Crime*, August 2001, U.S. Immigration and Naturalization Service, on-line, Internet, available from http://usinfo.state.gov/journals/itgic/0801/ ijge/gj04.htm.

35. Karon, T., "Why U.S. Top Brass Fears Getting Dragged into the Colombian Drug War."

36. Marcella, G., "Plan Colombia: An Interim Assessment."

37. DeLagarza, P., "To Some, Aid to Columbia a risky Maneuver for U.S.," *Chicago Tribune*, 18 February 2000, Cannabis News, on-line, Internet, 6 February 2002, available from www.cannabis news.com/news/thread4765.shtml.

38. Marcella, G., "Plan Colombia: An Interim Assessment."

39. Rabasa, A., and Chalk, P., *Colombian Labyrinth*, 61-62.

40. Selsky, A., "U.S. Troops in Colombia Threatened," *The Associated Press*, 1 October 2000, University of Virginia, on-line, Internet, 6 February 2002, available from http://lists.village.virginia.edu /lists_archive/sixties-1/1864.html, 2000.

41. McInerney, A., "Plan Colombia: "Declaration of War" Forces Line up For, Against Revolution," *Workers World Service*, Communist Party of Aotearoa, on-line,

Internet, 5 February 2002, available from Hhttp://home.clear.net.nz/pages/cpa/news/archive.htmH.

42. DeLagarza, P., "To Some, Aid to Columbia a risky Maneuver for U.S."

43. Selsky, A., "U.S. Troops in Colombia Threatened."

44. Johnson, Stephen, "U.S. Coalition Against Terrorism should Include Latin America," *Backgrounder, No. 1489*, The Heritage Foundation, 9 October 2001.

45. "Allegations that Colombian Rebels Used "Gas" in Attack on Police Station," *Emergency Net News*, 4 September 2001, ERRI, on-line, Internet, 6 February 2002, available from Hhttp://www.emergency .com/cntrterr.html#Question-8H.

46. Bush, G. W., "President Declares Freedom at War with Fear," *Address to a Joint Session of Congress and the American People*, 20 September 2001, The White House, on-line, Internet, 5 December 2001, available from Hwww.whitehouse.gov/news/release/2001/09/20010920-8.htmlH.

47. "Joint Inter Agency Task Force (JIATF) East," *JIATFE*, FAS.Org., on-line, Internet, 11 February 2002, available from http://fas.org/irp/agency/dod/usjfcom/jiatf-e/index.html.

48. "Joint Task Force Six," *JTF-6*, U.S. Army, on-line, Internet, 10 February 2002, available from http://www-jtf6.bliss.army.mil/html.

49. Kline, H. F., *State Building and Conflict Resolution in Colombia, 1986 – 1994*, The University of Alabama Press, 1999, 155.

50. Ibid., 155.

51. Rabasa, A., and Chalk, P., *Colombian Labyrinth*, 62.

52. Marcella, G., "Plan Colombia: An Interim Assessment."

53. Ibid.

54. Ibid.

55. "Leaders Debate Legalization of Drugs," *The Associated Press*, 16 November 2001, Cannabis News, on-line, Internet, 6 February 2002, available from www.cannabis news.com/news/thread11356.shtml, 2001.

56. Ehrenfeld, R., "U.S. Ignored Money Trail."

CHAPTER 4

Protecting America's Seaports: The Vulnerability of Intermodal Commerce

L. Edward Mayer

Few Americans appreciate the fact that liner shipping and container ports are key elements through which flows the vast array of products available for their purchase.

—Jon S. Helmick
Society of Logistics Engineers

Introduction

Liner shipping is the backbone of international trade in manufactured goods. Liners, sailing on regular schedules along established ocean trade lanes, move vast quantities of consumer, industrial, and military commodities. Liners transport 95 percent of peacetime commerce and wartime equipment and supplies. Containerized cargo is the method of choice between developed economies, and 16,000 containers enter the U.S. every day at any one of 361 seaports; the biggest U.S. seaports being Los Angeles, Long Beach, and New York/Jersey City.[1]

Intermodal Commerce

Intermodal commerce, or the container trade, is the containerized shipping of cargo. Ships loaded with as many as 6600 Twenty Equivalent-foot Unit containers (TEU) arrive in seaports worldwide and quickly transfer their cargo onto various forms of land transportation. In one eight hour period, a 6600 TEU "mega ship" can be off-loaded and readied for reload.[2] The TEUs are double stacked on railcars adjacent to the seaport or are placed on flatbeds and driven out using tractor-trailers.

In the intermodal business, time is money. Ninety percent of the TEUs clear customs electronically using the U.S. Customs Service's Automated Commercial Environment (ACE). ACE is a comprehensive system used by the U.S. Customs Service to track, control, and process all commercial goods imported into and exported from the United States. Shipping companies transmit manifests for their ships in advance so when the containers are offloaded they can be immediately transferred to land transportation.[3] This is one reason why only 2 percent of all TEUs entering the U.S. are searched by the U.S. Customs service.[4]

The Security Dilemma

The terrorist attacks on September 11, 2001, brought to light the vulnerability of America's critical infrastructure. In November 2001, Admiral James Loy, U.S. Coast Guard Commandant, met with the International Maritime Organization in London to propose sweeping changes to the international shipping industry. His point was clear, "The security challenges are enormous," referring to the world's seaports. Admiral Loy went on to say, "Are [seaports] secure? I am afraid my answer is no."[5]

The U.S. is dependent on liner shipping and intermodal commerce. The security dilemma lies in the fact that there must be a balance between seaport security and the ability to flow commerce. Strict seaport security will insure safety but lose trade dollars to other countries. Loose seaport security will increase trade dollars but risk shutting down the industry with a single terrorist event. This chapter will explore the critical vulnerabilities of U.S. seaports, the government agencies charged with U.S. seaport security, and the security measures in place to protect them. The author's views on the success of seaport security are summarized in the conclusion.

Seaport Vulnerabilities

> *A terrorist act involving weapons of mass destruction at one of these seaports could result in extensive loss of lives, property, and business, affect the operations of harbors and*

> *the transportation infrastructure, and cause extensive environmental damage.*
>
> —F. Amanda Debusk
> Commissioner of the Interagency Commission
> on Crime and Security in U.S. Seaports

U.S. shipping can be characterized as a system composed of seaborne shipping routes, seaports and their critical support infrastructure, and air and rail corridors. In many cases like New York/Jersey City, Los Angeles, or Long Beach the seaports are designed for maximum throughput with the docks, rail, air, highways, and some production facilities in close proximity.[6] The ports themselves can be strategic targets. They are typically in heavily populated areas, hold significant national infrastructure, and are terminals for multiple shipping vessels that can be targets themselves. Also, they are often associated with important economic or national security sectors (Strategic Sealift, Refineries, Airports) that are prime targets for adversaries.[7] The Center for Naval Analysis points out that an attack on a critical port or its adjacent waterways might not only destroy high value assets and shipping, but could cripple the U.S. economy.

In April 1999, President Clinton directed the Secretary of the Treasury, the Attorney General, and the Secretary of Transportation to establish an interagency commission to study the extent of crime and the state of security in U.S. seaports. The Interagency Report on Crime and Security in United States Seaports was released on September 7, 2000. A Presidential news release stated that the report documented the current crime problem in seaports, identified present and projected security threats, and recommended a number of measures aimed at reducing the vulnerability of maritime commerce and its supporting infrastructure. Some specific comments included:

1. U.S. seaports typically allow free access to docks and often to container storage areas.

2. Firearms are generally permitted at dockside.

3. The federal government has no unified plan for monitoring seaport security, although the ports are international gateways similar to the land portals at San Diego, Detroit, and Niagara Falls.

4. The ports receive no federal funding for creating or maintaining basic security systems. And at many ports, even such basic equipment as small boats, cameras, and vessel-tracking devices are lacking.

5. The agencies involved in port operations fail to share information, and they lack the kind of computer communication needed to adequately track vessels and cargo.

6. Lack of information about incoming vessels and their cargo, plus the freedom to enter ports, would allow ships loaded with explosives, jet fuel, or noxious chemicals to ram docks, devastating ports and surrounding areas.[8]

The general lack of security and relaxed policies at U.S. seaports help explain the high incidence of cargo theft and other dockside crime. Estimates of the annual cost of cargo theft run as high as $12 billion.[9] Free access to docks makes it possible for terrorists to retrieve illicit arms and explosives or even to hijack ships. This environment breeds opportunities with serious consequences. Last year in New Orleans, a container, labeled as empty, held oil exploration tools that became radioactive during work in Africa. When Customs officials opened the container in port, their radiation detector alarmed. The inspectors summoned a decontamination team to dispose of the equipment.[10] Another more devastating instance occurred in Mombassa, Kenya. Al Qaeda had shipped arms and bomb-making materials via Osama bin Laden's covertly owned freighters. The materials were subsequently used to blow up the U.S. embassies in Nairobi, Kenya and Dar es Salaam, Tanzania in August 1998.[11] To date, the world economy has enjoyed unencumbered trade at the cost of minimal security standards. Today, the security dilemma pendulum is at the extreme and is swinging back towards tighter security standards.

Commerce and Seaport Security

> *If the U.S. authorities find themselves having to turn off the maritime-container-trade spigot, we will have effectively self-imposed a blockade on our own economy.*
>
> —Stephen Flynn
> Senior Fellow, Council of Foreign Relations
> Testimony to Senate Government Affairs Committee

Security Agencies

Seaport security falls under the cognizance of the U.S. Coast Guard under the Department of Transportation, the U.S. Customs Service under the Department of Treasury, and the individual private or public Port Authorities who operate the seaport. *[Editor's note: With the passage of the Homeland Security Act in November 2002, the U.S. Coast Guard and the U.S. Customs Service now fall under the domain of the Department of Homeland Security.]*

The primary responsibility for defending U.S. ports and coastal areas in peacetime falls to the U.S. Coast Guard.

> The U.S. Coast Guard is responsible for enforcement of federal laws and international treaties and security of U.S. Ports and waterways. This includes but is not limited to: establishment of security zones, supervision over the loading of explosives, control of all vessel traffic within a port, harbor defense, and…law enforcement of limited access areas.[12]

This means that the Coast Guard protects U.S. maritime borders from intrusions and enforces federal law in U.S. waters. Unless overridden by an Executive Order, Posse Comitatus (18 USC 1385) prohibits the use of the Navy and other federal military services from the enforcement of local, state, and federal laws.[13]

The United States Customs Service is the primary enforcement agency protecting the Nation's border. They focus on commerce and are

chartered to enforce the laws of the U.S. pertaining to trade to foster lawful international trade and travel.[14]

The Port Authorities run the day-to-day operations of the seaport. A large port authority has a police force with the full authority of local police. Port Authority Police are responsible for the physical security of the seaport to include law enforcement, fire fighting, and rescue operations.[15]

Security Initiatives

Private Industry

In 1997 private industry, feeling the sting from stolen cargo, initiated a security regime for perspective freight carriers. The Technology Asset Protection Association (TAPA) is an association of high technology companies organized for the purpose of addressing emerging security threats. Members of TAPA include: COMPUSA, Hitachi America Ltd., Dell Computers Corporation, Sears, and Sun Microsystems Inc. As high tech items became smaller and more portable and the security for factories and warehouses became more sophisticated, criminals began to target the products in transit. Dan Purtell, the chairman of TAPA, stated TAPA demanded that shipping companies seal off cargo containers at the time they left overseas factories until their arrival in the United States.[16] Freight Security Requirements (FSR) were established to ensure the safe and secure in-transit storage and warehousing of TAPA assets. The FSR specify the minimum acceptable standards for security throughout the supply chain and the methods to be used in maintaining those standards. Security requirements depend on the value of the material but may include electronic container locks, surveillance cameras, Global Positioning System transmitters, and environmental sensors. Major freight service providers are moving toward TAPA-recognized security standards and are recognizing the inherent value of doing so.[17] For some companies the losses from theft are down 80 percent, yielding much lower insurance rates.[18] This form of shipping security not only protects the cargo, but also reduces the likelihood that a terrorist act could be performed with the container.

Coast Guard

The Coast Guard implemented *Operation Neptune Shield*, the maritime portion of *Operation Noble Eagle* on September 12, 2001. *Operation Neptune Shield* is the Service's largest homeland port security operation since World War II. It's comprised of 55 cutters, 42 aircraft, and hundreds of small boats patrolling 361 ports. Rear Admiral Terry M. Cross, Assistant Commandant for Operations, stated 2765 reservists and auxiliary were recalled to assist in port security operations. The goal of *Operation Neptune* is to allow risk-based decision-making to identify high-risk ports, high-risk vessels approaching our ports, and to strategically place Coast Guard resources where greatest threats lie.[19]

The heart of the Coast Guard port security plan is the Sea Marshal program. The Sea Marshal program was established to assign Coast Guardsmen to ride U.S. and foreign High Interest Vessels (HIV) entering port. A HIV is defined as a vessel over 300 Gross Tons:

1. entering a specific port for the first time.
2. having an intelligence hit on a crewmember.
3. coming from a specified list of ports.
4. defined by the Coast Guard Port Captain as a hazardous material carrier.[20]

Ships entering U.S. ports must now provide 96-hour advance notice of arrival to the U. S. Coast Guard along with crew, passenger, and cargo information. Previously, a 24-hour advance notice of arrival was standard. The longer advanced notice allows the Coast Guard and other U.S. law enforcement agencies time to review the information prior to arrival. The Coast Guard established the National Vessel Movement Center (NVMC) in Martinsburg, West Virginia, to track all vessels over 300 Gross Tons arriving or departing U.S. seaports. Previously, no national tracking system was in place and individual Coast Guard Port Captains of seaports were inconsistently notified.[21]

When a HIV is clear to enter port and within U.S. territorial waters a Sea Marshal and Safety and Security Team (SST) boards. The SSTs are comprised of specially trained Coast Guard law enforcement

officers from the Coast Guard Tactical Law Enforcement Team. The team performs an inspection following the requirements of the International Maritime Organization. Any deficiencies must be corrected prior to entering port. When the Sea Marshal approves final port entry, the SST station themselves in critical locations throughout the ship to insure ship operations are not hampered. The Sea Marshal will station in the pilothouse with SST members in the aft steering station and engine room.[22] A Coast Guard vessel establishes a security area around the ship as it transits through the port. The Sea Marshal and SST debark when the ship is moored. For ships carrying hazardous cargo, a Sea Marshal and a Safety and Security Team may be deployed for the outbound trip.[23]

In larger U.S. ports like Boston, New York/Jersey City, Los Angeles, and Long Beach, Maritime Security Squadrons (MSS) are deployed to assist the Sea Marshals and SSTs.[24] A MSS is comprised of 1 Medium Endurance Cutter (270ft), 2 Patrol Boats (110ft), and 1 Cyclone Class Patrol Craft. The Cyclone Class Patrol Craft are manned and operated by Navy crews with Coast Guard onboard to conduct law enforcement duties.[25]

Commander Chris Doane, director of *Operation Neptune*, Coast Guard Atlantic Command, stated it is important to level the playing field while applying the new security regime. If one Coast Guard Port Captain applies the new rules differently than another, one port may have an unfair trade advantage. These new security practices reinforce interagency cooperation, improve command and control, and use intelligence to screen vessels, cargo, and crew.

Customs

The new strategy of the U.S. Customs Service is to ensure proper security for cargo *before* it enters U.S. seaports. This will lessen the risk that a container will be used to deliver and detonate a weapon of mass destruction prior to entry inspections. Customs is pursuing this "beyond the border" security strategy in four ways; Customs-Trade Partnership Against Terrorism (C-TPAT), International Customs Zones (ICZ), Non-Intrusive Inspection Technology, and cargo-related intelligence databases.[26]

C-TPAT works with industry to improve security from factory to buyer similar to TAPA. Customs recognized that they couldn't provide the highest level of security while allowing the smooth flow of commerce without involving the shippers. In return, Customs would give "fast-track" status to containers meeting C-TPAT requirements.[27]

Customs is also seeking to establish International Customs Zones (ICZ) at major seaports around the world. ICZs would permit the same law enforcement authority to the U.S. Customs Service (power to question, search, and arrest) as if operating on U.S. soil. ICZs are to be established in Canada first followed by other countries with major seaports.[28]

Customs is also pursuing the installation of Non-Intrusive Inspection (NII) technology at foreign "mega-ports" such as Singapore and Rotterdam. In a speech to the Center for Strategic International Studies, U.S. Customs Commissioner Robert Bonner proposed the world's 10 biggest ports x-ray and electronically seal containers bound for the U.S. to circumvent potential terrorist threats. He painted a devastating picture of the end of container trade should a cargo box be used in a nuclear detonation. In return, he said the U.S. would tighten screening of U.S. exports, share technology and intelligence information, and "fast-track" cargo from shippers with airtight supply chains.[29]

The initiatives discussed above may take months or years to establish. In the meantime, Customs must accurately segregate "high-risk" containers warranting greater scrutiny from "low-risk" ones worthy of quick entry. Customs is doing this by screening incoming shipments with their Automated Commercial Environment. By "profiling" containers based on cargo and point of origin, Customs can make an educated guess on the containers that require inspection. The "high-risk" containers are then scanned by the VACIS system.[30] The Vehicle and Cargo Inspection System is a truck-mounted or permanently installed gamma-ray imaging system designed to non-intrusively inspect the contents of trucks, containers, cargo, and passenger vehicles for explosive devices and/or contraband. VACIS can scan two TEUs in one to three minutes. Customs has 29 units already installed at major U.S. seaports.[31]

Conclusion

> *The key is to meet the challenges of the 21st century and yet preserve globalization. To be a flexible border agency capable of working both at and beyond the border in its effort to protect America.*
>
> —U.S. Customs Strategy Memorandum

The U.S. Government finds itself in the unenviable position of balancing seaport security with U.S. economic viability. U.S. Customs Commissioner Robert Bonner hit the mark when saying that no country could afford a terrorist event using the container industry as its vehicle.[32] This scenario should be used as the impetus to make sweeping changes in worldwide shipping security.

Each agency charged with seaport security is making significant changes in their everyday security posture. The U.S. Customs Service has the proper long-term vision for container safeguards. International Customs Zones and the Customs-Trade Partnership Against Terrorism put the first line of defense overseas. Combined with these initiatives, a *worldwide* shipping database similar to the Customs Service's Automated Commercial Environment should be developed. The database would allow all nations to track goods from factory to buyer, anywhere in the world.

The new Coast Guard safeguards do well to defend against unsafe ships and rogue crews. But what the Coast Guard lacks is a worldwide maritime tracking system. Through the International Maritime Organization, the Coast Guard should require all transoceanic ships to have a Global Positioning System transponder similar to the ones used by the Federal Aviation Administration. The transponder would allow continuous tracking of all ocean-going ships and facilitate long-term surveillance. Knowing the seaports visited by a liner would give insight into possible terrorist activity.

Although little information was available on the physical security provided by the Port Authority Police Forces, strict border security and worker identification cards would reduce the number of unauthorized personnel on the docks.

Our seaports and intermodal transportation systems are strategic assets. Although not in the national news, I believe they are receiving the attention necessary to address their vulnerabilities. In the globalized world we live in, our seaport's protection will rely on our trading partners to combat economic terrorism.

Notes

1. Jon S. Helmick, "Intermodal Ports and Liner Shipping: A 21st Century Status Report," *Logistics Spectrum* 35, January-March 2001, 20.

2. Ibid., 2.

3. U.S. Customs Service, Importing and Exporting. On-line, Internet, January 2002, available from http://www.customs.ustreas.gov/impoexpo/impoexpo.htm.

4. Al Baker, John Sullivan, "Port of Entry Now Means Point of Anxiety," *New York Times,* Sunday, 23 December 2001, late edition (east coast), sec. B1.

5. Ibid.

6. Alarik Fritz, et al. *Navy Role in Homeland Defense Against Asymmetric Threats Volume One: Summary Report,* CNA Report CRM D0002158.A2. (Alexandria, Virginia: CNA, September 2001), 24.

7. Alarik Fritz, et al. *Navy Role in Homeland Defense Against Asymmetric Threats Volume Two: Appendices* CNA Report CRM D0002159.A2. (Alexandria, Virginia: CNA, September 2001), 47.

8. August Gribbin, "Seaports Seen as Terrorist Target," *Washington Times*, Monday, 22 January 2002, 1.

9. Adam Aston, John Cady, "Pandora's Cargo Boxes," *Business Week*, 22 October 2001, 48.

10. Al Baker, John Sullivan, "Port of Entry Now Means Point of Anxiety," *New York Times,* Sunday, 23 December 2001, late edition (east coast), sec. B1.

11. August Gribbin, "Seaports Seen as Terrorist Target," *Washington Times*, Monday, 22 January 2002, 1.

12. Quoted in Alarik Fritz, et al. *Navy Role in Homeland Defense Against Asymmetric Threats Volume Two: Appendices* CNA Report CRM D0002159.A2. (Alexandria, Virginia: CNA, September 2001), 18.

13. Ibid., 16.

14. U.S. Customs Service, Importing and Exporting. On-line, Internet, January 2002, available from http://www.customs.ustreas.gov/impoexpo/impoexpo.htm.

15. Port Authority of New York and New Jersey, *Port Commerce*. On-line, Internet, February 2002, available from http://www.panynj.gov/commerce/marframe.HTM.

16. Al Baker, John Sullivan, "Port of Entry Now Means Point of Anxiety," *New York Times,* Sunday, 23 December 2001, late edition (east coast), sec. B1.

17. Technology Asset Protection Association, *The Organization,* on-line, Internet, January 2002, available from http://www.tapaonline.org/organization.htm.

18. Al Baker, John Sullivan, "Port of Entry Now Means Point of Anxiety," *New York Times,* Sunday, 23 December 2001, late edition (east coast), sec. B1.

19. U.S. Coast Guard, Homeland Security. On-line, Internet, January 2002, available from http://www.uscg.mil/overview/Homeland%20Security2.htm.

20. CDR Chris Doane, Director, Homeland Security, U.S. Coast Guard Atlantic Command, interviewed by author, 25 January 2002.

21. U.S. Coast Guard, Homeland Security. On-line, Internet, January 2002, available from http://www.uscg.mil/overview/Homeland%20Security2.htm.

22. CDR Chris Doane, Director, Homeland Security, U.S. Coast Guard Atlantic Command, interviewed by author, 25 January 2002.

23. U.S. Coast Guard, Homeland Security. On-line, Internet, January 2002, available from http://www.uscg.mil/overview/Homeland%20Security2.htm.

24. Ibid.

25. CDR Chris Doane, Director, Homeland Security, U.S. Coast Guard Atlantic Command, interviewed by author, 25 January 2002.

26. U.S. Customs Service, draft memorandum, submitted by: U.S. Customs Service, Treasury Office of Enforcement, subject: Strategic Objectives.

27. U.S. Customs Service, Importing and Exporting. On-line, Internet, January 2002, available from http://www.customs.ustreas.gov/impoexpo/impoexpo.htm.

28. U.S. Customs Service, draft memorandum, submitted by: U.S. Customs Service, Treasury Office of Enforcement, subject: Strategic Objectives.

29. Beth Jinks, "MPA Backs Call to X-Ray Transhipments," *The Shipping Times*, January 2002, n.p., on-line, Internet, 29 January 2002, available from http://business-times.asia1.com.sg/shippingtimes/story/0,2276,34218,00.html?.

30. CDR Chris Doane, Director, Homeland Security, U.S. Coast Guard Atlantic Command, interviewed by author, 25 January 2002.

31. Science Applications International Corporation, *Safety and Security*, on-line, Internet, January 2002, available from http://www.saic.com/products/security/.

32. Beth Jinks, "MPA Backs Call to X-Ray Transhipments," *The Shipping Times*, January 2002, n.p., on-line, Internet, 29 January 2002, available from http://business-times.asia1.com.sg/shippingtimes/story/0,2276,34218,00.html?.

CHAPTER 5

Gulf of Mexico: Offshore Energy Infrastructure at Risk?

Brian S. Norman

Introduction

> *Crude oil must be refined and distributed if it is to be a meaningful source of energy. Power generation plants are worthless if the electricity cannot be transmitted to the factories, office buildings, and households that need it to power equipment and provide lighting and climate control. An adversary intent on disrupting America's reliance on energy need not target oil fields in the Middle East. The infrastructure for providing energy to end-users is concentrated, sophisticated, and largely unprotected. Further, some infrastructure lies offshore in the Gulf of Mexico, on the continental shelf, and within the territories of our North American neighbors.*
>
> *—America Still Unprepared—America Still in Danger*
> Report of an Independent Task Force
> Sponsored by the Council on Foreign Relations[1]

"Dateline 3:17 p.m. CST, July 4, 200X. As millions of Americans prepare to celebrate our country's birth with fireworks and revelry, what appears now to be the largest oil tanker disaster in history is unfolding 18 miles offshore of Port Fourchon, Louisiana. As the *Vahle Viking*, one of the ten largest oil tankers in the world, began offloading oil earlier this afternoon at the Louisiana Offshore Oil Port, a large explosion rocked its hull. Only minutes after the ship incident, a helicopter apparently crashed into the control platform less than a mile

from the stricken ship. Several fireboats, helicopters, and oil-spill responders are now on-scene and the Coast Guard has apparently rescued survivors from the ship and platform complex. The *Vahle Viking*, characterized as a single-hull Ultra Large Crude Carrier, was capable of carrying over 4.2 million barrels of oil. The ship, engulfed in a massive column of fire and smoke, appears to have broken apart. Officials have issued the highest Homeland Defense alert posture."

–Courtesy ZNN News Service.

Obviously, the above situation describes a presently fictitious event. Is such a scenario possible in today's global security environment? Is such a scene probable? What should we do to prevent, protect, or respond to such threats? As recently as November 2003, a major United States oil company was engaged in resolving forcible seizure of oil platforms off the coast of Nigeria.[2] On October 11, 2002, the French tanker Limburg was attacked and significantly damaged by an explosives-filled boat off the coast of Yemen, resulting in a spill of 90,000 barrels of oil into the Gulf of Aden.[3] Will similar actions occur in our own Gulf of Mexico? This chapter focuses on critical energy infrastructure assets within the Gulf of Mexico region and explores their security amidst the challenges of a "post-9/11" world.

What is in the Gulf of Mexico?

The Gulf of Mexico offshore area contains many valuable assets, including vast oil and natural gas production facilities, the Louisiana Offshore Oil Port (LOOP), large lightering zones for shuttling crude oil from larger vessels, major shipping routes and ports, fishing areas, and other maritime resources (tourism, mining, and more). All of these represent significant economic interests and potential targets that could to varying degrees be subject to harm by an enemy. The Gulf of Mexico serves as a major source of seafood and petroleum products, along with its facilities for loading and unloading ships, including bulk cargo.[4] Here are a few facts regarding what is in the Gulf of Mexico and why these resources are of strategic interest.

Oil and Natural Gas Production

Oil and natural gas production in the Gulf staggers the mind in terms of overall scale, support, and economic impact.

- The Louisiana Outer Continental Shelf territory has produced 88.1 percent of the 12.8 billion barrels of crude oil and 82.9 percent of the 139 trillion cubic feet of natural gas extracted from all U.S. Outer Continental Shelf territories from the beginning of time through 2000.[5]
- With more than 30 fields containing reserves of 1 trillion cubic feet or more, our own Gulf of Mexico is among the top 20 geological provinces in the world.[6]
- The Outer Continental Shelf currently provides 25 percent of domestic oil production and 26 percent of the natural gas output.[7]
- The U.S. Gulf provides 1.8 million barrels/day of crude oil and 14 billion cubic feet/day of natural gas.[8]
- Port Fourchon, Louisiana, is a supply base for oil rigs and production platforms in the central Gulf of Mexico; more than 600 offshore platforms are located within a 40-mile radius of Port Fourchon.[9]
- The Gulf of Mexico has the most extensive network of offshore oil and gas pipelines worldwide, stretching over 20,000 miles.[10]
- There are approximately 3,739 offshore oil platforms in the Gulf of Mexico; 3,203 lie off the Louisiana coast.[11]
- Outer Continental Shelf mineral lease revenues are second only to income tax generating revenue for the United States Government.[12]

Louisiana Offshore Oil Port (LOOP)

LOOP will be examined in more detail later in the chapter, but in short, it consists of a large two-platform marine terminal and giant "hoses" connected to three single-point mooring buoys located approximately 18 miles off the Louisiana coast. LOOP enables direct offload of deep draft tankers known as Ultra Large Crude Carriers and Very Large Crude

Carriers along with smaller tankers.[13] Pipelines from the offshore facility connect to an onshore oil storage facility, the Clovelly Dome Storage Terminal. The *LOOP Responder*, a support ship, facilitates port operations and provides security and emergency response capabilities.

- LOOP is the only offshore oil terminal in the United States and receives 15 percent of America's imported crude.[14]
- LOOP is connected to over 50 percent of the United States refinery capacity and has offloaded over 5 billion barrels of foreign crude oil since its inception.[15]
- LOOP transports approximately one million barrels of foreign oil a day and approximately 300,000 barrels of domestic crude from the Gulf outer continental shelf.[16]
- The offshore complex is connected to the Clovelly Dome on-shore storage facility by a 48-inch diameter pipeline.[17]

Lightering Zones

Lightering, simply defined, is the transfer of petroleum cargo at sea from a large tanker to a smaller one. Lightering became a routine practice in the Gulf about 30 years ago, and has increased significantly as strong economic incentives have led to the use of very large tankers for the long hauls from the Persian Gulf and Africa. Lightering is an effective and cost-efficient method of delivering foreign crude oil to the United States, and necessary today because very large tankers are too wide and too deep to enter most American ports.

- More than 25 percent of the 7.5 million barrels of crude oil imported each day is lightered.[18]
- A significant portion of the 6.4 million barrels of crude oil produced domestically is carried by water and lightered.[19]
- Approximately 95 percent of offshore lightering (i.e., outside the territorial sea, which generally extends three miles off the U.S. coastline), by volume, takes place in the Gulf of Mexico.[20]
- Four areas are designated offshore lightering zones in the Gulf.[21]

Shipping Routes and Ports

Our country's economy thrives upon free international trade. Years ago, the legendary Port of New Orleans and the steamboats of the Mississippi River Basin served as the vital trade linkages between America's Heartland and the world. Although the Internet has made the world smaller and we move some goods by air, today the real connections in terms of goods and commodities bought and sold still depend upon ships—ships that export America's goods and grain in exchange for goods and strategic materials from all over the world.

- Seven of the nation's top 10 ports in terms of tonnage or cargo values are located in the Gulf; of the top seven ports in the world, two are in the Gulf.[22]
- Over 50,000 barges and 4,000 ocean-going vessels call at the Port of Louisiana each year, as an example of volume at one of these key ports.[23]
- The Port of Louisiana handles over 245 million tons of cargo a year and is considered the largest tonnage port in the Western Hemisphere.[24]
- Port of Louisiana exports 70 million tons of cargo or more than 15percent of total U.S. exports a year.[25]

Fishing

Fishing and shellfish harvesting are huge businesses in the Gulf. As offshore oil development exploded in the post-World War II years, it appeared to be a dangerous rival to the rich fishing enterprises of the Gulf. However, much to the contrary, a vital symbiotic relationship developed as the oil and gas platforms served as artificial reefs and fostered as much as 50 times the amount of fish found in nearby mud-bottomed waters. Today, many environmental and fishing interests have turned from condemnation of the oil and gas platforms towards a dependence upon having these mini-reefs available to cultivate rich colonies of fish.

- Eighty-five percent of Louisiana fishing trips involve fishing around the huge artificial reefs created by oil platforms.[26]

- Annually, more than four million people take over 24 million sport-fishing trips into the Gulf waters.[27]
- The Gulf provides 40 percent of the entire United States commercial fisheries harvest.[28]
- About 98 percent of Gulf fish species depend on wetlands during some stage of their life cycle.[29]
- The Gulf's commercial fisheries industry produced 1.8 billion pounds of fish and shellfish in 2000, with a dockside value of $991.4 million.[30]
- Gulf landings of shrimp led the nation in 2000 with 288 million pounds, about 80 percent of the nation's total; Louisiana led all Gulf states.[31]
- The Gulf led in production of oysters with 20.7 million pounds of meats in 2000, 60 percent of the national total, valued at $44 million.[32]

Other Marine Resources

The Gulf ecosystem has been a resilient and vital treasure for our nation. Tourism, mining, and estuary habitat for a great deal of wildlife and marine life during crucial life cycle stages make the Gulf extremely valuable in ways beyond the scope of this chapter.

- Seventy-five percent of the migratory waterfowl in the United States utilize Gulf wetlands[33]
- The Gulf supports a tourist industry encompassing thousands of businesses and tens of thousands of jobs worth over $20 billion annually.[34]
- The largest population of bottlenose dolphins in the world is located in the Gulf, of which the Mississippi Sound sees the highest concentration.[35]

Trends

Several significant trends in offshore reliance and development emerge today. Three of the largest trends are: first, continued reliance on offshore oil port facilities; second, a steady increase in size and utilization of supertankers; and third, expansion of Gulf oil and gas production, notably through deepwater projects, to include the significant costs and reliance upon floating deepwater operations.

North America relies upon the Gulf offshore port facilities for importing crude oil. When LOOP opened, then and still our only offshore deepwater port, it provided our country the means to directly offload giant tankers that were too large to enter many U.S. ports. The Deepwater Ports Act of 1974 provided the legal and jurisdictional framework to proceed with developing such offshore facilities to accommodate the largest of supertankers. Lightering operations continue by necessity, but LOOP provides a much more efficient and effective means for offloading crude. Today, major oil companies are researching the feasibility of creating other deepwater ports. One proposal is to build a deepwater port much like LOOP off the coast of Texas.

As the second trend, supertankers have increased in size and our reliance on supertankers for importing crude has steadily grown. In the decades around World War II, oil tankers were small enough to travel directly from port to port. In years hence, the term "supertanker" was coined to describe any tanker of great size and carrying capacity, usually in excess of 100,000 deadweight tons.[36] Realizing the efficiency and economy of using larger tankers, oil producers and ship builders continued building larger tankers that would double what early supertankers could carry—Very Large Crude Carriers—with a gross deadweight tonnage in the range of between 200-400,000 tons.[37] Today, a generation of Ultra Large Crude Carriers patrol the oil routes. The Ultra Large Crude Carriers are supertankers of over 400,000 deadweight tons. One of the larger examples would weigh in at 533,000 deadweight tones, with a length of 1,360 feet, width of 208 feet, and drawing 93 feet of water. They are longer than a typical U.S. aircraft carrier. Viewed another way, Ultra Large Crude Carriers are longer than the Empire State Building is tall!

One more trend affecting the region: oil and gas developers are actively expanding their reach into the Gulf. And, thanks to new, costly technology, they are heading into water previously too deep to reach.

Deepwater oil production increased by almost 1,200 percent and deepwater gas production by about 2,850 percent during the period 1985 to 2001.[38] As of September 2001, a Minerals Management Service official stated there are 119 new exploration wells being drilled in Gulf waters, with 47 of those in water depths exceeding 1,000 feet.[39] Through 2006, it is anticipated that the oil and gas industry will invest $100 billion in deepwater exploration and development alone, with most of the activity expected in Brazil, West Africa, and the U.S. Gulf.[40]

There has been a 14.8 percent annual growth rate between 1998 and 2001 regarding the market for *floating* production facilities.[41] The basic floating structures include Tension Leg Platforms (TLP), converted or new built tankers used as floating production vessels or barges, semi-submersible production units, and spar towers. These platforms have been growing in popularity, particularly for development of the Outer Continental Shelf deepwater.[42] The demand for offshore oil and gas is set to grow, with large companies focusing on fields in deep waters, while many other smaller players are coming back to smaller-production fields closer to the coast that have nearly become ignored.[43]

These trends are interesting in several ways, including the effect of moving U.S. interests further offshore into deeper waters, along with the incredible expense of platforms and the challenges presented in supporting and protecting this vast array of valuable complexes.

Charting the Course

Upon examining the above facts regarding the tremendous strategic importance of the Gulf of Mexico and its value in terms of natural resources, commerce, and transportation, it should be clear that critical infrastructure located offshore certainly merits some protection as our nation struggles with establishing Homeland Security priorities and means. Given this chapter's review of valuable assets in the Gulf, we turn next to examine information regarding two example systems that comprise our offshore energy infrastructure—LOOP and a "flagship" deepwater platform named Mars.[44] This examination will provide a closer look into how open sources can significantly illuminate these very valuable assets, and allow one to appreciate these structures before we analyze hard questions involving their security.

Studying Two Offshore System Examples

> *A vast amount of competitive intelligence is legally and openly available from commercial databases, trade and scientific journals, corporate publications, U.S. Government sources, web sites, and computer bulletin boards…the worldwide web was not designed with security in mind, and unencrypted information is at high risk of compromise to any interested adversary or competitor.*
>
> —Texas A&M University Security Guide[45]

Before we analyze potential risks and security concerns, let's examine the ease in which data may be obtained on Gulf energy infrastructure, then focus specifically on two of the most valuable types of offshore resources in the Gulf of Mexico today. Understanding the systems and processes involved in these offshore complexes is vital to both those that wish to protect them and those who seek to do them harm. Furthermore, access to such information and understanding is vital for those who make their livelihood in vocations involving use of the Gulf. Rather than presenting an engineering analysis and exact "Global Positioning System" (GPS) coordinates, the intent here is to provide a simple overview of two types of the highest-value offshore structures, so we can properly appreciate the issues associated with protecting them.

Information is Easy to Find

Globalization and the creation of free trade, free markets, and "information super highways" are hallmarks of our free, democratic society and allow an explosion of positive idea sharing and innovation, but also provide would-be enemies insights into understanding our nation's critical energy infrastructure for their own schemes. Whether an innocently curious student, an oil and gas production professional, a mariner, a noble-minded security specialist, or a coldly calculating terrorist, one can find a great deal of open source information about offshore operations via the internet, libraries, trade sources, from the U.S. Government, and for sale. During the course of research for this chapter, the author was provided little via requests from official sources, ostensibly

in the name of infrastructure protection, but through simple searches was able to discover:

- Names and exact GPS references for thousands of offshore structures, including specifics regarding if they were manned or unmanned and if they had helicopter platforms.
- Free highly detailed navigational maps of the Gulf.
- Free services to chart waypoints and courses in the Gulf.
- Detailed descriptions of *specific* platforms, the systems and engineering considerations involved, and their critical subsystems and linkages.
- Schematics, diagrams, and consideration for various structures.
- Blueprint drawings and performance data on the *LOOP Responder*, the primary vessel providing dedicated on-site support to the LOOP Terminal.
- More detailed information on much of the above for sale at minimal cost.

Many of these items are necessary and vital to commercial and sport fishermen, merchant vessel operators, and oil and gas producers, thus the denial of access to such information would be counterproductive and harmful in many ways. Navigating in Gulf waters requires a serious understanding of the dangers and protocols detailed in reams of charts and regulatory guidance. Still, some of the information likely should not be available—that issue is beyond the scope of this effort, but serves as a consideration for oil and gas producers whose interests are at risk and the government entities who must help protect them from risk. As an interesting note along those lines, it appears the state of Louisiana has done some selective purging of their free on-line state map library—in placeholders where one could previously access several detailed offshore oil infrastructure maps. Even so, the bottom line is this: if an enemy desires to gain an understanding of the systems, what they are, what they do, and where they are located—information is readily available. The following paragraphs illuminate an understanding of LOOP and Mars via "open source" information.

LOOP

Figure 5.1 LOOP Marine Terminal

Source: Louisiana Offshore Oil Port Web Site,

Louisiana Offshore Oil Port (LOOP) LLC is a Limited Liability Company whose primary business is offloading foreign crude oil from tankers, storing crude oil, and transporting crude oil via connecting pipelines to refineries throughout the Gulf Coast and Midwest. LOOP is also the storage and terminalling facility for the Mars pipeline system and its supply of offshore Gulf of Mexico crude oil.[46] The author had never heard of LOOP prior to an Air War College elective study trip to New Orleans; it is entirely possible that many Americans are unfamiliar with it as well. Five oil companies came together to build and operate LOOP, and congressional actions supported selection of Louisiana to host the nation's first oil super-port.[47] About 18 miles off Louisiana's coast, two immense steel platforms serve as the nucleus of a complex operation through which flows 12-17 percent of the crude oil imported into the United States.[48] LOOP began operation in 1981 and is the only U.S. port capable of offloading deep draft tankers of the Ultra Large Crude Carrier and Very Large Crude Carrier class.[49] Before LOOP, supertanker operators only had the option of lightering, whereby they transferred their cargo into smaller tankers that could be accommodated by our Gulf ports.[50] The port consists of three single-point mooring buoys used for the offloading of crude tankers and a marine terminal consisting of a two-level pumping platform and a three-level control platform.[51] A 48-inch diameter pipeline connects LOOP's onshore oil storage and distribution facility, Clovelly Dome, to the offshore system.[52]

Offshore Platform Complex. The control platform consists of living quarters for 38 people, galley, a control room, a vessel traffic control station, offices, a helicopter pad, and life support equipment.[53] A 150-foot personnel bridge connects this platform to the pumping platform, which contains four 7,000 horsepower pumps, power generators, meters, and lab

facilities.[54] The pumps on this platform are capable of pumping crude oil at a rate of 100,000 barrels an hour.[55] This information plus another reference indicate that the oil must actually travel onto the terminal and through pumps on its way to the shore facility. At LOOP's marine terminal, vessel traffic controllers maintain a 24-hour watch over all vessel traffic in the LOOP controlled safety zone and stay in radio communication with the tankers.[56] The platform complex is situated in approximately 110 feet of water in order to accommodate Ultra Large Crude Carriers, which can draw upwards of 90 feet of draft when fully loaded.[57]

Figure 5.2 Single-Point Mooring

Source: Louisiana Offshore Oil Port Web Site, http://www.loopllc.com/f1.htm.

Single-Point Moorings. Three single-point mooring buoys are stationed approximately 1.5 miles (8,000 feet) from the platforms.[58] Giant hoses costing $2.5 million connect LOOP's pipeline to the ships to unload the cargo.[59]

Pipeline. An approximately 18 nautical mile long 48-inch pipeline connects the offshore platforms to the facilities on-shore. The line actually comes ashore at Fourchon, where four 6,000 horsepower pumps at a booster station pump the oil 23 miles farther to the north to the Clovelly facility.[60] Four pipelines connect the Clovelly onshore storage

facility to refineries in Louisiana and along the Gulf coast (Texas).[61] LOOP is also connected via a 53-mile, 48-inch pipeline to CAPLINE, a pipeline that delivers crude oil to Midwest refineries and through other connections, can take oil as far as Canada.[62]

The *LOOP Responder* and other support vessels. The *LOOP Responder* is a 155-foot emergency response vessel designed specifically to serve LOOP offshore port operations. This tractor tug can provide some assistance in positioning a tanker vessel and responding to oil spills and fires. Its two fire pumps can dispense 15,000 gallons per minute of water and foam in a spray up to 250 feet away. The author was able to discover schematics and performance data of the *LOOP Responder* on-line.[63] In addition to the *LOOP Responder*, the *LOOP Lifter*, a 200-foot maintenance vessel that has a 48-mile radar, supports the complex. These larger vessels share in the company of two 85-foot mooring launches, the *LOOP Line* and *LOOP Loader*, also maintained at the LOOP Marine Terminal to assist in operation of the port.[64]

Fourchon. Although on the Louisiana shore, Fourchon is a vital hub to not only LOOP, but also other Gulf offshore delivery and production operations. LOOP's offshore pipeline routes through booster stations located at Fourchon and on to storage and refinery facilities.

Figure 5.3 Clovelly Dome Storage Terminal

Source: Louisiana Offshore Oil Port Web Site, http://www.loopllc.com/f1.htm.

Clovelly Dome. Oil from the offshore system enters Clovelly Dome Storage Terminal via a 48-inch pipeline (via Fourchon).[65] Clovelly dedicates eight underground caverns leached out of a naturally occurring salt dome to the LOOP project.[66] The caverns are capable of storing approximately 48 million barrels of crude oil (the U.S. strategic oil reserve, a separate entity entirely, can store over 700 million barrels of oil in several locations, one of which is not far away from Clovelly in Louisiana).[67] These eight caverns at Clovelly, plus a ninth dedicated to support Mars, are each approximately 200 feet wide by 1,400 feet deep. Five lines connect to each cavern to pump oil or brine solution in and out of them.[68] This brine solution is actually heavier than the oil and is used as a displacement system to push crude oil back out of the caverns towards pipelines or processing centers as supply and demand dictates. A brine storage unit, basically a big man-made "heavy salt lake," is also part of the Clovelly facility.

Galliano. The LOOP control center is at Galliano, three miles west of Clovelly. Engineers start and stop pumps, select meters, and open and close valves remotely from this control center to direct the flow of oil from tankers through pumping stations and into caverns and on to the five pipelines that lead out of Clovelly.[69] Oil movement controllers from Galliano must stay in constant contact with the mooring masters on tankers that are transferring oil from tankers at the single-point moorings.[70]

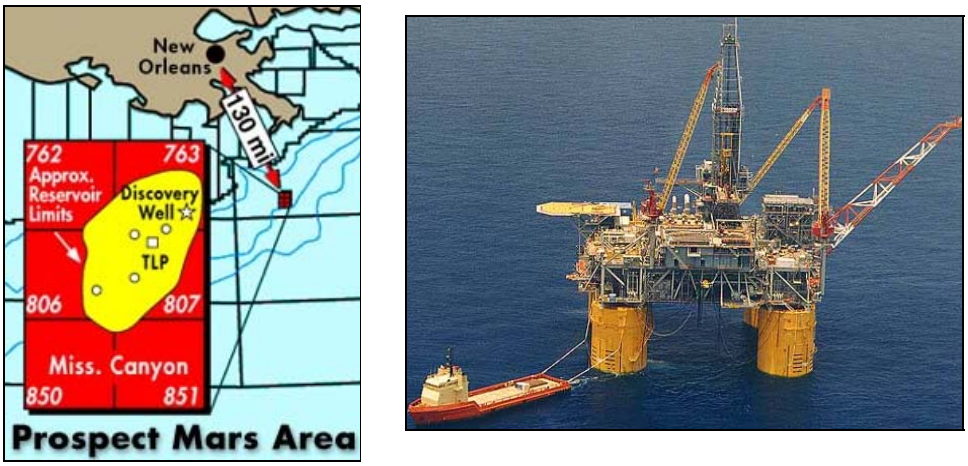
The LOOP system, including onshore and offshore, clearly constitutes a very valuable strategic asset for our country. Although other companies have been interested in developing more deepwater ports, the LOOP Port presently maintains its position as our only one. Of the nearly 4,000 other offshore platforms in the Gulf, perhaps some of the most interesting and valuable production facilities are the new and expensive deepwater platforms, an example of which the chapter will now focus.

Mars Deepwater Platform and the West Delta Complex

Some of the most successful and expensive operations in the Gulf today are the growing number of deepwater hubs, fixed platforms near the deepwater margin and giant Tension Leg Platforms (TLP) which house facilities for processing and transporting not just their own large production, but also oil and gas from producers throughout the region. Shell Oil Company currently owns a controlling interest in the two largest, Bullwinkle and Mars.[71] According to Coast Guard District Eight, at least 12

major deepwater production platforms currently reside in the Gulf. As the name implies, these facilities inhabit deepwater regions of the Gulf, a relatively new technological trend taking oil production beyond normal on-scene coordinator areas. These deepwater complexes include developments named Diana-Hoover, Auger, Joliet, Typhoon, Brutus, Genesis, Allegheny, Morpeth and Prince, Mars and Ursa, Marlin and Ran-Powell, and Neptune. For the purpose of examining deepwater facilities, this chapter details the Mars TLP and the supporting (non-deepwater) West Delta Complex.

Figure 5.4 Mars Prospect Area and Tension Leg Platform



Source: Shell Exploration & Production Company (SEPCo) http://www.shellus.com/sepco/where/offshore/mars.htm. Offshore Technology, The Website for the Offshore Oil & Gas Industry http://www.offshore-technology.com/projects/mars/mars1.html.

Mars TLP. The Mars TLP was installed in May 1996 in water 2,940 feet deep, with the platform itself 3,250 feet above the seafloor.[72] Mars was Shell's second "super" deepwater project after the successful Auger system launched a few years earlier. The development cost for phase I of this project was over $1 billion.[73] Production began July 8, 1996, and today Mars can send about 300,000 barrels of oil a day and deliver approximately 220 million cubic feet of natural gas per day to shore facilities via pipeline systems. An 18- and 24-inch diameter pipeline transports oil 116 miles to Clovelly, Louisiana, and gas travels 55 miles via a 14-inch pipeline to West Delta 143. Mars is designed to simultaneously withstand hurricane force

waves of 71 feet and winds of 140 miles per hour.[74] GPS waypoint detail for Mars and other offshore structures is available on-line, including information regarding heliport and manning information, year placed, and owner, along with supporting links to printable nautical charts.[75]

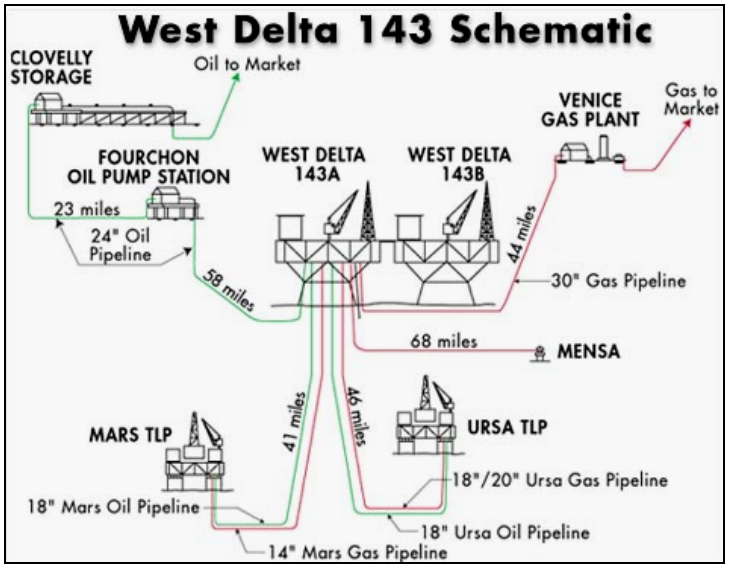
Hull. The hull is comprised of four circular steel columns, 66.5 feet in diameter and 162 feet high, and four pontoons 27 feet wide and 24 feet high, which connect the bottoms of the four columns.[76]

Deck. The Mars deck is composed of five modules: well bay, quarters, process, power and drilling. The deck is an open truss framing design, 245 feet by 245 feet by 45 feet high.[77]

Tendons/Piles. Mars has 12 tendons, three per corner, each with a diameter of 28 inches and a wall thickness of 1.2 inches.[78] Each tendon is approximately 2,852 feet long and connected directly to piles on the sea floor.[79] The drilling and accommodation module houses at least 106 people, plus a control room and an emergency response center.[80]

Drilling and Production Topsides. Mars has 24 well slots, and the sub-sea wells are tied back to the TLP. The development possesses complete separation, dehydration and treatment facilities.

Figure 5.5 West Delta Platform



Source: SEPCo—News—2000-07-Deepwater Hubs: A New View of Gulf Operations." On-line. Internet. Available from http://www.shellus.com/sepco/news/ 2000/07_hubs.htm.

Several of Shell's shallow water platforms also act as hosts for deepwater sub-sea developments. One example, West Delta 143, comprised of two shallow water platforms (143A and 143B), connects to the deepwater Mars, Mensa and Ursa complexes and in turn pumps oil and natural gas onto gas and oil centers in two separate areas. West Delta assists Mars' high production rates with its pipeline pumps, gas compressors, and slug catchers.[81]

Clearly, offshore assets are expensive and valuable. As a matter of necessity to marine shipping and fishing operations, a great deal of information regarding offshore structures can be obtained freely or for a relatively small investment. Understanding offshore operations also provides a starting point for those who wish to protect them or bring them harm. Some offshore assets, such as extremely large tankers, the LOOP complex, and the twelve modern deepwater hubs may require greater security consideration. Would anyone actually target offshore infrastructure? How? Is anyone doing anything to secure these expensive developments? The next sections provide insight into these questions.

Why Would Anyone Attack Gulf Interests?

> *The focus on economic targets is consistent with Al Qaeda's stated ideological goals and longstanding strategy. The September 11 attacks and commentary on these attacks by bin Laden and others indicate how central economic targets are to this strategy: The group's leaders have said that they aim to undermine what they see as the backbone of U.S. power, the economy. Our adversary is trying to portray American influence as based on economic might and therefore seeks to strike an economic target prominent enough for economic and symbolic reasons that it would have immediate resonance around the world.*
>
> —FBI Press Release, October 9, 2002[82]

Purposes and Impacts of Terrorist or Enemy Action

The era in which vast oceans coupled with our naval and air dominance protected American soil has ended. Today, the lethality of weapons, to include weapons of mass destruction and their relative proliferation, presents a broad threat spectrum ranging from individual acts of terror to traditional state enemies capable of delivering severe blows to our population and economy. In the fall of 2002, just two criminals on a deadly shooting spree with a single assault rifle in the National Capitol Region caused a great deal of trauma and expenditure of national resources.

Since before World War II, the United States Air Force bombing theories have targeted the destruction of enemy energy infrastructure—from the "industrial web concept" to "Warden's five rings."[83] Thus, in World War II, the Allies bombed oil production, refinement, storage, and distribution centers, and in Desert Storm, the Coalition hit some related target sets in Iraq, with the intent to deny enemy war machines and economic power and to induce "multiple cascading effects."[84] Today, even an enemy too poor to strike with precision munitions at a standoff distance can choose alternative "lower budget" means to destroy, deny, or disrupt American energy sources. Should we assume that modern enemies or terrorists are too naïve to understand these principles?

Whether a state or non-state actor chooses to cause harm, their intended or actual attack results will usually involve at least four areas, each to varying degrees: physical destruction and loss of life; economic and financial loss, public concern and disruption; and environmental impacts. These categories are not necessarily mutually exclusive, and the effects can cascade across the artificial boundaries of such a model. Consequences can further be thought of as ranging across a spectrum of effect within each category—from *negligible* to *marginal* to *critical* to *catastrophic*. For example, from a national perspective, the loss of 14 individuals may be tragic yet produce negligible results in the physical destruction and loss of life category, while a widespread smallpox outbreak could result in catastrophic losses. An open-minded assessment of these factors, using another scale of probability of occurrence, from *improbable*, to *remote*, to *occasional*, to *probable*, to *frequent* can add another dimension towards assessing any potential attack scenarios. Probability of occurrence can be assessed given the relative access to

supporting resources, the complexity involved, and past inclinations to use a similar approach. While this section focuses on the four general areas of "impacts and outcomes" of any attack, the next section details more thought on potential means and modes of attack.

Physical Destruction and Loss of Life

Sheer physical destruction and loss of life can satisfy enemy intentions. Note the words of Osama bin Laden during a taped interview after 9/11: "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 that would be hit would be three or four floors. I was the most optimistic of them all. (...Inaudible...) due 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."[85] War theorists including Giulio Douhet have believed that the swifter and more severely the fight is delivered to the enemy, including its civilian population, the quicker they may capitulate, although Douhet's idea of striking civilians has been criticized as "war against the unarmed."[86] Douhet's thoughts regarding taking a fight to the population, including use of weapons of mass destruction, merit a fresh reading for those of us who seek to protect our nation from a "Douhet-like" enemy today.

In today's world of precision-guided munitions and standoff weapons, America has seemed increasingly reluctant to both suffer combat manpower losses or to inflict "collateral damage" upon non-combatants. Potential enemies have much less discretion, but are perceptive to manipulate American sensitivities as much as possible. The bombing of a U.S. Marine compound in Beirut provided the catalyst for a U.S. withdrawal from Lebanon. The "Black Hawk Down" incident in Somalia led to an exit from operations there. In Kosovo, President Clinton seemed so attuned to potential risks to U.S. ground forces that he chose airpower as the primary military means to pressure Milosevic. The loss of over 3,000 innocent civilians during September 2001 prompted strong military action from the U.S., yet still tempered with a concern for force protection.

If enemies continue to seek visible destruction of American physical assets and lives, opportunities abound. Terrorists have clearly shown an inclination to wreak greater destruction and take lives without concern for

their own fate. In Israel, young men and women strap bombs to their bodies and sacrifice their own lives "for the cause." Offshore facilities seldom offer clusters of more than 200 people in a given area, but those lives are still viewed as precious in the eyes of other Americans. Offshore facilities, helicopters, support ships, tankers, and fishing boats are largely undefended. Depending on how close to shore or other infrastructure, these assets may be within the viewing of others or relatively remote and isolated.

Economic and Financial Loss

For many contemporary terrorists, including Osama bin Laden and Al Qaeda, the targets are our economy and our way of life. In his taped messages, bin Laden has referred to the U.S. economy as the "key pillar of the enemy" and has called for strikes against critical sectors of our economy "through all possible means." Kenneth Juster, Under Secretary of Commerce, Bureau of Industry and Security, said, "there is now specific evidence that Al Qaeda has obtained detailed information about U.S. power plants, dams, and other key infrastructure assets."[87]

New deepwater platforms like Mars cost hundreds of millions, and sometimes a few billion of dollars. Losing a tanker or major platform can mean a significant financial loss on top of money lost to interrupted production.[88] When the 40-story, Brazilian-owned Petronas P-36 oil platform, then the largest platform in the world, sank into the Atlantic Ocean in March 2001, the $500 million loss caused a "global insurance problem," even before the destruction of the Twin Towers precipitated a similar insurance dilemma on-shore for large buildings.[89]

For enemies seeking to maximize loss in terms of physical, human, and economic devastation, it might appear that America should prioritize its defensive efforts on targets that initially appear much more lucrative than offshore facilities. Attacks upon large cities, financial and industrial centers, major sporting events, nuclear facilities, dams, or many other precious assets located upon the continent certainly merit high consideration in developing Homeland Security strategies. In contrast, a single strike against one of the thousands of oil and gas platforms may not yield as powerful a result as other options available to an aggressor. Despite this fact, consider the economic ramifications if the LOOP complex, an ultra-large tanker, or a large deepwater platform were

successfully stricken by an explosives-laden fishing vessel. Recall the serious damage inflicted upon the U.S.S. *Cole* in 2000 during a similar scenario and imagine the potential economic impact to every American at the gas pump should such an asset be destroyed. Furthermore, consider the scenario of an oil tanker, container vessel, or cruise ship being attacked and sunk in a critical waterway such as the main channel of the Mississippi near the heart of New Orleans: critical economic linkages could be disrupted for months. Even worse, consider a synchronized maritime attack occurring upon several ports, for example, Baltimore Harbor, New York, Los Angeles, and New Orleans. Simultaneous attacks could cripple our port capacity, disrupting shipping and production for a significant time. In New Orleans, even after the toxic fires from such a strike were extinguished, the hulking wreckage could cut off access to one of the nation's largest clusters of refineries, cause chaos and panic within adjacent large civilian populations, disrupt huge import and export businesses, decimate Gulf fishing, and devastate the stock market.[90] Stock market reaction to any of these scenarios could cause massive losses, trigger a recession, or otherwise seriously undermine our financial and economic structures.

Public Concern and Disruption

Isolated or major attacks against critical infrastructures could be used to create panic and decrease public confidence in government or the critical infrastructure itself.[91] Attacks to Gulf infrastructure would certainly imprint the psyche of Americans, especially if the result of these attacks was visible along the coast. Imagine huge plumes of dark smoke, oil along miles of shoreline, or dramatic film footage of some offshore event. The public outcry regarding the 1989 *Exxon Valdez* incident in Alaska was significant; spilling multiple times more oil in our warm Gulf waters would certainly generate a large outcry.

In November 2002, the tanker Prestige broke apart and sank off the coast of Spain. The Prestige sinking has impacted thousands of families who for generations have depended upon fishing and tourism for a livelihood along the coast of Spain, Portugal, and France.[92] On a contrary note, crimes or attacks against offshore platforms, particularly those "over the horizon" from our shoreline, may be much less visible in

the public's eye than a major negative event striking directly at on-shore infrastructure.

Environmental Impacts

The 1989 *Exxon Valdez* oil spill in Alaska provides several lessons regarding what can be lost to the environment during a crude oil spill, whether the causes are intentional or unintentional. Some experts would assert that in general, even with the best technology and assistance, large spills cannot be contained, oil cannot be recovered effectively from water or shorelines, ecological damage can be extreme and long-lasting, and once such ecological damage occurs, it is not easily correctable.[93] The *Exxon Valdez* disaster, although not even ranked in the world's top ten oil spills by volume, represented a symbolic, defining moment for the nation and the oil industry in the same manner that Chernobyl highlighted the world nuclear energy industry. The *Exxon Valdez* lost around 40,000 tons of oil (compare that to a Ultra Large Crude Carrier carrying 400,000 tons today) as 8 of 11 cargo tanks ruptured upon grounding near the waters of Prince William Sound. Over 1,500 miles of shoreline were oiled to a varying degree, the industry spent over $2 billion in attempts to mitigate the spill, and fish and wildlife populations collapsed for generations.

"Eco-terror" is not beyond the mind and capability of potential enemies. During the 1991 Gulf War, Saddam Hussein's forces deliberately discharged crude oil into the Persian Gulf, causing a spill that could be seen from space and endangering desalinization plants located miles away on the Saudi coastline.[94] In addition, the Iraqi army was trained on detailed procedures to destroy and disable Kuwaiti production facilities, thereby damaging and setting fire to a majority of Kuwait's wells. Again, during the 2003 Gulf War, Iraqi forces attempted similar actions to its crude oil pumping platform in the Persian Gulf.

In April 1998, the United States General Accounting Office released a report titled Threat and Risk Assessment Can Help Prioritize and Target Program Investments.[95] Of special note in regard to defending offshore infrastructure, the report highlighted a multinational oil company's five-step qualitative risk-assessment process.[96] Using the above categories of impact, level of severity, and anticipated frequency or potential, oil and gas developers, oil tanker owners, and the

government can proactively assess their risks and vulnerabilities, and many have already done so. These players should also clearly understand how attacks could be carried out, in order to build specific scenarios that can help even more to prepare ways we can prevent, protect, and recover from such events. The next section analyzes some potential answers to the "how" and ends with a few reflections on offshore infrastructure vulnerability.

Modes of Attack and Relative Vulnerability

> *Al Qaeda may be targeting oil and gas infrastructure for a spectacular attack within the United States…The highest priority targets remain within aviation, petroleum, and nuclear sectors…the next attack could be more conventional, utilizing explosives and low-technology platforms such as truck bombs, commercial or private aircraft, small watercraft or explosives easily concealed and planted by terrorist operatives.*
>
> —FBI warnings as outlined in *Oil and Gas Journal*[97]

Offshore Infrastructure faces at least four basic mediums of threat: air, surface, sub-surface (underwater) and cyber (computer network). To add another dimension to the means of threat, actions could be taken through internal agents or external agents or a combination of both. That is, oil and gas developers must contend with people on their payrolls and providing support to their offshore infrastructure—not just "bad guys" trying to attack from the outside. Counter-terror and counter-attack strategies depend not only upon understanding why and what enemies seek to attack, but how attacks could be carried out, what weapons can be employed, and what tactics and methods they may use. Examining a potential aggressor's will and resources provides valuable insight into their true capability to inflict damage to U.S. interests. For example, China may have the resources to carry out a comprehensive cyber attack on our nation today, but may not presently have the will or inclination to do so. On the other hand, Al Qaeda may have the will to carry out a cyber

attack, but may not possess anywhere near the resources to launch such a sustained and widespread attack.

Government and industry experts need to define and flesh out scenarios regarding modes of attacking offshore structures, historical and potential techniques for strike, and the resources available to state actors, rogue states, and terrorists in order to better understand security requirements.

Modes of Attack

Aerial Attack

There are abundant scenarios whereby aerial attack could be attempted by terrorists or state-sponsored aggressors. Given the demonstrated ability of terrorists to use large commercial aircraft as deadly and powerful weapons in the 9/11 events, one should not rule out that such an approach would not be tried again. A fleet of over 500 commercial helicopters services the thousands of Gulf platforms in a constant hum of activity in the airspace block from sea level to 5,000-feet. This flying beyond the coastal shores operates almost exclusively under visual flight rules and relies on "seeing and being seen." Radar coverage is minimal in this low-altitude environment and detailed flight plans are the exception, therefore detailed tracking by the Federal Aviation Administration is sketchy at best.[98] To provide an idea of the scope of these daily over water shuttles of personnel and equipment, a 2000 Helicopter Safety Advisory Conference report records over 1.4 *million* flights annually, with nearly 600 helicopters making about 2,429 flights per aircraft, with an average flight duration of 16 minutes and only nine reported accidents.[99]

Would the U.S. or another state at war ever consider striking enemy petroleum platforms? Do we think potential enemies would think of attacking ours? In the 1980s, Iraq and Iran exchanged blows on their respective energy infrastructure. On 17 and 18 January 1991, the guided-missile frigate U.S.S. *Nicholas* (FFG-47) and her helicopters scouted the Dorra oil field, about 40 miles from Iraqi-occupied Kuwait. These missions confirmed that Iraqi troops had been placed on the structures. Flying low and without visible lights on the night of 18 January, the helicopters launched a barrage of guided rockets on anti-aircraft positions

placed on the platforms.[100] Thus, not only have potential aggressors performed aerial operations on offshore oil infrastructure—the United States has done the same. Today, given aggressor access to funding, skilled operators, or use of hijacking techniques, it is conceivable for them to consider coordinated aerial attack employing some of the following modes:

- Light or commercial plane "kamikaze-style" suicide attack of a structure.
- Helicopter delivery of a load of explosives or iron bombs, crashing into a ship or structure.
- Helicopter assault of platforms, in broad daylight or at night using night vision systems, either through rockets and weaponry or actual boarding teams.
- Seizure or temporary use of offshore platforms, especially unmanned ones, as a base of operations or as "gas and go" heliport staging links. Many offshore platforms have helipads, and many of these possess aviation refueling capabilities.
- Air-launched munitions including anti-ship or anti-tank missiles such as Exocets, Hellfire, Stinger, and similar U.S. or foreign systems.
- Remotely piloted unmanned aerial vehicle observation or attack.
- Cruise missile attack.

Surface Attack

Given the ease of obtaining a vessel and the historical propensity for enemies to employ them to do harm, surface attack is probably the simplest means to inflict serious harm to the Gulf's multi-billion dollar infrastructure. Early in the war against Al Qaeda, many media reports estimated that bin Laden possessed a terrorist fleet of approximately 40 craft of various tonnages. Given the prevalence of fishing and pleasure boats in the Gulf, one could easily purchase or commandeer a boat (or several) for operations against the LOOP or other offshore target. High speed "cigarette" or racing boats are available today that can outrun many

other vessels and could be loaded with explosives, run well into an exclusion zone without being intercepted, and rammed into a structure to create serious damage. Commercial fishing boats are designed to carry a great deal of ice and their cargo of fish; this large amount of cargo space could be used to instead hide a vast explosive charge.

Piracy, although rare in the Gulf, is another practice that is almost commonplace in several other parts of the world and should not be ruled out. Over 330 maritime piracy acts were recorded worldwide in 2001 with many Asian areas greatly affected, including the legendary Straits of Malacca, although some acts were carried out in the Mediterranean and Caribbean.[101] The fact that ships today can be pirated or hijacked by "rogue crews" or insiders engaged in espionage is real. Many ships sail under "flags of convenience" with crews of dubious credentials and uncertain nationality, compounding the problem and making it easier to create undesired substitutions that could place dangerous people on board seagoing vessels.

Perhaps one of the simplest and greatest surface threats offshore continues to be remotely directed or manned suicide boats loaded with high explosives. Any tanker struck with the explosive power that the U.S.S. *Cole* endured would not likely fare as well, but instead sink with great loss. The armor-plated warship sustained and yet survived a 40-foot by 40-foot waterline hole, losing 17 crewmen, with another 35 injured.[102] On October 7, 2002, the French oil tanker Limburg was attacked near Yemen via a speedboat laden with high explosives.[103]

In past years, people other than oil and gas company workers have sought to and successfully occupied offshore platforms. Environmental concerns have prompted protesters to temporarily occupy structures to bring attention to their concerns and interfere with operations until their demands have been registered. Indigenous people in Alaska, South America, and Nigeria have occupied platforms to protest economic and environmental issues. A great fear arises from the thought of terrorists holding a population of platform workers and the platforms themselves as hostages, then very publicly announcing their demands.[104] Over the years, terrorists and disgruntled employees have threatened bombing or sabotage of offshore facilities. In March 2003, Nigerian ethnic militants threatened to blow up 11 multinational oil installations they claimed to have captured in retaliation for government military raids.[105] In the conflict between Iran

and Iraq, and again in the Kuwait crisis, regular army combatants captured and occupied offshore structures, and even used them for observation or artillery platforms. In the March 2003 Operation Iraqi Freedom, U.S. forces found themselves capturing several Persian Gulf platforms, in order to prevent Iraqi sabotage and preserve the facilities for continued service.

Do conventional forces attack offshore facilities with intent to destroy? Iran and Iraq violently attacked each other's offshore infrastructure in their long war during the 1980s. U.S. forces reportedly were directed to attack several Persian Gulf oil platforms in response to the U.S.S. *Stark* incident, in which an Iraqi fighter struck the vessel with missiles. In the unrelated January 18, 1991, engagement cited earlier, the helicopter attacks were followed up with surface attacks from the U.S.S. *Nicholas* and a Kuwaiti patrol boat. The force fired three shots at each platform to set range, followed by about 20 rounds of high-explosive shells upon seven of the platforms.[106] Teams also boarded each of nine platforms and destroyed remaining fortifications and seized or destroyed all remaining weapons.[107] Looking back upon this discussion, surface threats, whether the attack is launched from a small pleasure craft, a mid-sized fishing boat, or a large vessel, have been conducted and are certainly feasible and one of the most likely means any enemy will continue to consider when seeking to harm the Gulf of Mexico infrastructure. A few surface threat modes that are plausible include:

- Small, fast speedboats used as "manned torpedoes" to carry loads of explosives and ram structures or ships. (Most likely surface threat based on historical operations).
- Tying up a fishing boat, including the type used by small independent fishermen (under 100 foot vessel), near a structure and detonating a powerful explosive device.[108]
- Commandeering (via piracy or employing a rogue crew) a tanker or other large ship and intentionally ramming another ship or an offshore platform.
- Using one or several small boats or fishing boats as a weapons platform to launch missiles, torpedoes, or other projectiles at a structure.[109]

- Boarding a structure from a surface mode and killing workers, stealing or destroying systems, or creating a hostage situation.
- Covert placement of a bomb on the structure, with either "real-time" detonation or triggered to include standoff or timed detonation.
- Wholesale destruction of numerous oil facilities to interfere with production or redirection of oil pipeline flows with specific intent to cause environmental harm.
- Using a container vessel as a helicopter or speedboat tender/assault ship to transport multiple teams to the Gulf to launch strikes before being suspected or identified by Coast Guard as a "high interest vessel."[110]

Subsurface Attack

Although one of the least likely and potentially one of the more technologically challenging routes for attack, it is possible to conceive of assaults to tankers or platforms via underwater routes. A fair amount of semi-submersibles are available and employed by oil and gas developers to drill, place, and maintain the vast underwater infrastructure. North Korean special forces possess unique semi-submersible gunboats, and North Korea has exported such craft to countries in the Middle East. In the Gulf, divers and diver support vehicles are available. Divers, and in particular, undersea welders and explosives experts, require a great deal of training and support to accomplish their routines, and schools offer certification courses. More conventional undersea military means could include mines and submarines. Mines in the Persian Gulf have presented a formidable threat to petroleum industry vessels. The Iraqis, Iranians, and our own U.S. Navy have conducted significant mining or anti-mining operations in the Persian Gulf in the past two decades—much to either interfere with or enhance oil transport security (most U.S. operations have been conducted to remove mines and to facilitate freedom of the seas rather than denial).

Does this underwater menace sound too ridiculous? Imagine this true-to-life scenario. On July 9, 1942, at approximately 11:25 p.m., the Standard Oil Company tanker *Benjamin Brewster* was torpedoed and set

afire just 2.5 miles off the Caminada Bridge that connects Grand Isle, Louisiana to the mainland.[111] A tiny U.S. Coast Guard patrol boat, armed with rifles and pistols, picked up a handful of survivors.[112] It can happen. In less than 12 months, 17 German U-boats sent 56 merchant vessels to the bottom of the Gulf, and 14 others were severely damaged.[113] What about today? Countries all over the world possess submarines. Red China has over 70, and North Korea has been described as having the largest submarine force in the world, if you include their smaller subs.[114] Even if we tracked large submarines that would dare enter and operate in Gulf, smaller submarines would be easier to hide in a cargo vessel or containers and launched when a "mother ship" came nearer to a target. Subsurface threats, though more technologically a challenge, could strike a dramatic blow, as outlined in the following:

- Placement of underwater explosives on pontoons or key production units by divers or via diver-delivery vehicle.
- Divers severing cables or damaging pipelines or breaching underwater floatation systems.
- Release or placement of contact or proximity or timed mines.
- Using a semi-submersible to sabotage or directly attack a complex.
- Firing torpedoes or missiles from a submarine.
- Ramming an old diesel-electric submarine into a structure below the waterline.

Cyber and Electronic

Cyber attacks could be stand-alone or accompany a more conventional attack to further spread confusion or to isolate an offshore unit. Control centers such as the LOOP's Galliano facility operate a vast array of remote switches, sensors, valves, and pump systems. Interference with offshore control center operations could be catastrophic. Exploration, production, storage and transportation (miles of pipeline and pumping systems) crisscross the Gulf, many dependent on some type of remote command and operation. Some cyber threats include:

- Overriding or corrupting production or pumping command and control systems to allow catastrophic failure.
- Interference with safety systems to allow physical attacks maximum opportunity for damage.
- Blocking, rerouting, or spoofing command and control or vital communications links to sever contact with structures.

Considerations Regarding Vulnerability

Many of the Structures are Built Tough to Endure

Offshore oil and gas platforms are built to endure tremendous forces of nature—to protect oil company investment from the perils of typhoons, hurricanes, and more. In the North Sea or off the coasts of Alaska or Newfoundland, design considerations must even include collision with icebergs. Sixteen huge concrete claws built to deflect powerful forces of ice surround the Hibernia unit off Newfoundland.[115] In the Gulf of Mexico, platform designs are not so stringent as the Hibernia's, although they are still impressive, particularly those with safety considerations mandated with construction in the past 20 years. Still, when Hurricane Andrew visited the Gulf, a Class 5 event with sustained winds in excess of 155 miles per hour, 22 offshore facilities fell and another 65 sustained major damage.[116] More recently, with 800 platforms in the path of Lili, a Class 4 storm with sustained winds of 145 miles per hour, 25,000 workers were evacuated and yet only six older platforms and four exploration rigs received substantial damage from the storm.[117] The Minerals Management Service asserts that these minimal effects were due in part to a series of more stringent design requirements mandated over past decades.[118] Current design standards require industry to design facilities to withstand 100-year storm criteria.[119] Production platforms, particularly the newer platforms including the deepwater complexes, are massive investments built to endure nature's most powerful forces.

Not only are offshore systems built to survive the rigors of Mother Nature; they are also designed to meet the challenges of hazards inherent in harvesting and transporting their flammable "liquid gold." Power systems, valves, and pumps are designed with redundancies and swift shutdown mechanisms, especially to prevent feeding fires from the wells.

Fire detection and control systems are available and ready. Fire protection is based on rapid detection, aggressive suppression, and reliable shutdown of fuel feed to any fire. Platforms are equipped with alarm and automatic detection systems, backed up by "fire watches" for hot work such as welding or cutting events.[120] Even so, a gas explosion destroyed Occidental Petroleum's Piper Alpha platform in the North Sea back in 1988, killing 167; deficient safety practices were cited.[121] In Gulf waters, Coast Guard regulations require facilities to have full water deluge systems, in addition to portable chemical extinguishers, to protect personnel and to give them sufficient evacuation time, if required.[122] Anti-spill and post-spill cleanup protocols are established and exercised. Radio communications and emergency systems, including protected lifeboats, are available.

In the final analysis, modern oil and gas facilities, through governmental mandate and the necessity to preserve the interest of developers, have become fairly robust in regard to surviving anticipated natural threats. Nevertheless, these structures, particularly our Gulf developments, have not been intentionally engineered to deter, prevent, and respond to acts of war.

Other Considerations

Many structures, and in particular, the very expensive new deepwater platforms, sit very high up, like castles in the air. Although some coastal platforms are relatively low, deeper platforms can be anywhere from 50 to 300 feet above the water.[123] This height requirement has not been driven by a need to "repel enemies" but by a need to survive storm surges and to increase drill slot opportunities. Visibility can be good from a platform or ship, with the ability to see a potential visitor a great distance away. Some key structures have their own radar or beacons. Helicopter pads allow quick evacuation or re-supply in addition to providing any aggressors potential access. Some platforms with helicopter pads have locked barrier gates between the pads and the rest of the structure. Platforms, particularly with a larger population, have small security details, not only to provide security from outsiders, but also primarily to provide security controls involving actions of members working on the platform.

One consideration already in use before 9/11 includes the establishment and enforcement of safety or exclusion zones around

platforms, initially with the intent of avoiding collision by vessels operating outside normal shipping channels. The U.S. Coast Guard announced effective May 1, 2001, that most vessels (larger than 100 feet) would be barred from operating within 500 meters of seven of Shell Oil's Gulf of Mexico high-production oil and natural gas platforms (most being associated with deepwater projects including Mars and West Delta examined earlier in this chapter.[124]

One can see that Gulf offshore energy infrastructure could fall prey to many potential modes of attack. Many of these modes of violence would seem shocking to us in our own "back yard," even if history has confirmed their use elsewhere in the world or years ago right off our own coast. Understanding the ways in which offshore structures might be attacked can help us form strategies to dissuade, deter, or mitigate the effects of an enemy's attempts to cause harm. There are many plausible scenarios for destruction, but much of the offshore system is also robust and somewhat protected by design. Studying the inherent strengths, advantages, and operations of offshore infrastructure can also serve as a foundation for beginning to determine the right course of action to preserve and protect our interests, and to assess if we have done enough in this arena.

Are We Moving in the Right Direction?

> *The industry has long assigned a high priority to protecting its facilities from attack. Since September 11, we have taken thousands of actions designed to further enhance the security of pipelines, refineries, oil and natural gas platforms, and other facilities. We recommend quick adoption of the new warning system by all levels of government. We will eventually incorporate the new system into our industry security guidance and suggest that our companies adopt it for their own security plans.*
>
> —American Petroleum Institute, March 13, 2002[125]

In Fuller and Lesser's article, Persian Gulf Myths, the authors assert that the United States spends $60 billion a year to protect the import of $30 billion worth of oil that would flow anyway—that is, our naval and air

presence provides a vast amount of security on the Persian Gulf end of the supply chain, and since those countries need the money that oil generates, they would export oil, despite the risks, anyway.[126] If we are willing to provide such expensive protection in that region, then should we be willing to provide the means and resources to better protect matters at the receiving end—in this case, in our own Gulf of Mexico? Many stakeholders are involved in the security of offshore enterprises, including the oil and gas developers, their support contractors, government agencies at all levels, maritime shippers, fishermen and recreational users of the Gulf, environmental groups, and various collectives of these players. Current initiatives, many relating to or facilitated by the Coast Guard, are underway to improve and enhance offshore infrastructure security, but much more work is required.

Current Initiatives

Existing Teams and Protocols

Presidential Decision Directives. President Clinton issued Presidential Decision Directive 39 in June 1995 to help energize national efforts to "detect, prevent, defeat, and manage consequences of weapons of mass destruction."[127] In 1998, the Clinton White House introduced Presidential Decision Directive 62 to combat terrorism and Presidential Decision Directive 63 to protect America's critical infrastructure, with a focus primarily upon cyber vulnerabilities.[128] Presidential Decision Directive 39 stated that America should have the ability to respond rapidly and decisively to acts of terrorism, using all appropriate instruments.[129] Under Presidential Decision Directive 39, the FBI operates as the overall Lead Federal Agency (LFA) for *crisis management*, which is primarily the law enforcement aspect of an incident, but may define an entity such as the Coast Guard as a lead agency to support a function, depending upon their resources and capabilities to meet a specific challenge.[130] The Federal Response Plan focuses more on the *consequence management* aspects of an incident (overall LFA for terrorist incident consequence management is the Department of Homeland Security–FEMA), and clearly highlights the important role of the Coast Guard in maritime situations.

[Editor's note: The Federal Response Plan and associated terminology is currently undergoing a thorough review and update by the

Department of Homeland Security and is expected to be released as the National Response Plan in late 2004.]

Federal Response Plan. The January 2003 Federal Response Plan details a fairly robust strategy for reacting to hazardous materials spills, including catastrophes involving oil and gas production. Emergency Support Function Annexes #10 and #12 provide two of the most relevant frameworks. The Environmental Protection Agency serves as the National Chair and lead agency for activation of hazardous spill response, in close coordination with the Coast Guard in geographic locations under U.S. Coast Guard jurisdiction. The Coast Guard serves as Regional Incident Chair for areas only under Coast Guard jurisdiction. Region Oil and Hazardous Pollution National Contingency Plans have been established, along with a "superfund" to provide money for response efforts.[131] The National Response Team, composed of 16 federal agencies with major environmental and public health responsibilities, is the primary vehicle for coordinating federal agency activities under the National Contingency Plan.[132] The Coast Guard maintains the National Response Center and manages the National Strike Force (NSF), three strike teams located on the Pacific, Atlantic, and Gulf coasts to facilitate responses.[133] In the Gulf, the U.S. Coast Guard Eighth District Response Group provides the on-scene coordinator with technical assistance, personnel, and equipment during responses involving maritime zones.[134]

FRP Emergency Support Function #12 deals with energy incidents. The Department of Energy takes the lead to facilitate responses to energy system damage.[135] "Energy" includes production, refining, transporting, generating, transmitting, conserving, building, and maintaining energy systems and system components.[136] For offshore facilities, the Minerals Management Service is specifically tasked to provide energy production and well reserve information, assess energy production damage and projected repair schedules, and provide engineering and technical support.[137]

Department of Homeland Security Key Documents.[138] The National Strategy for Homeland Security outlines a template of strategic objectives to protect the homeland. These objectives in order of priority are to: prevent terrorist attacks within the United States; reduce America's vulnerability to terrorism; and minimize the damage and recover from attacks that do occur. To accomplish these objectives, the national

strategy identifies six critical mission areas: intelligence and warning; border and transportation security; domestic counter-terrorism; protecting critical infrastructure; defending against catastrophic terrorism; and emergency preparedness and response. The National Strategy transcends federal, state, and local levels of government and into the private sector and is designed to protect and build from the sacred American foundations of law; science and technology; information sharing and systems; and international cooperation.

Colonel Robert "Bob" Stephan, USAF (Retired), and his team from the Department of Homeland Security drafted a milestone document that will serve as a steppingstone and overarching framework to work critical infrastructure security issues in a coordinated, cohesive national approach. The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, released in February 2003, outlines guidelines and initiatives to steer a cooperative effort between government, industry, and private citizens to secure our nation's infrastructure and assets. This national strategy builds on the evolution of past homeland security initiatives and identifies 11 critical infrastructure sectors including energy. Two of the published oil and natural gas initiatives include "developing strategies to reduce vulnerabilities" and "developing standardized guidelines for physical security programs." These specific measures are a definite step in the right direction to protect such critical nodes as those in the Gulf. Over recent years, the Gilmore, Bremer, and Hart-Rudman Commissions all endeavored to study and publicize means to prevent, combat, and mitigate terrorism: today, the Department of Homeland Security has launched a focused effort to turn many of the best ideas found in these Commission reports into real courses of action. The race is on to see if the bureaucratic process required to implement such needed protection is quick enough to outpace potential terrorist activity.

Gulf Safety Committee (GSC). The GSC is a marine transportation system committee that grew out of a series of informal meetings among Gulf waterway stakeholders, users, and regulators that commenced on October 10, 2002, spurred by the events surrounding 9/11. The GSC has one standing subcommittee dealing with security issues, with additional standing and ad-hoc subcommittees formed as necessary.[139] The Draft Gulf Safety Committee Meeting Notes for November 7, 2002, yield some interesting insights as to the progress of the organization.[140] The GSC

now champions four initiatives, including two that concern distributing information to industry groups. The first explains the different security policies championed by the Coast Guard and Department of Homeland Security, and the second tells ship owners how to report suspicious activity.[141] The third project deals with creating a notification system to alert industry officials when security threats change, and the fourth idea relates to creating voluntary standards for oil industry and fishing vessels to take for each level of alert.[142]

Industry Involvement

For years, international private companies have faced nearly every conceivable threat to their oil and gas exploration, development, transportation, and production infrastructure. Stakes have been high, particularly in developments abroad, many of which reside in "cauldrons" of specific dangers. Not long ago, a major international oil company employed its own organic helicopters and security coordinator to deliver Nigerian assault troops, driving off bands of people who had taken over several oil platforms. American citizens working on offshore developments internationally have had to endure significant risks. Conversely, oil and gas company developments in or near the United States have escaped much violence or harm, with the exception of damage from natural threats. Risk assessment is not new to the oil and gas business, and industrial security has long been a consideration for the profession. Many physical and process protocols are in place to deal with threats to their valuable assets. To some degree, the same experience applies to merchant ships, facing myriad threats as they course the world's seas in trade.

On the other hand, fishermen of the Gulf have not had to be very concerned about security matters regarding protection of offshore facilities. As noted earlier, around 85 percent of the time, their destinations involve traveling to or near the "artificial reef" environments created by offshore structures. It's common practice to fish near these structures, and even tie up to them. Now fishermen are in a position to participate in measures to increase offshore security, either in cooperative partnerships to allow their continued access to offshore developments, or in forced arrangements excluding their presence from stricter "security zones" near high-value structures.

Coast Guard

The United States Coast Guard provides the backbone and muscle for Gulf security today. The National Strategy for Homeland Security, July 2002, asserts as a key priority to "recapitalize the U.S. Coast Guard."[143] The document states intentions to acquire the sensors, command-and-control systems, shore-side facilities, boats and cutter, aircraft, and people the Coast Guard needs to perform all of its missions, including assuring the safety of Americans at sea, maritime domain awareness, and fisheries enforcement.[144] Three major Homeland Defense related U.S. Coast Guard concepts include "Deepwater," creation of Maritime Safety and Security Teams, and Maritime Domain Awareness. These strategies are representative of actions taken by the U.S. Coast Guard; however, they are not "all-inclusive" in regard to the full-court press this resource-challenged organization has made regarding Homeland Security. Money is flowing to the Coast Guard at unprecedented levels, but none too soon.

Deepwater Project. Over the next 20 years, the U.S. Coast Guard intends to invest $10 billion to recapitalize its deepwater fleet.[145] Deepwater missions are those that generally occur more than 50 miles offshore.[146] Coast Guard activities in this zone typically require longer-duration transit times or presence, forward deployment of forces, or a combination of these considerations.[147] Three industry teams are developing competing proposals on strategies and systems to perform the required deepwater missions in a long-term cost-effective manner.

Maritime Safety and Security Teams (MSST). These federal maritime "Special Weapons and Tactics" (SWAT) teams are highly trained, strategically located, and specially equipped to provide a much-needed extra layer of security to key ports, waterways, and facilities.[148] The Coast Guard has established their Special Missions Training Center at Camp Lejeune, North Carolina, to train new MSSTs and other Coast Guard members on port security.[149]

Maritime Domain Awareness. The goal of maritime domain awareness is the timely possession of information and intelligence, and the ability to conduct surveillance and reconnaissance of all vessels, cargo, and people that operate in the maritime domain well before a potential threat enters U.S. maritime borders.[150] The President's 2003 budget included $88 million towards that goal.[151] Currently, the idea of maritime domain awareness is much more a concept than a reality. Captain Richard

Kelly, a Coast Guard spokesman, has remarked that the agency's existing ships and planes are "blind, deaf, and dumb," and they often fail to detect and identify vessels.[152] He further noted that Coast Guard ships and aircraft have little ability to share data that would provide everyone with the same situational awareness. GPS transponders aboard some vessels and the Coast Guard's limited Vessel Tracking System, used in several ports, provide a partial cure. The shipping industry has not mandated a GPS-based worldwide maritime tracking system using transponders to identify and track ship movements in the manner of airline aircraft today, but many ships, notably large tankers, now employ such systems on a volunteer basis.

A Few Recommendations

Organizing, Training, Equipping and NORTHCOM

Cross-tell of tactics, training, and procedures. Other nations such as Australia, Great Britain, Norway, Brazil, and Persian Gulf operators have developed extensive protocols for protecting and defending offshore infrastructure. Harbors and petroleum companies across the world, including our own Alaska operations, for example, share similar concerns and seek similar solution sets. Coast Guard and oil company representatives involved in the Gulf should engage in deliberate and on-going cross-tell discussions with these entities. "Same eyes" interdisciplinary teams could visit numerous sites and harvest useful "best practice" descriptions to pass along to other interested stakeholders.

Develop a fully integrated command structure. In light of the creation of U.S. Northern Command and the Homeland Security Department and the realization that the Gulf region is a unique maritime/airspace region, old regional divisions, to include not only lines on the map, but actual organization and distribution of units and their assets should be *thoroughly* reexamined.[153] U.S. Northern Command should take the lead to integrate Coast Guard, airspace surveillance, air defense, special operations, naval units, and related agencies into a new, functionally cohesive response force for *effectively* coordinating defense and threat response in the Gulf region. The Joint Interagency Task Force used for drug interdiction may provide a few insights into what to do and what to avoid. In addition, old "Continental Air Defense Command" or

"Air Defense Command" concepts could be excavated for any practical principles.

Contingency Plans. Detailed risk analysis, vulnerability assessments, scenarios, and contingency plans need to be developed by the above integrated command structure with significant input and review by offshore infrastructure owners, users, and supporting technical experts. Great infrastructure may be in place to react to an oil spill, but limited comprehensive planning and thought has been vested in fully integrated plans to deter, protect, and mitigate actions potentially caused by terrorists or state actors in this region. In 1985 and 1987, the author served as a planner in exercises code named BRIM FROST, a defense of the Alaskan peninsula and oil infrastructure in particular from potential enemy attack. Active, Guard, and Reserve forces of all components played in these exercises, highlighting strengths and weaknesses and iteratively improving our capacity to defend that area of responsibility. Contingency plans already in place to defend Alaska or Hawaii may be of use as starting points in strengthening Gulf contingency planning. U.S. Northern Command and the Homeland Security Department should partner to build the organizational structures and plans to accomplish the mission of defending the Gulf, not just leaving the Coast Guard to "go it alone." *[Editor's note: The U.S. Coast Guard now falls under the domain of the Department of Homeland Security.]* Defensive operations need to be coordinated and joint, even if the Coast Guard eventually will have the bulk of the capacity to meet the challenge. Finally, we need to train, test, and evaluate all players using scenarios that drive integrated response.

For example, exercises need to be planned and conducted that require an integrated, cohesive response. One of the best exercises for this region in recent years was Exercise Amalgam Virgo 01, a joint-service, cruise-missile defense exercise conducted in June 2001.[154] In another case, a scenario involving several high-speed watercraft and unfriendly aircraft could be reported as intending to damage specific offshore targets. Military attack helicopters, rendezvousing with seasoned Coast Guard helicopters as guides, could practice intercepting "explosive-laden" speedboats or fishing boats. Practice in intercepting these surface vessels and aircraft, using a combination of Coast Guard, Active/Guard/Reserve Army helicopters, Special Operations Teams, and Air Force assets could

be tested and evaluated. When an unwanted visitor chooses to violate a safety zone and ignores repeated radio communications to divert, time is of the essence. Developing Quick Reaction teams, whether from the Coast Guard Maritime Safety and Security Teams or other forces, is essential. How well would joint players work together? How interoperable is their equipment? What strength would each bring? How can we foster better integration? Visible exercises such as these could in themselves deter potential wrongdoers from considering offshore harm, while other "not so visible" exercises could hone unique skills necessary to defeat an attack.

Air Warning, Tracking, and Defense. Today, the United States spends over $7 billion a year on developing a national missile defense. Meanwhile, as our nation's air traffic control shifts towards tracking on-board GPS beacons rather than always "painting" aircraft with active radar, America's interior radar systems are deteriorating. Tough decisions decades ago led our country to largely dismantle or neglect maintenance of highly integrated air defense zones, although some efforts have been made after 9/11 to lash together systems into an integrated picture via the Joint Surveillance System (JSS).[155] Defense against "air breathing" threats that don't happen to be squawking via a GPS transponder can be a significant challenge, especially if the threats are traveling at low altitudes, where even the existing Federal Aviation Administration and military radars can have dead space due to physical obstructions or other technical reasons.[156] Technology exists to greatly improve airspace visibility, and throughout the 1980s and 1990s, efforts to interdict drug smuggling operations led to using a picket line of balloon-suspended radars along the Gulf coast to provide detailed radar coverage. These Tethered Aperture Radar Systems (TARS) provided long-range and low-altitude visibility.[157]

These radars, along with other balloon systems using newer technology, and bolstered by potentially basing modern radars on offshore structures (similar to the old Air Force "Texas Towers" off the east coast) could be employed to provide early warning and intercept tracking in the Gulf. An integrated stationary radar system could provide the coverage necessary to deter, detect, and destroy air-breathing threats. Several of the balloon radars have fallen into disrepair, and North American Aerospace Defense Command (NORAD), in their posturing of limited funding, has

chosen to allow them to stay inoperative, citing the command has "no mission" for them.[158]

In the meantime, Coast Guard officials, seeing the value of these Gulf TARS sites, are begging for their revived operation.[159] This is a current example of a critical "fault line" and "budget war" preventing true revitalization of U.S. air defense capability, and in this case, allowing Gulf assets and ports to continue under the risk of harm. Another option would be to permanently patrol the Gulf with Aegis-capable Navy ships, which would be an ideal umbrella—but at a very significant cost to maintain on station.

Today, alert pilots at fighter bases around the nation report to CONAR, the Continental United States Region of NORAD. For the Gulf, the Southeast Air Defense Sector work with FAA to match aircraft with flight plans—and if things don't track, they can arrange a fighter intercept. This practice does not necessarily cover the whole country's air space "seamlessly" and thoroughly, let alone provide well-constructed layered defensive zones for defending offshore interests, particularly those in deep water. It is absolutely amazing that the United States, with a strategy that understands the significance of systematically destroying any enemy's integrated air defense system, has such a limited air defense in the Continental United States to defend vital centers including key cities or our own oil production, import, refining, and storage (national strategic reserves, approximately 700 million barrels)—many located within a 200-mile radius of each other. Semi-Automatic Ground Environment, Nike-Zeus missile sites, "Sky-Witch" radar-controlled anti-aircraft guns, and Delta Dagger interceptors haven't been seen by several generations of Americans…what do we want to buy back to defend our skies—and how much of the Gulf do we want to include in that defense?

In the meantime, we'll need to do a lot of partnering with the operators of the hundreds of helicopters, support boats, fishing vessels, and oil and gas industry workers to develop a set of "eyes and ears" to help authorities observe and report unusual acts or behavior, and promote more "personnel reliability" and licensing/credential verification to ensure these operators and workers are "true-blue" patriots themselves.

Surface Vessel Tracking. As noted earlier in the "Maritime Domain Awareness" Coast Guard discussion, another lucrative area for breakthrough improvements involves surveillance and tracking of surface

vessels out in the Gulf. Today, satellite communications and GPS systems are available which, if mandated on all commercial ships, would be a good stepping stone towards increased visibility of surface tracking. SHIPLOC, a relatively inexpensive satellite tracking system now commercially available, allows shipping companies (and perhaps through new protocols, the U.S. Coast Guard, too) to monitor the exact location of their vessels using a personal computer with Internet access.[160] The SHIPLOC device can be concealed on board the ship without the knowledge of the crew; if the ship deviates from course, it can be flagged. SHIPLOC, GPS transponder, and active surface tracking radar data systems output eventually need to be fused together into digital systems that can provide a common sight picture for vessel tracking through large areas of the Gulf, especially approaches to major ports and offshore facilities. Perhaps one day, high-altitude loitering Unmanned Aerial Vehicles or geo-stationary satellite systems could be employed to provide accurate and relatively low-cost and reliable surface and air traffic visibility.

Counting the Costs

We must continue to facilitate more meaningful interaction among key stakeholders in the Gulf, leverage ongoing avenues and institutions, and provide and spend dollars *prudently* to meet the challenge. Priorities and an understanding of acceptable levels of risk must guide our efforts, or huge amounts of dollars will have been wasted and perhaps the most catastrophic circumstances neglected. Turf battles and seams must be healed, and we cannot force either the Coast Guard or the Gulf inhabitants—shippers, fisherman, and the oil and Gulf enterprises—to bear the burden alone.

Conclusion

> *Commercial aircraft, natural gas pipelines, the electric power grid, offshore oil rigs, and computers storing government and corporate records are examples of sabotage-prone targets whose destruction would have derivative effects of far higher intensity than their primary losses would suggest…the foci of communications,*

> *production, and distribution are relatively small in number and highly vulnerable.*
>
> —Robert Kupperman
> Facing Tomorrow's Terrorist Incident Today[161]

The United States must recognize the value of our offshore energy infrastructure in the Gulf of Mexico, consider the risks, and take continued prudent measures to protect our interests there. This chapter provides a brief overview of valuable assets in the Gulf, to include oil and gas platforms, the LOOP, tanker traffic and lightering zones, and critical pipelines and links to onshore support. Offshore systems require a great deal of helicopter and ship support, and share a symbiotic relationship with a robust fishing industry. The trend is for us to see more Gulf of Mexico oil and gas development, more expansion into the deeper water, and more expensive floating platforms further out in the Gulf. From this analysis it is clear how readily available and detailed "open source" information can aid those who seek to understand offshore infrastructure, whether for good or harm. Two example "high value" systems were highlighted: the LOOP and the Mars complex, that helps us understand our offshore investments. Clearly the Gulf's offshore infrastructure is vulnerable to attack, with possible attack consequences, threatening destruction and loss of life, public disruption, major economic and financial loss, and potential destructive environmental outcomes. The Gulf is vulnerable to multiple modes of attack—by air, surface, subsurface or cyber strikes. Presently, there are some ongoing actions to provide better security and this study proposes a few additional recommendations regarding security of offshore interests. Threats to U.S. Gulf of Mexico assets are real and require a balanced and deliberate approach towards defending them. The Gulf of Mexico harbors immensely valuable sources of wealth for the United States and this is offered as a preliminary analysis to help U.S. policy-makers better understand the costs and benefits of various paths to better protect this important region of our homeland.

Notes

1. Gary Hart and Warren B. Rudman, *America Still Unprepared—America Still in Danger*, Report of an Independent Task Force Sponsored by the Council on Foreign Relations, 2002.

2. Chevron Texaco Oil Company in Nigeria; in previous years, oil company helicopters ferried Nigerian troops out to confront locals who had seized oil platforms, resulting in forcible removal and loss of several lives. Information from Hector Igbikiowuba and Kingley Omonobi Warri, "Navy Storms Oil Platform, Releases 18 Hostages…" *Vanguard (LAGOS) News*, 21 November 2003. On-line. Internet, 13 Dec 2003. Available from http://allafrica.com/stories/printable/2003112110819.html and "Nigeria: Chevron Texaco Yet to Start Talks with Protesters," *LAGOS*, 21 August 2002 (IRIN). On-line. Internet, 2 Dec 2002. Available from http://www.irinnews.org/report.asp?ReportID=29440.

3. Al Mukalla, "Evidence Points to Yemen Terror Attack," *CBSNews.com*, 11 October 2002, 1. On-line. Internet, 2 December 2002. Available from http://www.cbs news.com/stories/2002/10/06/world/printable524488.shtml.

4. In addition, the coastal marshes are a key habitat in their own right, reference Humberto Fontova, "Offshore Oil Drilling: An Environmental Bonanza," *NewsMax.com, America's News Page*, 12 April 2002, 1-3. On-line. Internet, 26 November 2002. Available from http://www.newsmax.com/archives/articles/2002/4/12/132638.shtml.

5. "LA 1 Coalition, Facts and Figures," *LA 1 Coalition, a non-profit corporation to improve a critical U.S. energy corridor*, 1. On-line. Internet, 13 November 2002. Available from Hhttp://www.la1coalition.org/facts.htmlH.

6. Ibid.

7. Confirmed by sources within the Mineral Management Service in October 2002.

8. Michael L Godec, "Future Gulf Supplies: Role of Federal Government," *Oil and Gas Journal;* Tulsa, 2 Sep 2002, 32-38.

9. LA 1 Coalition, 2.

10. Ibid., 3.

11. Fontova, 1-3. This number tracks closely with data provided by the U.S. Coast Guard Eighth District provided to an AWC Homeland Security Elective Course field trip to New Orleans 7 November 2002. Other relatively current information sources, including data from the Minerals Management Service (MMS), a Federal government entity, articulate that more than 4,000 platforms operate in the Gulf, but some of these also include barges or converted vessels serving as drilling or service platforms. More

useful Gulf information can be secured through MMS and may be available on-line at Hhttp://www.Gulfr.mms.govH.

12. "Facts about the Gulf of Mexico," *Gulf of Mexico Foundation*, n.p. On-line. Internet, 6 December 2002. Available from http://www.gulfofmexicofundation.com/facts.htm.

13. LOOP, LLC. On-line. Internet, 26 November 2002. Available from www.loopllc.com/content2a.cfm. The LOOP, LLC. Official Web Site also contains four movies that detail many aspects of LOOP operations; these movies contributed a great deal to the facts described in the paper. The LOOP web site also appears to be a portal for companies that use LOOP facilities, to include booking arrivals and transactions (password required).

14. LA 1 Coalition, 1.

15. LOOP, LLC., n.p.

16. LA 1 Coalition, 4.

17. LOOP, LLC., n.p.

18. Committee on Oil Spill Risks from Tank Vessel Lightering, Marine Board, *Oil Spill Risks from Tank Vessel Lightering* (Washington D.C.: National Academy Press, 1998), 2.

19. Ibid., 9.

20. Ibid., 3.

21. Ibid., 4.

22. Gulf of Mexico Program.

23. "Port Overview," *Port of Louisiana.* On-line. Internet, 3 December 2002, n.p. Available from Hhttp://www.portsl.com/pages/15_overview.htmlH.

24. Ibid., n.p.

25. Ibid., n.p.

26. Fontova, 2-3.

27. Gulf of Mexico Foundation, n.p.

28. Ibid., n.p.

29. "The Gulf of Mexico: A Valuable National Resource," Gulf of Mexico Fact

Sheet, *Gulf of Mexico Program*, accessed 2 Dec 02, available on-line at http://www.onegulf.org/Gulffacts.html , 1.

30. Ibid., 2.

31. Ibid.

32. Ibid., 3.

33. Gulf of Mexico Foundation, n.p.

34. Ibid.

35. Gulf of Mexico Program.

36. Perhaps at this point it may be useful to note that one ton of crude oil is the equivalent of about 311 U.S. gallons or roughly 7.4 barrels of oil. Oil and oil capacity, depending upon the frame of reference, may be characterized by any of these measures.

37. A builder of VLCCs noted that seven "Statues of Liberty" would fit into one of their ships.

38. Gulf of Mexico Program.

39. Ibid.

40. "Industry Trends," *Oil and Gas Journal*, 14 October 2002, 7.

41. Ibid.

42. Ibid.

43. John Westwood, "Special Report—Offshore Petroleum Operations: Worldwide Offshore Sector Offers Major Challenges," *Oil and Gas Journal*, Tulsa, 30 April 2001, 72-76.

44. Developers have christened deepwater platforms and many other offshore oil and gas complexes with colorful names.

45. This security guide is available from http://rf-web.tamu.edu/security/ SECGUIDE/About.htm. The guide is Version 1.0 of a program developed for the Defense Security Service Academy by the Defense Personnel Security Research Center. The content is, of course, unclassified and approved for public release.

46. LOOP, LLC., n.p.

47. Rafael Bermudez, "LOOP Performing Well Environmentally," *Lousiana Environmentalist Magazine*, Louisiana State University, May-June 1994, 2. On-line. Internet, 20 November 2002. Available from Hhttp://www.leeric.lsu.edu/le/cover/lead054.htmH.

48. Current year estimates from various sources reflect between 15-17%; references from the early 1990s reflect as low as 11%.

49. LOOP, LLC., n.p.

50. Bermudez, 2, 5.

51. LOOP LLC., n.p.

52. Ibid.

53. Bermudez, 2.

54. Ibid., and LOOP LLC movie clip.

55. Bermudez, 2.

56. Ibid., 4.

57. Available from multiple sources on-line.

58. 1.5 miles per Bermudez; 8,000 feet per LOOP LLC movie available on-line.

59. Bermudez, 2.

60. Available per the LOOP LLC movie on-line.

61. LOOP LLC., n.p.

62. Via the interconnectivity with CAPLINE, a major U.S. distribution system.

63. The *LOOP Responder* schematic drawings reside at an academic site, not on any directly sponsored by LOOP or the state of Louisiana. *LOOP Responder* performance data was available via several sites, including the LOOP LLC home page and that of the vessel's manufacturer.

64. LOOP LLC Port Booklet, January 2002, section 12, available on-line at the LOOP LLC Home Page. A detailed written description of LOOP facilities has been intentionally removed and cited as "no longer available" from this booklet by LOOP.

65. LOOP LLC., n.p.

66. Ibid.

67. Ibid.

68. All discussed on LOOP LLC movies available on-line.

69. Discussed on LOOP LLC movies available on-line—could find very few other references to this facility.

70. Per LOOP LLC Port Booklet.

71. "SEPCo—News—2000-07-Deepwater Hubs: A New View of Gulf Operations." On-line. Internet. Available from http://www.shellus.com/sepco/news/2000/07_hubs.htm, 3.

72. "SEPCo—Where We Operate—Offshore—Mars." On-line. Internet, 26 November 2002. Available from http://www.shellus.com/sepco/where/offshore/mars.htm, 2.

73. Ibid.

74. Ibid., 3.

75. One free service that provides this data to fishermen and divers is copyrighted by Rigs, Reefs, and Wrecks, Inc. It is interesting the page's "fine print" notes "the list has been seeded with slight changes to over 1,000 records that will not interfere with the use of the data but will identify any duplication, republication or redistribution of the data. On-line. Internet, 26 November 2002. Mars coordinates available from http://www.rodnreel.com/gps/GpsPointDetail.asp?ID=34371. I looked these up and cross-referenced them on other navigational maps and found the data quite accurate for basic navigational use (although unclear if literally "on the money" for GPS precision-guided purposes).

76. SEPCo, Mars, 3.

77. Ibid.

78. Ibid.

79. Ibid.

80. Ibid.

81. SEPCo, News, 3.

82. Taken from a Federal Bureau of Investigation press release. On-line. Internet. Available from www.fbi.gov/pressrel/pressrel02/nlets100902.htm.

83. Oil and gas production, refining, and distribution are critical to industrial societies. United States air strategists have long recognized the value of striking enemy energy infrastructure. Attacking offshore infrastructure, especially in parallel attack against other vital centers, could have severe consequences. Colonel Phillip S. Meilinger, USAF, describes American airpower theories in *The Paths of Heaven: The Evolution of Airpower Theory*, Air University Press, Maxwell Air Force Base, Alabama, 1997.

84. From British strategist Liddel Hart to the Gulf War's Col John Warden, such a viewpoint of strategic paralysis has been espoused.

85. Full text of bin Laden interview/transcripts available through Cable News Network at Hhttp://cnn.allpolitics.printthis.clickability.comH, 3.

86. Meilinger, 10-19, 160.

87. Remarks of Kenneth I. Juster, Under Secretary of Commerce, Bureau of Industry and Security, "Economic Security and Community Leadership`" at the Conference on Critical Infrastructures: Working Together in a New World, 23 April 2002, n.p.; On-line. Internet, 19 December 2002. Available from http://www.bxa.doc.gov/press/2002/JustSpeaking4_23_NJ.html.

88. Steve Clark, "Hurricanes Make Gulf Oil and Gas Production a Risky Business," *BusinessReport.com*, 8 October 2002, n.p. On-line. Internet. Available from www.businessreport.com. Clark describes the millions of dollars lost when hurricanes shut down production from offshore platforms: a significant economic impact.

89. Clark,n.p., an eye toward destruction, discussed in chapter one.

90. John Yaukey, "Cargo Shipping Poses Big Problems for Homeland Security," *Gannett News Service*, 2 December 2002, 1. On-line. Internet. Available from Hhttp://www.gannettonline.com/gns/911/more4.htmH.

91. Matthew G. Devost and Neal A. Pollard, *Taking Cyberterrorism Seriously: Failing to Adapt to Emerging Threats Could have Dire Consequences*, The Terrorism Research Center, TRC Analysis, 27 June 2002, 2.

92. From the article "Oil Tanker Disaster Destroys Livelihoods in Spain," as contained in *Drillbits and Tailings*, Volume 7, Number 10, December 2002. On-line. Internet, 22 January 2003. Available from www.moles.org/ProjectUnderground/drillbits/7_10/2.html.

93. "Oil Spills: Lessons from Alaska for Sakhalin," *Slavic Research Center*, Hokkaido University, 1999. On-line. Internet, 3 December 2002. Available from http://src-h.slav.hokudai.ac.jp/sakhalin/eng/71/steiner6.html, 2.

94. Professor Paul R. Baumann, "Environmental Warfare: 1991 Persian Gulf War," n.p., on-line, Internet, 31 March 2004, available from http://employees.oneonta.edu/baumanpr/geosat2/Environmental_Warfare/ENVIRONMENTAL_WARFARE.htm.

95. United States General Accounting Office, *COMBATTING TERRORISM: Threat and Risk Assessment Can Help Prioritize and Target Program Investments*, April 1998, GAO/NSIAD-98-74.

96. GAO/NSIAD-98-74.

97. "Once Again World Petroleum Warned of Possible Terrorist Attacks," World Industry News, *Oil and Gas International*, 16 November 2002. On-line. Internet, 4 December 2002. Available from http://www.oilandgasinternational.com/departments/world_industry_ news, 1.

98. Per interview with Col Ray Kruelski, USAF Special Operations helicopter pilot, December 2002.

99. Per report of 25 major Gulf of Mexico helicopter operators, "Gulf of Mexico Offshore Helicopter Operations and Safety Review," 17 April 2000. On-line. Internet, 2 Dec 2002. Available from Helicopter Safety Advisory Conference Home Page, Hhttp://www.hsac.org/stats.htmlH.

100. George Rodrique and Robert Ruby, "Desert Storm: Taking Down the Oil Platforms," *Proceedings*, U.S. Naval Institute, Volume 117/4/1,058, April 1991, 53.

101. Judy Clark and John Bray, "Added Global Risks Impact Security Planning for Oil, Gas Expatriot Workers," *Oil and Gas Journal*, Tulsa, 22 April 2002, 32-37.

102. Steve Hara relates the devastation of the 12 Oct 2000 attack while the *USS Cole* was refueling in Yemen in his news release carried by the Armed Forces Press Service. On-line. Internet, 22 January 2003. Available from http://www.defenselink.mil/news/Oct2000. Years earlier, on 17 March 1987, the *USS Stark* was hammered by two Exocet AM39 air-to-surface missiles fired from an Iraqi Mirage F-1. The Exocets had a range of 40 miles and each carried a 352-pound warhead. One missile tore a ten-by-fifteen foot hole in the warship's steel hull on the port side and another plowed into the frigate's superstructure. Earlier that day, Iraqi jets had fired missiles into a Cypriot tanker, crippling the vessel, as discussed in Jason Manning's article on "The *USS Stark* Incident," *The Eighties Club* on-line, Internet, 22 Jan 2002, available from Hhttp://eightiesclub.tripod.com/id280.htmH, n.p. Thus, enemies have and do possess means to attack our warships through several means--approaching in explosive-laden boats or using sophisticated sea-skimming missiles—and could try similar operations against unarmed vessels.

103. Shelley Kerr, "U.S. Warns of Increased Terrorist Threat Against Ships," *Tankerworld.com*, 29 October 2002. On-line. Internet, 2 December 2002. Available from www.tankerworld.com/news/oct2002/news_29102002_5.htm, 1.

104. Duane John Phillips, LCDR, USN, *Deterring Offshore Terrorism*, 3 March 1989, Naval War College, Newport, RI. LCDR Phillips provides one of the very few serious treatments on this subject I have found. He highlights terrorism as a crime that needs attention advocating use of joint military forces and strengthened international law to counter the threat.

105. "We'll blow these stations and blast the pipelines. We will take Nigeria 20 years backward," Dan Ekpebide, a leader of the Ijaw tribal fighters in Nigeria's oil-rich Niger Delta, told the Associated Press. His fighters were armed with machine guns and grenades. Courtesy of AP On-line, as reported in "News Headlines" portion of Poten and Partners web site, March 2003. On-line. Internet, 22 March 2003. Available from Hhttp://www.e-topics/com/H n.p.

106. Rodrique, 53.

107. Ibid. Little is spoken of U.S. Special Forces operations involving Persian Gulf platforms; some general mention is recorded in USSOCOM's official history, but these actions and others have taken place, including practice missions to "retake" oil platforms besieged by aggressor forces.

108. Fishing boats are permitted to enter certain zones and even literally tie up to many platforms to fish.

109. Gulf narco-traffickers have had experience in operations to evade law enforcement and have employed the latest communications, navigation, and certainly the fiscal means to purchase arms that could outfit vessels for this task. U.S. and other nation's watercraft builders even design and sell craft "ready made" to operate as small patrol or gunboats. Normal fishing or pleasure craft could be adapted for this use as well.

110. The U.S. Coast Guard has been working diligently to identify and board "high interests vessels" prior to their arrival in U.S. port facilities.

111. C.J. Christ, "War in the Gulf: Oil Tanker Sinking Brings War Close to Grand Isle Shore," as described in the 18 February 2001 edition of *The Courier*, Houma, Louisiana. On-line. Internet, 6 December 2002. Available from http://www.crt.state.la. us/crt/tourism/lawwii/courier_articles/oil_tanker.htm, 1-3.

112. Ibid., 2.

113. Robert A. Church and Daniel J. Warren share some fascinating stories in their article entitled "U-Boats in the Gulf of Mexico," *Go Gulf Magazine, The Leading Magazine for Gas, Oil and Oil Technology*, July/August edition, 27, also available from Hwww.gogulf.netH.

114. These assessments can be confirmed by PACOM experts as of 2003. Only

four years earlier, North Korea (DPRK) had been described as having the fourth-largest submarine fleet in the world.

115. "Hibernia Grand Banks, Canada," *Offshore Technology, the Website for the Offshore and Gas Industry*. On-line. Internet, 3 December 2002. Available from http://www.offshore-technology.com/projects/hibernia, 1-4.

116. "Mineral Management Service (MMS) Preliminary Report on Lili," released 16 October 2002, n.p. On-line. Internet, 7 December 2002. Available from http://Gulfr. mms.gov/homepg/whatsnew/newsreal/021016.html.

117. Ibid. See also Steve Clark, n.p. The Clark article goes on to detail economic impact of loss of production during Isadore, which had come weeks before Lili was only labeled as a Tropical Storm. Approximately 3 days of production were lost, equating to 4.5 million barrels of crude oil and 25 billion cubic feet of natural gas for losses of around $137 million and $90 million respectively.

118. MMS Preliminary Report on Lili, n.p.

119. Ibid.

120. Hallie Ephron Touger, "NFPA and the Offshore Oil Industry are Helping to Resolve Dueling Federal Fire Safety Standards," *NFPA Journal*, National Fire Protection Association, September/October 2001, Volume 95, Issue 5, 46-50, on-line, available via Proquest.

121. Ibid., 47.

122. Ibid., 48.

123. Ibid.

124. "Vessel and Facility Compliance News May 2000," *MSO Morgan City Summer 2000 Newsletter*, U.S. Coast Guard, n.p. On-line. Internet, December 2000. Available from Hhttp://www.marinecompliance.org/newsletters/uscgnewsmay200.htmH. Very interesting to note these exclusion zones were added around *VERY HIGH* value platforms (Boxer, Bulwinkle, Ursa TLP, West Delta, Mars TLP, Ram-Powell TLP, and Auger TLP), most being new super deepwater platforms, of which there are only around 12 such complexes in the Gulf.

125. "API Applauds New Homeland Security Alert System," *Modern Bulk Transporter*, On-line Exclusive, 13 March 2002, n.p. On-line. Internet, 30 November 2002. Available from Hhttp://bulktransporter.comH.

126. Graham Fuller and Ian O. Lesser, "Persian Gulf Myths," *Foreign Affairs*, May/June 1997. On-line. Internet, 1 Dec 2002. Available from http://www.foreignaffairs.org.

127. Quote extracted from the Presidential Decision Directive 39 (PDD-39) unclassified readings found at http://www.dartmouth.edu/~engs05/readings/md/wmd/WMDHTML/sld003.htm, np.

128. PDD-62 and PDD-63 are illuminated in http://cns.miis.edu/research/cbw/pdd-62.htm and http://www.usdoj.gov/criminal/cybercrime/factsh.htm, respectively.

129. PDD 39, references are cited in the Federal Response Plan (FRP), together with other secondary sources. Further, PDD-63 contains insights supporting such incidents.

130. TI-15, Terrorism Incident Annex to the Federal Response Plan (FRP)

131. Ibid., ESF #10.

132. Ibid., ESF #10-18.

133. Ibid., ESF #10-16.

134. Ibid., ESF #10-17.

135. Ibid., ESF #12-1.

136. Ibid.

137. Ibid., ESF #12-5.

138. The *National Strategy for Homeland Security* is available at Hhttp://www.whitehouse.gov/homeland/bookH. This strategy serves as the basis for the following paragraph, and The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets is available at http://www.whitehouse.gov/pcipb/physical.html, which provides the basis for the material discussed in the second paragraph of this section. Colonel Robert Stephan USAF, retired, served on the senior executive staff for infrastructure protection on the Department of Homeland Security team and lectured at the Air War College AY 2002-2003 in the Homeland Security Elective course.

139. "Gulf Safety Committee (GSC)." On-line. Internet, 18 November 2002. Available from http://www.uscg.mil/hq/g-m/harborsafetyGulf%20 Safety%20Committee.htm.

140. GSC meeting notes thus far are available on-line at Hhttp://www.uscg.mil/hq/g-mH.

141. Matt Gresham, "New Terror Alert Aimed at Oil-and-Gas Facilities," *The Courier*, 23 October 2002, 2-3. On-line. Internet. Available from http://www.houmatoday.com/news/stories/16089001003n6.html.

142. Gresham, 3.

143. *The National Strategy for Homeland Security*, Office of Homeland Security, July 2002, 68.

144. Ibid.

145. U.S. Coast Guard Fiscal Year 2003 Budget. On-line. Internet, 26 November 2002. Available from http://www.house.gov/transportation/cgmt/03-07-02/03-07-02memo.html, 6.

146. Ibid.

147. Ibid.

148. "U.S. Coast Guard News and Events," 2. On-line. Internet, 26 November 2002. Available from http://www.uscg.mil/news/homeland_security/homeland_security.html.

149. Ibid.

150. U.S. Coast Guard Fiscal Year 2003 Budget, 4.

151. Ibid.

152. Paula Shaki Trimble, "Coast Guard Floats Deepwater Ideas," *Federal Computer Week*, 27 April 2000, n.p. On-line. Internet, 19 January 2003. Available from Hhttp://www.fcw.comH.

153. U.S. Northern Command's web site notes "U.S. Northern Command's area of operations (AOR) is America's homefront." The AOR includes air, land and sea approaches and encompasses the continental United States, Alaska, Canada, Mexico, and the surrounding water out to approximately 500 nautical miles. It also includes the Gulf of Mexico, Puerto Rico and the U.S. Virgin Islands. The defense of Hawaii and our territories and possessions in the Pacific remain the responsibility of U.S. Pacific Command." From "Who We Are—Homefront," *U.S. Northern Command*, n.p. On-line. Internet, 10 December 2002. Available from http://www.northcom.mil/index.cfm?fuseaction=s.whoweare&section=4. Prior to the fairly recent creation of NORTHCOM, U.S. SOUTHCOM had responsibilities for operations within the Gulf of Mexico. Effective March 2003, the Homeland Security Department has control of the U.S. Coast Guard, which previously had been within the Department of Transportation.

154. Airman 1st Class Ann Marie Santa, "Joint Forces Counter Simulated Cruise Missile Threat," *Release No. 01121*, Official Air Force Reserve Command Public Access Web Site, 1-3. On-line. Internet, 16 December 2002. Available from http://paweb.jcs.mil/htdocs/afrcnews/01121.htm.

155. The Joint Surveillance System (JSS) provides command, control and communications (C3) capability in support of NORAD's (North American Aerospace Defense) Atmospheric Tactical Warning and Attack Assessment (ATW/AA) air sovereignty, and air defense requirements. Source: Unclassified "Department of the Air Force RDT&E Descriptive Summaries for Fiscal Year 2002 Amended Budget Submission," Volume III, June 2001, Exhibit R-2 (PE 0102325F), page 1 of 5 pages.

156. A turf battle has been playing out on the issue of available electromagnetic spectrum for Joint Surveillance System (JSS) defensive radars; while the FAA and USAF would like to preserve the bandwidth necessary to make JSS radars "jam-proof" and provide the required detailed coverage, the U.S. Government has sold/intends to sell electromagnetic bandwidth that encroaches on the JSS system—another example of "competing interests or seams" in how the U.S. deals with security issues.

157. "Air Combat Command Fact Sheet." On-line. Internet. Available from http://www2.acc.af.mil/library/factsheets/tars.html, 1.

158. NORAD TARS Briefing, Fall 2002, Microsoft Powerpoint.

159. Ibid.

160. "Weekly Piracy Report," 11-17 March 2003, courtesy of International Chamber of Commerce, ICC Commercial Crime Services, with more information available at http://www.iccwbo.org, np. SHIPLOC also maintains a web site.

161. Robert Kupperman, *Facing Tomorrow's Terrorist Incident Today*, Washington, DC: U.S. Department of Justice, Law Enforcement Assistance Administration, 1977, as quoted in Grant Wardlaw, *Political Terrorism*, Second Edition. Cambridge: Cambridge University Press, 1989, 26.

CHAPTER 6

Computer Network Defense: Department of Defense and the National Response

James M. Jenkins

Ground Zero in Cyberspace

> *Cyberspace is the battlefield of tomorrow…instead of confronting us head-to-head on the traditional battlefield, adversaries will confront the U.S. at its point of least resistance—our information.*
>
> —Senator Fred Thompson

Assault on the Information Infrastructure

0200, Day 1. Network operations centers on the east and west coasts of the United States are receiving a continual stream of inputs reporting their constituent mail servers are shutting down, from an apparent denial of service attack. Similar activities are noted throughout the Federal sector at U.S. Government agencies nationwide. The Department of Defense Computer Emergency Response Team monitoring capabilities report that military intrusion detection system data indicates Department of Defense firewalls and routers are experiencing millions of hits on a targeted port range, mail servers are rapidly becoming overtaxed, and grinding to a halt under the load. In an attempt to contain the outbreak, the Department of Defense Computer Network Operations authorities direct all installations to electronically isolate themselves from the Internet.

By 0800, the impact is widespread and felt throughout the United States. Initial examination by computer scientists indicates the offender is a combination Internet "worm" and "virus," exploiting a common scripting mechanism as the means of attack and propagation. Further, there are at least 15 reported variants of the

worm – each possessing a common underlying software architecture, but displaying discernible distinctions in the precise mechanism of attack. Computer security experts believe this attack may be the result of an "adaptive," or "polymorphic" virus.[1]

0900, Day 1. The Internet worm is spreading rapidly and has affected commerce, inhibiting Wall Street economic data communications and electronic commerce transaction capabilities. By 1130, operations are severely impacted on all networks accessing the various stock exchanges. By mid-afternoon, major segments of the U.S. business and Federal sectors are effectively shut down. Computer security experts have now identified over 200 variants of the worm, confirming it as the worst possible scenario to defend against – an ingeniously devised, maliciously inserted polymorphic worm. In addition, during the night the Metropolitan Area Exchange East, Metropolitan Area Exchange Central, and Metropolitan Area Exchange West Internet switching nodes and the Internet domain naming system experienced highly sophisticated electronic attacks and their communications throughput has been reduced to approximately 5 percent of normal levels—effectively grinding the Internet to a halt.[2]

0700, Day 2. With mounting pressure from business, state, and Federal agencies, the President's Critical Infrastructure Protection Board convenes an emergency meeting to discuss the growing crisis, and formulate a recommendation to the President for how the nation should respond. After their meeting, the recommendation is made that due to the severity, widespread effects, and escalatory nature of the attack, immediate measures must be taken to protect critical infrastructures and prevent further spread of the virus.

Is such a scenario plausible? How widespread would the impact be to the nation? Which Federal agency has the capability and mandate to lead the national response, and direct the actions required for its implementation?

This chapter will explore the answers to these questions, within the context of methodologies employed to defend the United States' National Information Infrastructure. First, threats to the National Information Infrastructure will be examined, along with the implications posed by those threats. Next, the national policy relative to cyberspace security and the information infrastructure, organizations with roles in its defense, and technological approaches for defending the infrastructure will be analyzed.

These elements will be examined to determine their effectiveness in providing an adequate national defensive posture. Finally, recommendations will be offered to buttress the overall national computer network defense strategy, to include an expanded role for the Department of Defense.

Threats to the National Information Infrastructure

> *We cannot and must not make the mistake of assuming that terrorism is the only threat. The next threat we face may indeed be from terrorists, but it could also be cyber war, a traditional state-on-state conflict, or something entirely different.*
>
> — Secretary of Defense Donald Rumsfeld

Defining the Context

Information and the infrastructure through which it traverses are ubiquitous in America, touching virtually every segment of national endeavor to some degree. This combined national information infrastructure facilitates commerce, education, government administration, national defense, recreation, and a multitude of other types of information exchange. This aggregate national information infrastructure has been defined as:

> [T]he nationwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users. The national information infrastructure encompasses a wide range of equipment, including cameras, scanners, keyboards, facsimile machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, networks of all types, televisions, monitors, printers, and much more. The friendly and adversary personnel who make decisions and handle the transmitted information constitute a critical component.[3]

A closely related and associated term becoming increasingly familiar to most Americans is "cyberspace," the notional environment in which digitized information is communicated over computer networks.[4] Cyberspace may be thought of as simply the medium through which information is conveyed via the information infrastructure from originator to recipient.

The nation's growing dependence on its information infrastructure was highlighted by a 2001 survey conducted by the U.S. Department of Commerce. The survey concluded that 143 million Americans (about 54 percent of the population) use the Internet – an increase of 26 million in 13 months. Forty-five percent of the on-line population uses electronic mail, and 39 percent of these on-line users make Internet purchases. These usage trends are likely to continue, as the number of Internet users is expanding at the rate of two million per month.[5] Information technology is equally entrenched in the American workplace, with 48 million Americans using Internet connected computers at work.[6]

Similar dependence exists within the national defense establishment. The Department of Defense uses globally connected information systems and networks to support all aspects of military operations, and they comprise an essential element in enabling commanders to achieve information and decision superiority. In addition, these information systems, technology, and networks are integral elements in transforming the Department of Defense to meet the anticipated demands of future warfare.[7] However, America's increasing dependence on information technology and networked computers is a double-edged sword. Our dependence engenders the creation of accompanying vulnerabilities to a wide spectrum of threats that may seek to disrupt, deny, degrade, destroy or deceive critical information or information systems.[8]

Characterization of the Threat

Threats to interconnected computer systems are continually evolving and increasing in sophistication, complexity, and scope. The major threats identified in unclassified sources reviewed in this analysis include those posed by criminal groups, foreign intelligence services, hackers or hacktivists, virus writers, insider threats, and information warfare of state and non-state origin.[9]

Criminal threats are those threats perpetrated by criminals, primarily for the purpose of financial gain. In a broader sense, criminally oriented attacks against computer systems may encompass the full spectrum from fraud, scams, destructive attacks, identity theft, or theft of intellectual property.[10] Foreign intelligence services use Internet tools as part of their ongoing collection efforts, targeted in particular against open societies such as the United States where large amounts of information are readily available and sometimes afforded limited protection.

Conversely, hackers pose an entirely different type of threat. Hackers probe and attack systems simply because they exist, and they possess the wherewithal to penetrate them. Hactivists are attackers who execute politically motivated attacks against public web sites or e-mail systems, to promote their particular interests or agenda. Virus writers develop and maliciously introduce software via the Internet designed to destroy files, disrupt systems, or deny services to infected systems and networks. Viruses can cause extensive damage to information in automated systems, and may have significant economic impact caused by lost productivity and actions required to repair infected systems.

The impact of virus threats received worldwide attention in 2001, when the Code Red virus attack infected one million systems, creating an estimated $2.6 billion worldwide economic impact.[11] However, insider threats constitute approximately 70 percent of all cyber attacks, and represent the threat posed by insiders – authorized users of computer systems who may strike at their employers through destruction, corruption of information, or theft of intellectual property.[12] Finally, an emergent and significant threat is posed by the possibility of state and non-state actors waging offensive information warfare against U.S. systems or networks. In testimony before the U.S. Senate, George J. Tenet, Director of Central Intelligence, observed the significance of this threat:

> "…[A]s this century progresses, our country's security will depend more and more on the unimpeded and secure flow of information. Any foreign adversary that develops the ability to interrupt that flow or shut it down will have the potential to weaken us dramatically or even render us helpless…already, we see a number of countries expressing interest in information operations and information warfare as a means to counter U.S. military superiority. Several key

> states are aggressively working to develop their information warfare capabilities and to incorporate these new tools into their war fighting doctrine."[13]

The spectrum of threats from these sources poses significant challenges to defending the National Information Infrastructure from attacks of both internal and external origin. In addition, successful penetrations and attacks against the infrastructure may have significant economic, operational, and national defense implications.

Implications of Attacks

Cybercrime is alive, well, and doing *big* business in America. The Computer Security Institute's 2002 Computer Crime Survey reported 90 percent of its corporate respondents experienced computer security breaches during that year. Eighty percent of those breaches resulted in lost revenue, with aggregate dollar losses of $455,848,000.[14] Electronic attacks of this nature have the potential to not only cause significant initial impact from containment and eradication actions, but even greater potential downstream impact from second and third order effects resulting from the interruption of supply chains, business loss, and possible decline in stock prices.[15]

In contrast, threats posed by information warfare attacks against the military portion of the Internet, the Global Information Grid, and its interconnected systems, have potential to disrupt, deny, degrade, destroy or deceive information systems and networks, adversely impacting national defense.[16] The United States military is heavily dependent on technology-rich weaponry, most of which requires the collection, processing, and transmission of data in some form. Information warfare directed against U.S. systems and networks would have the aim of denying information needed for military operations.

This type of warfare could encompass a variety of forms ranging from electronic warfare, psychological operations, deception techniques, offensive computer network attack, to physical destruction of U.S. command and control nodes.[17] In addition, as U.S. military doctrine espouses concepts of offensive information warfare, it is logical to assume our potential adversaries are incorporating similar concepts into their strategic, operational, and tactical warfighting doctrine. The asymmetrical

possibilities inherent in information-based warfare have not escaped the Chinese, whose Army newspaper *Jiefangjun Bio* reported:

> After the Gulf War, when everyone was looking forward to eternal peace, a new military revolution emerged. This revolution is essentially a transformation from the mechanized warfare of the industrial age to the information warfare of the information age. Information warfare is a war of decisions and control, a war of knowledge, and a way of intellect. The aim of information warfare will be gradually changed from "preserving oneself and wiping out the enemy" to "preserving oneself and controlling the opponent." Under today's technological conditions, the "all conquering stratagems" of Sun Tzu more than two millennia ago--"vanquishing the enemy without fighting" and subduing the enemy by "soft strike" or "soft destruction"—could finally be truly realized.[18]

To counter these potential threats to the nation's information infrastructure, an extensive and growing policy, organizational, and technological framework exists. This framework constitutes the strategic foundation harnessing national resources in response to these threats.

Approaches for Defending the National Information Infrastructure

> *We have evidence that a large number of countries around the world are developing the doctrine, strategies, and tools to conduct information attacks on military-related computers.*
>
> —John M. Deutsch, Director, CIA

Strategic/National Level Framework

The national policy and organizational framework for computer network defense has undergone virtually continuous evolution since the mid-1990s. In addition, the tragic 9/11 attacks against the Pentagon and World Trade Center further crystallized interest in protecting critical infrastructures, spawning a surge of new legislation, organizations, and

interest in supporting technologies. Understanding of the national strategic defensive framework requires an examination of the extensive mosaic of underlying policy. Table 6.1 provides a chronology of key policy instruments related to defense of the National Information Infrastructure.

Executive Order 13010 began the process by establishing the President's Commission on Critical Infrastructure Protection that conducted its initial examination into the state of critical national infrastructures, including the information infrastructure, and submitted its first report in 1997. This concluded that America's technology dependence rendered it vulnerable to cyber-threats, identified a "lack of awareness" within the government concerning the existence and severity of this threat, and concluded national defensive measures should be a cooperative effort between the public and private sectors.[19]

Table 6.1 Key Infrastructure Protection Legislation

Legislation	Year	Issue
Executive Order 13010	1997	Defined critical infrastructures; established President's Commission on Critical Infrastructure Protection
Presidential Decision Directive 63	1998	Established infrastructure protection as national goal, Critical Infrastructure Protection Office, NIPC within FBI, structure for liaison and coordination
National Plan for Infrastructure Protection	2000	Focused Federal efforts, required vulnerability assessments, defined Federal government to be model for security, linked funding approvals to information security plans
Executive Order 13231	2001	Established President's Critical Infrastructure Protection Board to coordinate Federal efforts with protecting national infrastructures; 10 standing committees to support board
Executive Order 13228	2001	Established Office of Homeland Security to develop comprehensive strategy to secure U.S. from attacks
National Strategy to Secure Cyberspace	2002	Established collaborative implementing strategy to secure U.S. information systems against attack

Source: Arnaud de Borchgrave, et al. *Cyber Threats and Information Security: Meeting the 21st Century Challenge* (Washington, D.C.: The Center for Strategic and International Studies (CSIS), 2000), 56-59.

In 1998, Presidential Decision Directive (PDD) 63 established information infrastructure protection as a national goal, defining milestone dates for the year 2000 to achieve an initial operating capability, and 2003 for full protective capabilities. In addition, PDD 63 established two agencies integral to nationwide infrastructure defensive efforts, the Critical Infrastructure Assurance Office in the Department of Commerce, and the National Infrastructure Protection Center within the Federal Bureau of Investigation. The former organization's charter was to craft a national plan for infrastructure defense, while the latter focused on warning, assessment, law enforcement investigation, response, and reconstitution monitoring.[20] Other significant tenets of PDD 63 were establishment of the National Infrastructure Assurance Council to facilitate private and public sector cooperation, partitioning of the infrastructure into segments with lead responsible agencies, and a structure for information exchange on threats. Within this portioning plan, the Department of Defense was established as the lead agency for the special function of national defense.[21]

In 2000, having just grappled with the Year 2000 (Y2K) computer problem, the White House released the next element of the national policy framework, the National Plan for Infrastructure Protection, which further focused Federal efforts, established additional milestones, required vulnerability assessments for each segment of the infrastructure, and made security a criteria for sustaining program funding. In addition, this plan also directed the establishment of a national warning center for infrastructure attacks.[22]

Executive Order 13231, enacted in October 2001, established the President's Critical Infrastructure Protection Board, chaired by the Special Advisor to the President on Cyberspace Security. This board "coordinates cyber-related Federal efforts and programs," with the assistance of ten supporting committees. An additional responsibility of the President's Critical Infrastructure Protection Board is coordination with the Office of Homeland Security on issues related to attacks against the U.S. information infrastructure.[23]

The latest and most significant evolution in the national policy for defending the information infrastructure is the February 2003 *National Strategy to Secure Cyberspace*. This document serves as an overall

strategy for synergistically integrating efforts of the previously mentioned initiatives. Its overall purpose is to provide:

> [A]n implementing strategy, which supports both the *National Strategy for Homeland Security* and the *National Security Strategy of the United States.* The *National Strategy to Secure Cyberspace* describes initiatives to secure U.S. information systems against deliberate, malicious disruption and to foster an increased national resiliency. This strategy, together with the complementary *Homeland Security Physical Protection Strategy*, provides the strategic foundation for the nation's efforts to protect its infrastructures.[24]

Development of *The National Strategy to Secure Cyberspace* represents a collaborative effort between Federal and private sector lead agencies, and provides specific recommendations for each major infrastructure segment. In addition, two key themes of the strategy are: (1) the need for coordinated, voluntary partnerships among infrastructure segments to defend the information infrastructure, and (2) strengthening Federal information security to make it a model for other infrastructure segments.[25]

This extensive body of policy and organizations provides a basic structure for management and defense of the national information infrastructure. Similarly, the underlying technological framework provides the flesh and blood, giving our national defensive capability its substance.

Computer Network Defense Supporting Technology

The technological foundation supporting the defense of the information infrastructure is comprised of a complex array of physical, electronic, software, and procedural elements. While a detailed discussion of the technological underpinning of computer and network security is beyond the scope of this chapter, the elements most commonly used in both the private and public sectors will be briefly examined.

Physical defensive measures include those actions taken to prevent unauthorized users from obtaining physical access to computer equipment and networks. These measures also include the use of passwords for authorized users to gain access, along with newer, emergent technologies such as biometrics, which may include handwriting, voiceprints, face recognition, or fingerprints to identify authorized users.[26]

Electronic measures include the use of firewalls, which function as electronic barriers between local area computer networks and the Internet. Another widely employed electronic measure is the virtual private network, a secure connection over a public network. Serving to provide continuous electronic surveillance over a network, intrusion detection systems serve as burglar alarms, monitoring networks to detect potential attacks. Combined with vulnerability scanners, which provide a self-help tool to detect vulnerabilities, these two capabilities are employed by virtually all major private sector enterprises and Department of Defense installations as key elements of their defensive posture.[27]

Software defensive measures include security features built into the design of operating systems such as *Microsoft Windows*, and applications software providing security functionality such as anti-viral software. However, a significant number of vulnerabilities are created by software design defects. The industry average software development error rate is typically five to fifteen errors or "bugs" for each thousand lines of computer code written.[28] Each of these errors is a potential security risk that may be exploited. To prevent exploitation of these vulnerabilities, software manufacturers release updates, patches, or service packs, which normally require manual installation by systems support personnel. Installation of these patches represents a significant expenditure of time and effort to sustain adequate security.[29]

Finally, procedural elements such as local security policies, and user training and awareness programs, are important parts of the overall defensive framework. Security policies address the organizational rules of engagement for computer and network security and proper use of these systems. These programs are essential, as even the best policies and supporting technological tools are of marginal value unless coupled with effective training programs.

Effectiveness of National Information Infrastructure Defensive Measures

> *Our challenge in this new century is a difficult one. It's really to prepare to defend our nation against the unknown, the uncertain and what we have to understand will be the*

> *unexpected. That may seem on the face of it an impossible task, but it is not. But to accomplish it, we have to put aside the comfortable ways of thinking and planning, take risks and try new things so that we can prepare our forces to deter and defeat adversaries that have not yet emerged to challenge us.*
>
> —Secretary of Defense Donald Rumsfeld

Thus far, key policy, organizational, and technological components employed to defend the National Information Infrastructure have been examined. In this section, the effectiveness of these elements will be scrutinized to assess their adequacy in providing adequate defense of the information infrastructure.

Evaluation Criteria

The metrics used to establish benchmarks to assess the effectiveness of computer network defense measures are: (1) recent findings from investigations conducted by the United States General Accounting Office (GAO), (2) network incident data collected and reported by the Carnegie-Mellon University Computer Emergency Response Team, Coordination Center, (3) field interviews and discussions conducted as part of the research for this chapter, and (4) the personal experiences of the author as an Air Force communications squadron commander, systems/database administrator, and organizational director of technology.

GAO Audit Findings

The GAO report titled, *Critical Infrastructure Protection: Significant Challenges Need to be Addressed*, provides a comprehensive assessment of the overall state of the nation's ability to protect its critical infrastructures.[30] This report summarizes previous GAO efforts pertinent to infrastructure security, identifying four major areas requiring improvement: (1) the lack of a national cyber and physical critical infrastructure protection strategy; (2) the need for improved analysis and warning capabilities; (3) the need for improved information sharing within the federal government, and between the federal government, private sector, state and local governments; and (4) persistent pervasive weaknesses in Federal computer systems.[31]

1. Lack of a national cyber and physical critical infrastructure protection strategy. Due in large part to the events of 9/11 significantly elevating national awareness of vulnerabilities to our critical infrastructures, some progress has been made in this area since the GAO audit. The aforementioned *National Strategy to Secure Cyberspace*, an overarching strategy for information infrastructure protection efforts, was published in February 2003.

However, GAO did not address one of the most pronounced shortcomings of the strategy. Although the document will no doubt meet the letter of the law in providing a national strategy, it unfortunately suffers from the notable deficiency of being a "paper tiger," lacking any statute authority to direct implementation of its numerous recommendations.

This unfortunate result directly stems from PDD 63 itself, which calls for only *coordinating* authority, and *encouraged* participation, by private sector infrastructure segments. While these are worthwhile goals, it is unclear if private sector infrastructure segments will voluntarily submit to its recommendations for securing their networks and systems if a substantial expenditure of resources is required. However, our increasing vulnerability points to the need for a more structured management approach. The overall effects of the national strategy would be enhanced by some degree of underlying *mandated* compliance combined with a program of private sector compliance incentives to ensure minimum standards for nationwide security.

2. Need for improved analysis and warning capabilities. Similarly, The National Infrastructure Protection Center, operated by the FBI, was chartered under PDD 63 as the nation's nerve center for warning and assessment for infrastructure protection, and is empowered to issue warnings and *guidance* to owners and operators of critical infrastructure components. However, that organization's effectiveness has been hampered by the lack of an analytic framework with which to assess strategic infrastructure attacks, personnel shortages, and limited nationwide understanding of its intended purpose.[32]

Once again, GAO described the symptom, but only partially identified the underlying cause. The lack of statute authority to direct actions be taken in response to significant threats is a key deficiency in establishing a viable national defense structure. The absence of an

underlying statutory standards framework for key infrastructure components is a substantial deficiency, which must be resolved.

3. Need for improved information sharing. The GAO also observed that additional emphasis is needed to enhance sharing of information between and among Federal and private sector organizations. This issue has historically been problematic, as commercial enterprises are often reluctant to admit that they have experienced a network penetration or attack. While the FBI has expanded its capabilities to detect and respond to infrastructure attacks, particularly those with suspected criminal intent, their efforts will be of limited value without an open and unrestricted information flow from the private sector.[33] Although additional dialogue is needed, mechanisms must be established for promoting the free flow of information, while addressing private sector concerns for reporting anonymity.

4. Persistent pervasive weaknesses in Federal computer systems. GAO auditors identified the need for improvements and an overall strategy to resolve security weaknesses in Federal computer systems. The GAO viewed a central aspect of this problem as the lack of an overarching security strategy within the federal government, coupled with often-unclear roles and responsibilities.[34] As discussed earlier, the *National Strategy to Secure Cyberspace* provides at least an initial starting point for an integrative Federal strategy, but must be coupled with corresponding security programs within each agency to resolve their respective deficiencies.

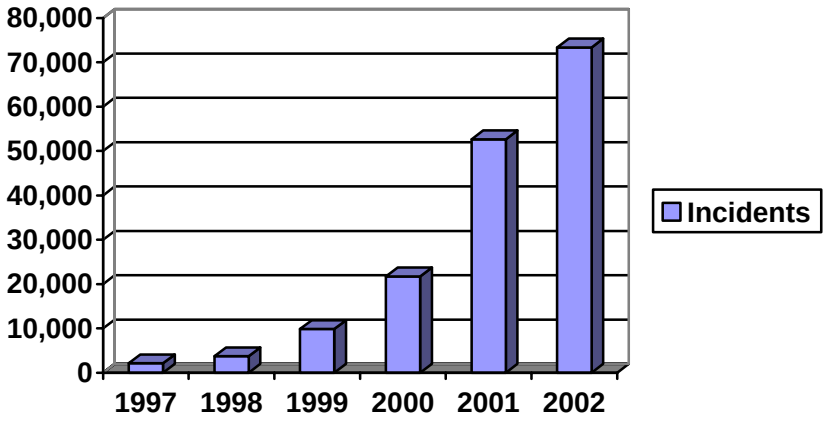
5. Other issues. GAO also observed that while approximately 50 organizations exist with roles in critical infrastructure protection, not all critical infrastructures were represented by these organizations, and the roles of the various agencies are not widely understood.[35] However, the GAO again stopped short of identifying a critically important aspect for strategic defense of the information infrastructure—unity of command. While there are many agencies involved in infrastructure protection, there is no *single* agency with the mandate to act *authoritatively* and *decisively* in the event of a significant crisis or attack on the national information infrastructure. PDD 63 tasks the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, who reports to the President through the Assistant to the President for National Security

Affairs, with overall PDD 63 implementation, but specifically states this individual "*will not direct* Departments and Agencies."[36] To resolve these deficiencies, a single Federal agency should be designated with the charter and tools for providing strategic direction to the national infrastructure defensive effort, to include prevention, detection, characterization, and response to assaults.

Network Incident Data

In addition to deficiencies that must be resolved in the current national policy and organizational structures, existing infrastructure defensive strategies, as measured by the incidence of reported attacks, are ineffective and require significant improvement. Figure 6.1 summarizes incidents reported to the Computer Emergency Response Team during the years 1997 through the third quarter of 2003.

Figure 6.1 Computer Emergency Response Team (CERT) Incident Data, 1997-2003



Source: CERT Coordination Center Statistics 1988-2003, http://www.cert.org/stats/cert_stats.html

As depicted in Figure 6.1, the number of reported network incidents has increased exponentially since 1997 when the inaugural national initiatives for information infrastructure protection began. In addition, the Computer Emergency Response Team estimates that up to 80 percent of all incidents go unreported.[37] In spite of increased awareness, widespread availability

of threat information, a substantial number of organizations involved in promulgating infrastructure security information, and technical means to mitigate the impact of most threats, these collective measures have not produced a corresponding decline in incidents. The reasons for this situation are twofold. First, there are simply more information systems, networks, and vulnerabilities to contend with each year. Second, in the absence of statutes mandating their implementation, available protective measures are not universally employed. The Business Software Alliance's July 2002 survey of information technology professionals indicated even common tools, such as anti-viral software and password changes, were not universally used and security updates were not regularly made.[38]

Finally, even though the events of 9/11 raised awareness and resulted in some infrastructure security improvements in the U.S., this trend has been far from universal. An August 2002 SearchSecurity.com survey of 500 corporate security and IT personnel reported more than half of the surveyed organizations have seen *no* improvement in their organization's security posture since the attacks of 9/11.[39] Although the trend is better in the Federal sector, with 71 percent of Federal agencies reporting improved security, 29 percent indicated no significant improvements had occurred in their agencies since 9/11.[40]

Field Interviews and Discussions

During my research for this chapter, I had the pleasure of discussing views on protection of the National Information Infrastructure with several private sector and Federal subject matter experts. One of these experts was Mr. Steve Goldsby, Chief Executive Officer of Integrated Computer Solutions, Inc., a Certified Information Systems Security Professional who draws upon an extensive information security background in both the Federal and private sectors.[41] He observed that *substantial* increases in an organization's information security posture are typically achieved through an iterative process whereby an organization's security status is assessed, and basic technological elements such as firewalls, intrusion detection systems, anti-viral software, and security policies are implemented.

Further, Mr. Goldsby believes that a greater degree of synergy and leveraging of strengths of both the private sector and public sector can be achieved. One of the private sector's key strengths, according to Mr. Goldsby, is "the ability to deliver tailored solutions quickly" to meet the

information security needs of organizations. He observes that the most promising method by which the federal government can stimulate private sector development and deployment of enhanced security technologies needed to buttress information infrastructure defense is through more Federal grants for basic research.[42] Both of these areas are promising and have significant potential for improving overall infrastructure security, could be integrated into an overall public-private sector partnership program, and should be the subject of further research.

In addition, during the development of this chapter, this author's research period for this project coincided with the August 25-29, 2002, Air Force Information Technology Conference, held at the Montgomery Civic Center, in Montgomery, Alabama. At this event, representatives from many of the nation's premier information security technology providers were on-site, exhibiting the latest information security technologies. Virtually all of these vendors offered off-the-shelf security solutions comprised of variants of the basic technological building blocks that have been discussed earlier in this chapter. Consequently, organizations desiring to design a defensive strategy enhancing their security posture have a wealth of private sector resources to draw upon.

Personal Experiences

Based on over two and a half decades of practical experience in information technology, coupled with analysis of available data compiled during research for this project, this author's assessment is that the overall state of National Information Infrastructure security, although marginally improved during the last decade and showing increased emphasis since 9/11, requires additional systematic attention to afford adequate protection to this critical national resource. In this regard, while the GAO recommendations discussed earlier did not go far enough in some areas, their overall observations correctly captured the most significant issues adversely affecting infrastructure defense.

From this author's direct observations and experience in the Air Force computer network operations environment, it is clear that the most significant problems which must be resolved are those of: (1) "human capital," sustaining and equipping an adequately trained computer operations technical force, and (2) following a path of disciplined, systematic utilization of available technological tools.

First, military manpower shortages and increasing military operations tempo create significant challenges for understaffed network operations centers to sustain day-to-day operations. Additional research is needed to determine possible solutions to this problem, e.g., bonuses, incentives, privatization, etc.

Second, Air Force organizations for the most part have the *basic* technical tools needed to secure the military's portion of the national information infrastructure. Unfortunately, the areas not addressed by these tools continue to create problems. An area where this is particularly problematic is that of security update/patch management. And while some installations have partially automated this process, and General Services Agency contract vehicles for patch management are now available, more adaptive, less manpower intensive automated tools are needed.[43]

Overall, although implementing legislation and organizations have been in existence since 1997, and most of the required technical means are available to design a satisfactory defensive architecture, additional emphasis is needed in both the private and Federal sectors to elevate National Information Infrastructure defense to the level it warrants.

Recommendations

While our nation has begun the journey to secure its critical infrastructures, we have not yet reached the destination. In view of the significant changes occurring throughout the federal government since 9/11 to buttress infrastructure security of all types, we are at a key juncture to implement additional improvements building upon those already taken. The recent creation of the cabinet level Department of Homeland Security holds great promise to simplify the consolidation, streamlining, and simplifying of the national structure for critical infrastructure defense against both physical and electronic attack. In addition, a tremendous potential for private and public sector synergism exists, which if exploited could result in significant improvements in the nation's infrastructure defense. To implement these improvements, five recommendations are suggested, expanding upon and providing solutions to the problems framed by the GAO—resolving structural, indications/warning, information sharing, and overall systemic security deficiencies.

Recommendation 1: Establish a single agency for information infrastructure defense

Changes are required to the current organizational framework for protection of the National Information Infrastructure. As addressed earlier, there are currently some 50 organizations with roles in infrastructure protection, and broad agreement exists that a central entity is needed to achieve unity of effort.[44] No evidence was found that any *single* agency has the statute authority to direct the scope of actions that would be required to mount the defense to a strategic assault on the information infrastructure.[45] This would cause confusion, delay, and unpredictable outcomes in the event of a scenario such as this chapter posited in its opening paragraphs. In light of its role in protecting the nation, a logical candidate for this function would be the new Department of Homeland Security. Designation of this agency for this role would consolidate response actions for infrastructure protection within one agency, engender unity of action in the event rapid response is needed to react to strategic level events, and provide one universally recognized governmental organization for private sector interface and coordination.

Recommendation 2: Establish a baseline regulatory environment

Thus far, the Internet has largely been unregulated, decentralized, and relatively unconstrained by government intervention or regulation. However, the increasing inability to prevent, contain, and adequately respond to information infrastructure threats and vulnerabilities warrants more scrutiny, and at least minimal implementation of nationwide guidelines. Improvement is needed in two major areas: (1) the provision of a common set of computer and network security standards applicable to all segments of the national infrastructure, and (2) guidelines specifying minimum security requirements for core Internet service providers.

Currently, there are multiple sources of standards that organizations desiring to enhance their security posture may consult to obtain guidance. Some have their origins in the federal government; others from a variety of private sector security organizations. An initiative promising to provide a set of common standards, NIST Special Publication 800-37, "Guidelines for the Security Certification and Accreditation of Federal Information Technology Systems," was released October 28, 2002, under the auspices

of the National Information Assurance Partnership. The Partnership is a joint effort of the National Institute of Standards and Technology (NIST) and the National Security Agency to meet the security testing, evaluation, and assessment needs of both information technology producers and consumers. The goal of the project is to provide a clear, step-by-step roadmap for agencies to develop and implement enterprise security programs and certification processes.[46] These standards should be evaluated for possible mandated use not only within the federal government, but also as required performance standards for agencies desiring to transact business with government agencies.

There are currently over 4,000 active Internet service providers and over 165,000 Internet points of presence registered in the U.S. and Canada, forming the bulk of the domestic information infrastructure.[47] These Internet service providers operate under varying, self-regulated degrees of security, and require some measure of foundational security standards to guard the overall integrity of the domestic backbone network. The reasons for this are twofold: first, it is unlikely that each of the 143 million private citizens connected to the Internet can or will implement appropriate security controls (firewalls, anti-viral software, security patches, etc.) on their home personal computers. However, proper firewalls, anti-viral software, filters, and intrusion detection devices at Internet service providers could significantly reduce the promulgation of viruses and other threats throughout the Internet, and should be mandated.

Additionally, during the course of research for this chapter, the most pervasive denial of service attack against the Internet to date was launched against the domain name server infrastructure. The domain name server architecture translates Internet plain text addresses, such as www.maxwell.af.mil, into Internet protocol addresses such as 124.45.69.2, for routing and delivery of messages across the Internet. The attack flooded all 13 servers in the worldwide network, and was reportedly launched from servers in the U.S. and Korea.[48] Due to the potential widespread disruption from this type of attack, the domain name server infrastructure should also be examined for possible hardening, additional redundancy, and included within the regulatory umbrella suggested for Internet service providers.

A workable and mutually beneficial model adaptable to information infrastructure security is found in the U.S. Environmental Protection

Agency's "Partners for the Environment Program." In this program, existing environmental law is enforced, but participation in this voluntary program benefits private sector participants via cost savings, increased profits, improved access to technical assistance, and provision of a framework for improving environmental performance. Both private and public sectors benefit through better overall environmental compliance, energy savings, and awareness. [49]

Implementation of a similar partnership program for information infrastructure security would have similar benefits and achieve the objectives delineated in the *National Strategy to Secure Cyberspace*. While it is recognized there are concerns over Internet privacy issues and increased governmental control that must be addressed, a basic foundation of standards is essential to raising the overall level of security within the information infrastructure. Additional study is needed to address these issues, devise an optimum structure for public-private interaction, and determine the type of incentives that should be employed.

Recommendation 3: Utilize Core Competencies of the Department of Defense

In consonance with the tenets of *The National Strategy to Secure Cyberspace's* theme of increased information sharing between the Federal and private sectors, great potential for synergism exists. The Department of Defense has long recognized the importance of protecting its systems, and the essential need to sustain an uninterrupted information flow to accomplish its national defense mission. Joint Vision 2020, encapsulating future joint war fighting doctrine, defines this concept as information superiority, "the capability to collect, process, and disseminate an uninterrupted flow of information while denying an adversary's ability to do the same."[50] In this regard, networks provide military forces the ability to shape the battlespace, command, and control assigned forces. Based on extensive experience of the Department of Defense, four areas of competency appear especially promising for export to other infrastructure segment protection initiatives: (1) indications and warning architecture, (2) hierarchical network management, (3) enterprise security and information assurance program management, and (4) the use of exercises.

Indications and warning architecture

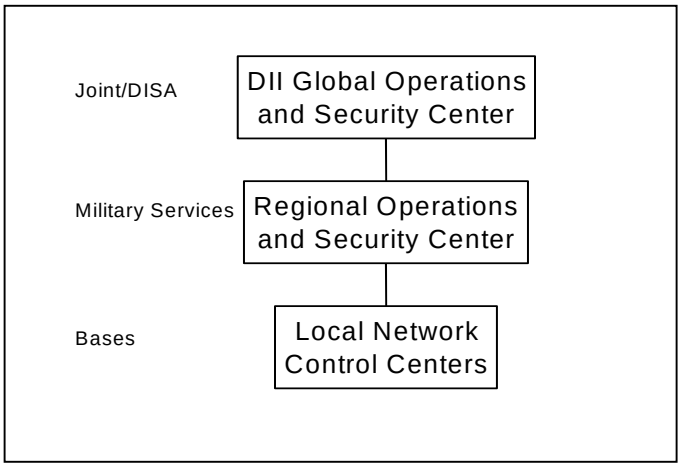
First, the ubiquitous indications and warning architecture of the Department of Defense is an important resource that should be leveraged by the Department of Homeland Security, and other infrastructure defense agencies, to provide strategic early warning. For example, in 1998 the Department of the Air Force deployed network management capabilities and base information protection tools at 109 bases. These capabilities included firewalls, scanning tools, and network management tools at main operating bases. This architecture was expanded in 2000 to include intrusion detection systems to provide indications and warning. These aggregate capabilities formed a highly effective Air Force enterprise security system--capturing on its sensor grid over 315 million suspicious connection attempts during the year 2000. This successful defensive capability allowed only one unauthorized connection by an outsider for every 20 million suspicious connection attempts.[51] This architecture has proven highly effective in detecting attempted network penetrations, and should be employed both as a data source in a centralized national control and monitoring scheme, and also as a model for other infrastructure segments.

Hierarchical network management

The *National Strategy to Secure Cyberspace* recommends the creation of a national cyberspace network operations center, to provide early detection, prediction, and response to attacks on the information infrastructure.[52] This concept should be pursued, and modeled on the experience of the network operations hierarchy successfully employed by the Department of Defense. The Pentagon's hierarchical network management structure is depicted in Figure 6.2. At the apex, the Defense Information Systems Agency's Global Operations Support Center is responsible for overall worldwide enterprise management of the Department of Defense's portion of the national information infrastructure. Aiding in overall management are regional centers located in the Continental United States, Pacific, and European theaters. The final tier consists of network control centers at each installation, which provide local operations and information assurance support. Information flows from local network control centers and regional operations centers to the global operations center, which provides overall network management

oversight of the Defense Information Infrastructure. The success of the system stems from a continual flow of information regarding the overall performance, status, and threat environment of the global network.

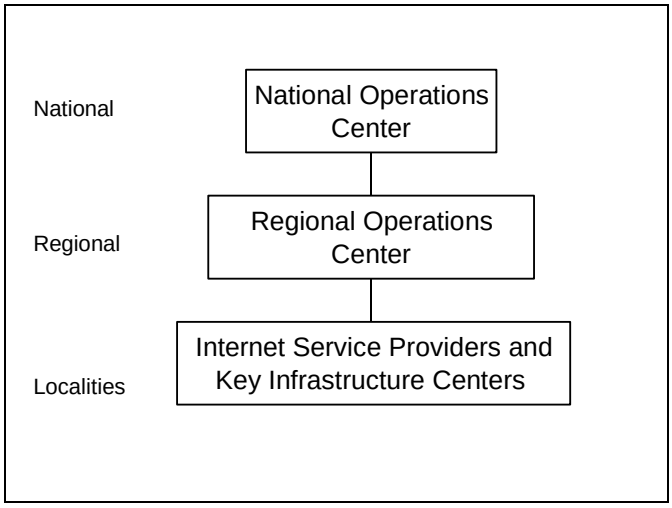
Figure 6.2 Department of Defense Network Management Structure



Source: Author's Model

A similar concept could be employed to manage the National Information Infrastructure. Figure 6.3 provides a notional view of how such a nationwide indications, warning, and response architecture might be developed. Implementation would employ a national operations center, controlled by the Department of Homeland Security and operated by one of its agencies. This national center would be equipped with the required data feeds from indications and warning capabilities, receiving these inputs from subordinate level regional operations centers, or directly from individual Internet service providers, domain name server organizations, and major Internet backbone providers. A key benefit of this architecture would be development of a capability to receive, characterize, and disseminate response actions rapidly throughout the national infrastructure.

Figure 6.3 Notional National Cyberspace Management Structure



Source: Author's Model

Enterprise Security and Information Assurance Program Management

The Department of Defense has extensive organizational information and computer security programs implemented at all levels throughout its structure. These programs address all aspects of computer security, from the definition of organizational security policies, assessment, accreditation and certification of systems, to comprehensive user training. It is likely many of these programs could in part or total be exported to other segments of the infrastructure for their use in developing enterprise information security programs.

The Use of Exercises

Finally, the use of exercises should be increased to provide a realistic environment within which to evaluate and plan responses to possible attacks on the information infrastructure. Exercises were heavily employed during national preparation for the Y2K computer event, and provide valuable experience in remediation, recovery, and contingency

planning. A pioneer effort, which could serve as a nationwide model, is the joint city, private sector, and Air Intelligence Agency "Operation Dark Screen" exercise planned by the Center for Infrastructure Assurance and Security at the University of Texas, San Antonio. Dark Screen is a three-phase exercise designed to help participants better understand how to prepare for, recover from and protect a city's critical infrastructure in case of a cyber attack. As national mentors, Department of Defense organizations should foster and increase their participation in such combined exercises with state and local governments.[53]

Recommendation 4: Build bridges between Federal, State, and Local Governments

The National Strategy to Secure Cyberspace stresses the importance of increased communication and coordination between local, state, and federal governments. The need for this strategy is essential to accomplish the collective goal of securing America's information-based resources.

While state governments in general have initiated efforts toward systems security and may use existing Federal linkages for this purpose, it is likely that local governments will require some degree of mentoring and assistance to raise their level of security. Although rudimentary means exist for the sharing of information infrastructure threats, such as Information Sharing and Analysis Centers and web sites such as the *Infraguard* site (www.infraguard.net), more effective methods are available.[54]

An excellent example upon which to employ Department of Defense mentorship and coordination with local municipalities is the Year 2000 Preparation Model. Preparation for the Year 2000 computer event was unprecedented in the history of information technology, both in America and throughout the world. Planning efforts for preparing America and its information systems for the Year 2000, or Y2K, affected every segment of the national infrastructure. Germane for purposes of this discussion are the numerous partnerships between the Department of Defense and local officials that were created to address Y2K related issues throughout the country. The author's experiences in this regard as the installation project officer at Altus Air Force Base, Oklahoma, were both challenging and rewarding. Working with the local municipality included every aspect of planning for the Y2K issue, to include "worst-case" and "what if"

scenarios. In each case, local officials were more than willing to both accept recommendations and dialogue with the Department of Defense regarding solutions for addressing contingency scenarios. Drawing upon these type partnerships that were established throughout the United States could serve as an excellent starting point for Department of Defense mentorship in infrastructure security, and could expand to include other critical infrastructure sectors such as water, electric power, transportation, and public health services. Such efforts would have the dual benefit of bolstering the defensive posture of key national infrastructures, as well as strengthening relations between the Pentagon and local governments for the common good.

Recommendation 5: Utilize Department of Defense as National Mentor

One of the central tenets of *The National Strategy to Secure Cyberspace* is that of creating an infrastructure security environment in which the federal government serves as the model for other segments of the infrastructure. Although Department of Defense's current engagement and deployment of its resources in the global war against terrorism could limit its capabilities, its long experience with securing critical information and infrastructures ideally equips it to serve as a national guide, or mentor. It is envisioned the Department of Defense could serve in this capacity through liaison with the Department of Homeland Security, until that organization is fully implemented and capable of leading the national defensive effort.

Nationally, we are at a critical juncture in light of 9/11. While terrorists are currently not employing cyberspace methods to attack the U.S., the potential asymmetrical advantage such attacks would afford cannot be discounted. Implementing improvements in the national policy structure, creating a baseline regulatory environment, leveraging Department of Defense's extensive experience, and building bridges to other infrastructure segments and governments with overall Department of Defense mentorship, promises to point America in the right direction to accomplish the goals of *The National Strategy to Secure Cyberspace.*

If the recommendations posited in this chapter stimulate discussion leading to improvements in the nation's ability to defend its information infrastructure, it is likely the fictional opening scenario concludes with a successful resolution to the postulated cyber attack as follows:

1600, Day 1. The nation quickly returned to normal after countering the potential threat from the recent attack launched against its information infrastructure. Stemming from substantial improvements to America's capability to defend its critical infrastructures incident to the establishment of the Department of Homeland Security, the National Cyberspace Operations Center, baseline security standards, and enhanced national indications and warning structure, a joint Federal-private sector response team quickly formulated a defense rendering the polymorphic "super" virus ineffective. Using the nationwide link from the National Cyberspace Operations Center to ISPs and Internet carriers, the fix was rapidly disseminated and the threat contained before any significant damage could occur. The President expressed his appreciation to the Special Advisor for Cyberspace Security, the Departments of Defense and Homeland Security, and all members of the infrastructure protection team for the success of the effort.

In conclusion, America has been given a rare opportunity in modern warfare, the chance to prepare itself for an asymmetrical assault that is all-but-certain to come on a future electronic battlefield. With an effective national strategy, coupled with synergistic public and private sector effort, we will transform ourselves to ensure that America is ready for the challenges of 21st century information-realm warfare.

Notes

1. Polymorphic viruses are those viruses that reproduce themselves in a different manner each time they infect a system, greatly complicating eradication efforts. On-line. Internet. Available from http://antivirus.about.com/library/glossary/bldef-poly.htm.

2. The MAEs (Metropolitan Area Exchange) are large Network Access Points to the Internet. On-line. Internet. Available from http://www.cknow.com/ckinfo/acro_m/mae_1.shtml.

3. Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 7 May 2002, 294.

4. Ibid., 114.

5. *"A Nation Online: How Americans Are Expanding Their Use of the Internet,"* February 2002, Executive Summary. On-line. Internet, 26 September 2002. Available from Hhttp://www.ntia.doc.gov/ntiahome/dn/html/anationonline2.htmH.

6. Ibid., Chapter 6.

7. Air Force Doctrine Document 2-5, *Information Operations*, defines information superiority as "that degree of dominance in the information domain which allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition." In addition, two of the six 2001 QDR goals relative to Defense Transformation are directly linked to the application of information technology. See Deputy Secretary of Defense Paul Wolfowitz's *Prepared Statement to the Senate Armed Services Committee Hearing On Military Transformation*, 9 April 2002. On-line. Internet, 28 September 2002. Available from http://www.defenselink.mil/speeches /2002/s20020409-depsecdef2.html.

8. Air Force Doctrine Document 2-5, Information Operations, 4 January 2002, 7.

9. Joint Publication 3-13, *Joint Doctrine for Information Operations*, 9 October 1998, I-15. Additionally, the National Infrastructure Protection Center expands these threats to include hactivists, in General Accounting Office, GAO-02-74, *CRITICAL INFRASTRUCTURE PROTECTION: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems*, July 2002, 5.

10. Bruce Schneier, *Secrets & Lies: Digital Security in a Networked World* (New York City, N.Y.: John Wiley & Sons, Inc., 2000), 23-27.

11. *Computer Economics Malicious Code Attack Economic Impact Update*, August 31, 2001. On-line. Internet, 28 September 2002. Available from http://www.info-sec.com/viruses/01/viruses_091901c_j.shtml.

12. The President's Critical Infrastructure Protection Board, *The National Strategy to Secure Cyberspace*, February 2003 (Washington, D.C., The President's Critical Infrastructure Protection Board, 2002), 40.

13. Prepared Statement of George J. Tenet, Director of Central Intelligence, to Senate Select Committee on Intelligence, 2 February 2000. On-line. Internet, 28 September 2002. Available from http://www.cia.gov/cia/public_affairs/speeches /archives/2000/dci_speech_020200.html.

14. Computer Security Institute, "2002 Computer Crime and Security Survey." On-line. Internet, 3 October 2002. Available from http://www.gocsi.com/press /20020407.html.

15. Michael Erbschloe, *"Information Warfare: How to Survive Cyber Attacks,"*

(Berkeley, CA: Osborne/McGraw-Hill, 2001), 51-64.

16. Air Force Doctrine Document 2-5, *Information Operations*, defines the Global Information Grid as "The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data security services, and associated services necessary to achieve information superiority."

17. Air Force Doctrine Document 2-5, *Information Operations*, 4 January 2002, 11-19.

18. Quoted in Bruce Schneier, *Secrets & Lies: Digital Security in a Networked World* (New York City, N.Y.: John Wiley & Sons, Inc., 2000), 58.

19. Arnaud de Borchgrave, et al. *Cyber Threats and Information Security: Meeting the 21st Century Challenge* (Washington, D.C.: The Center for Strategic and International Studies (CSIS), 2000), 56-59.

20. *Critical Infrastructure Protection: Significant Challenges Need to Be Addressed*, United States General Accounting Office Report GAO-02-96IT (Washington, D.C., General Accounting Office, 2002), 4.

21. Ibid., 4-7.

22. This role was later filled in part by the National Infrastructure Protection Center (NIPC), an agency of the FBI. Arnaud de Borchgrave, et al. *Cyber Threats and Information Security: Meeting the 21st Century Challenge* (Washington, D.C.: The Center for Strategic and International Studies (CSIS), 2000), 67.

23. *Critical Infrastructure Protection: Significant Challenges Need to Be Addressed*, United States General Accounting Office Report GAO-02-96IT (Washington, D.C., General Accounting Office, 2002), 8.

24. The President's Critical Infrastructure Protection Board, *The National Strategy to Secure Cyberspace*, February 2003 (Washington, D.C., The President's Critical Infrastructure Protection Board, 2002), 1.

25. Ibid., 4-11.

26. Bruce Schneier, *Secrets & Lies: Digital Security in a Networked World* (New York City, N.Y.: John Wiley & Sons, Inc., 2000), 141-143.

27. Ibid., 188-197.

28. Ibid., 210. Industry standard software production is typically characterized by error rates in this range. In "Code Complete"' by Steve McConnell (Microsoft Press, 1993), the noted industry average for code production is 8-20 lines of correct code per day. In addition, it notes that industry average experience suggests that there are 15-50 errors per 1000 lines of delivered code. The security implications are significant. The continuous stream of warnings and updates from major vendors such as Microsoft highlight the severity of this problem.

29. Typically, installation of software patches when configuring a new system requires several days effort by a fully qualified network technician. My experience has been that installation of recurrent patches after a new system is in operation may take from minutes to several hours, depending on its complexity and if problems are encountered during the installation.

30. United States General Accounting Office, *Critical Infrastructure Protection: Significant Challenges Need to be Addressed* (Washington, D.C.: United States General Accounting Office, 2002), 2-3. This report summarized previous GAO work in this area, to include a similar GAO effort published in, *Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems*, July 2002.

31. Ibid.

32. Ibid., 22.

33. "FBI Seeks Help vs. Cyber Crime," *Federal Computer Week*, 1 November 2002. On-line. Internet, 2 November 2002. Available from http://www.fcw.com/fcw/articles/2002/1028/web-fbi-11-01-02.asp.

34. United States General Accounting Office, *Critical Infrastructure Protection: Significant Challenges Need to be Addressed* (Washington, D.C.: United States General Accounting Office, 2002), 3.

35. United States General Accounting Office, *Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems* (Washington, D.C.: United States General Accounting Office, 2002), 1.

36. Presidential Decision Directive 63 White Paper. On-line. Internet, 7 October 2002. Available from Hhttp://www.ciao.gov/resource/paper598.htmlH.

37. Ibid., 11.

38. "U.S. Business Cyber Security Survey," conducted by the Business Software Alliance, 24 July 2002, 14.

39. "SearcSecurity.com Survey Shows more talk than Action." On-line. Internet, 12 October 2002. Available from http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci846961,00.html.

40. "Government Computer News Survey," August 2002, *Government Computer News*, 11 September 2002, 2.

41. ICS is a Montgomery, Alabama based full-service information security consulting firm, which provides security for computer systems and enterprise networks in commercial businesses, not-for-profit associations, educational institutions, and government agencies. "The ICS Difference,: *Integrated Computer Solutions*". On-line. Internet, 2 November 2002. Available from http://www.integrate-u.com/icsDifference.asp.

42. Mr. Stephen Goldsby, CEO, *Integrated Computer Solutions*, interviewed by author, 30 August 2002.

43. Maryann Lawlor, "National Strategy Tackles Tough Security Issues," *Signal*, August 2002, 24.

44. Anthony H. Cordesman, Cyber-Threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland (Westport, CT.: Praeger Publishers., 2002), 171.

45. This fact was borne out not only by examination of all relevant documentation, as delineated within this chapter, but by supplemental discussion with security personnel at the NIPC, the Air Force Intelligence Agency, and private sector security firms contacted during this project.

46. "NIST-NSA Team Readies Systems Security Guidance," *Government Computer News.* On-line. Internet, 12 October 2002. Available from Hhttp://www.gcn.com/vol1_no1/daily-updates/20220-1.htmlH. The draft guidance is available on-line, Internet, at http://csrc.nist.gov/sec-cert/.

47. Internet Service Provider Directory. On-line. Internet, 12 October 2002. Available from Hhttp://www.findanisp.com/H.

48. "FBI Says DNS Server Attacks Came from U.S., Korea, *InfoWorld.* On-line. Internet, 2 November 2002. Available from Hhttp://ww1.infoworld.com/cgi-bin/fixup.pl?story=http://www.infoworld.com/articles/hn/xml/02/11/01/021101hnfbi.xml&dctag=securityH.

49. "Partners in the Environment," United States Environmental Protection Agency. On-line. Internet, 6 November 2002. Available from http://www.epa.gov/partners/benefits.html.

50. Joint Vision 2020, 8.

51. House Armed Services Committee, Statement on AF Information Assurance, by Lt Gen John L. Woodward Jr., AF/SC, 17 May 2001.

52. The President's Critical Infrastructure Protection Board, *The National Strategy to Secure Cyberspace*, February 2003 (Washington, D.C., The President's Critical Infrastructure Protection Board, 2002), 55.

53. "CIAS Prepares for Operation Dark Screen," University of Texas San Antonio. On-line. Internet, 14 October 2002. Available from http://business.utsa.edu/news/news_stories/2002/Aug02/cias.htm.

54. Information Sharing and Analysis Centers were prescribed by Presidential Decision Directive 63, and provide a means for voluntary sharing of threat information by infrastructure lead agencies.

CHAPTER 7

Improving The Effectiveness Of First Responders In Homeland Security

Phillip A. Bossert

Introduction

The horrendous events of September 11, 2001, firmly focused the nation's attention on homeland security. Since then, many actions occurred and continue to be taken at the federal, state, and local levels to deter another terrorist incident and to effectively deal with the aftermath of an attack. At the forefront of many of these efforts have been first responders, those police, firemen, medical, and other personnel who are first on the scene. While their courage and dedication are impressive, recent reports indicate that many are not properly trained or equipped to effectively handle a terrorist attack, especially one involving weapons of mass destruction (WMD).

The U.S. must greatly accelerate its efforts to train and equip its first responders; to do otherwise would be to risk certain disaster, especially with the proliferation of WMD and the increasing likelihood that terrorists will use these on U.S. soil. We will first review the role and crucial importance of first responders by examining the *National Strategy for Homeland Security* and discuss specific problems with the state of first responders based upon the recent release of two major reports. Then, we will analyze the challenge of dealing with so many local governments and how the concept of federalism makes improving first responders a daunting task. We will conclude by recommending two solutions: significantly increasing funding for equipment and training and directing U.S. Northern Command (NORTHCOM) to assist in establishing Homeland Security Training Centers for each state.

First Responders and Homeland Security

The *National Strategy for Homeland Security* was released in July 2002 and unequivocally states, "The U.S. Government has no more important mission than protecting the homeland from future terrorist attacks."[1] It explains further that homeland security is an "exceedingly complex mission that requires coordinated and focused effort from our entire society—the federal government, state and local governments, the private sector, and the American people."[2] This strategy states: "America's first line of defense in the aftermath of any terrorist attack is its first responder community—police officers, firefighters, emergency medical providers, public works personnel, and emergency management officials."[3] These first responders number over eleven million spread over 87,500 counties, cities, towns, villages, boroughs, parishes, and other governments.[4]

The homeland security strategy places great responsibility and importance on state and local governments. It says that states and localities "have primary responsibility for funding, preparing, and operating the emergency services that would respond in the event of a terrorist attack."[5] This strategy also emphasizes the importance of planning, equipping, training, and exercising first responders in order to minimize damage from an attack. But it frankly admits that there are multiple plans that dictate the federal government's support of first responders, there are too many seams in current plans and capabilities, and many geographic areas have little or no capability to respond to a terrorist attack, especially one involving WMD.[6]

But the *National Strategy for Homeland Security* offers a solution to this frightening state of affairs: the Federal Emergency Management Agency (FEMA) is taking the lead in improving the effectiveness of first responders. *[Editor's note: Due to the evolving nature of the Department of Homeland Security (DHS), some of the procedures and organizational structures discussed in this essay may have been overcome by events; however, the overall thesis of this article is still relevant. As of the publication date of this document, FEMA is no longer a separate agency and has been incorporated in the DHS Preparedness and Response Directorate. It will retain its "brand" name FEMA since it is widely recognized.]* Specifically, FEMA's

Office of National Preparedness, which was established four months before 9/11, is the nation's central coordination point for all federal programs dealing with terrorism preparedness.[7] Its three main focuses include first responders, providing a central point for all federal preparedness programs, and Citizen Corps.[8] Preparation for terrorist attacks is divided into the following areas: planning, equipment, training, and exercises. Since the FEMA Office of National Preparedness was established, their efforts have had minimal impact in improving first responders' effectiveness. Two recent reports, discussed below, clearly show this and underscore the need to accelerate training efforts.

First Responder Preparedness: Enormous Problems Remain

While the *National Strategy for Homeland Security* and Congressional testimony by the director of the Office of National Preparedness, Mr. Bruce Baughman, admit there are problems in quickly getting first responders proficient in handling terrorist attacks, especially catastrophic terrorism, two reports issued by private groups are much more critical and foreboding. A task force sponsored by the Council on Foreign Relations and chaired by former senators Gary Hart and Warren Rudman said that despite the terrorist threat being as grave now as it was just before September 11, 2001, the country is, "dangerously unprepared to prevent and respond to a catastrophic terrorist attack on U.S. soil."[9] In an eerie warning reminiscent of its earlier report released prior to 9/11 predicting a major terrorist incident, the report says, "In all likelihood, the next attack will result in even greater casualties and widespread disruption to our lives and economy."[10]

The Council's report highlights specific problems including the lack of intelligence sharing of terrorism watch lists among the 650,000 local and state police officials, inability of first responders to communicate because their radios cannot talk to each other, and lack of training and equipment to deal with chemical and biological attacks.[11] Its key recommendation is for the federal government to immediately increase funding for equipment and training, especially training involving WMD.[12]

Throughout this task force report one senses the urgency of fast-tracking these recommendations, given the ongoing Global War on Terrorism.

The Council on Foreign Relations report is one of several indicators of the urgent need to train first responders immediately. On October 21, 2002, the University of Maryland Center for Health and Homeland Security released a report stating, "Our nation's public health infrastructure remains woefully ill-prepared to properly manage a similar [9/11] crisis."[13] This report criticized the "obsession" with the organizational structure of the Department of Homeland Security, which is causing the neglect of first responders. It points out that, "Once a terror attack occurs, it is the first responders who will be prominent again."[14] In his Congressional testimony, Chief Ray Alfred of the International Association of Fire Chiefs said that his peers are concerned about the lack of coordinated federal effort, "both in terms of the preparedness of support programs…and the seemingly endless federal response capabilities that appear duplicative and continue to grow."[15]

Additional chilling statistics were released by the White House, further painting a bleak picture of the capability of first responders. It said, "fewer than 10 percent of counties surveyed by the National Association of Counties said they are prepared to respond to a bioterrorist attack."[16] It also said that many areas have little or no capability to respond to any WMD attacks and that many local communities rely on volunteer firefighters with very scarce resources for equipment, training, and other requirements.[17] And it appears that nationwide, the momentum and sense of urgency to improve first responder effectiveness is lapsing as a sense of complacency has reasserted itself.[18]

Attorney General John Ashcroft summarized the various readiness problems of first responders and the challenges in correcting these when he told Congress, "Long before the attacks of September 11th, you recognized the importance of inter-agency coordination and planning, information sharing with state and local law enforcement, and training and equipping first responders."[19] Highlighting the enormity of this problem, he said that countering terrorism in the homeland requires unprecedented cooperation and coordination, and that "no single individual, agency, department or government can succeed alone."[20]

All these reports, Congressional testimony, and other sources clearly show that the main needs of first responders in the Global War on

Terrorism include adequate equipment to deal with catastrophic terrorism, effective training that is timely and standardized nationally, compatible radios, better command and control of on-scene terrorist events, greater interagency cooperation especially in intelligence sharing, and adequate funding to quickly correct all these shortfalls. New York City's valiant response to the most destructive attack on the U.S. highlighted the strengths and weaknesses of first responders.

In the minutes after the first World Trade Center tower was attacked, the police and fire departments set up separate command posts several blocks apart, without any communications between them.[21] After the first World Trade Center tower collapsed, police directed their personnel to evacuate the remaining tower on the recommendation of one of their helicopter crews, but this information never got to the firemen in that tower because of this lack of interagency cooperation and interoperable communication. Most of the police in the second tower escaped, but 120 of the 343 firemen who died that day did not.[22] This lack of coordination between the New York Police and Fire Departments existed for years, and had tragic consequences on 9/11. In after action reports, this disconnect between two key first responder organizations was labeled "tribalism, us-versus-them, and the Battle of the Badges."[23] If the needless death of so many heroic emergency workers on 9/11 was not tragic enough, brawls erupted at the World Trade Center disaster site weeks later between police and firemen, highlighting the cultural differences between them, and further overshadowing their heroism. The truly sobering aspect of this catastrophe is that New York City had one of the best first responder programs in the nation and the world prior to 9/11, with an advanced emergency operations center, a robust training program, and good equipment.

The Challenges of Improving First Responder Preparedness

The shortcomings in New York City's response to the World Trade Center attacks points out the challenges facing the Office of National Preparedness in its efforts to get first responders nationwide up to par. There first has to be a cultural change in terms of interagency cooperation and coordination. Fortunately, there appears to be a national consensus for this and headway is already being made. For example, Paul Karis, the

chair of emergency medicine at Saint Vincent Catholic Medical Centers in New York City, says that since 9/11, disaster plans have been updated and practiced much more often, and there is finally an understanding that hospitals have to network with the entire city infrastructure.[24] However, while there appears to be a national consensus for seamless interagency and intergovernmental cooperation, old habits die hard, and only through extensive education and training will old habits be broken.

The magnitude of this task is enormous, especially when one considers the scope of educating and training eleven million first responders in over 87,500 state and local governments. There are over 3,000 counties alone in the U.S., and many of these counties conduct centralized training for police and firemen from numerous cities and municipalities.[25] As the *National Strategy for Homeland Security* states, "The challenge is to develop interconnected and complementary systems that are reinforcing rather than duplicative and that ensure essential requirements are met."[26] Based upon the immediate threat of catastrophic terrorism involving WMD and the technical training required to meet these diverse threats, attempting to get these local governments adequately trained and standardized is even more daunting.

The concept of federalism in which the federal government shares some power with the states has helped create these numerous local governments. Many Americans often criticize democracy for moving too slow. But our government was designed this way on purpose. Supreme Court Justice Louis Brandeis said in 1926: "The doctrine of the separation of powers was adopted by the Convention of 1787, not to promote efficiency but to preclude the exercise of arbitrary power."[27] In the Global War on Terrorism, however, the country must find a way to efficiently train first responders in over 87,500 local governments while at the same time respecting the concept of federalism. The key question is how to accomplish these with the threat of catastrophic terrorism in the homeland growing by the day.

Proposed Solutions

This chapter proposes two solutions. First, the federal government needs to increase funding for first responders' training and equipment.

Washington only awarded $170 million to 2,756 fire departments under the Assistance to Firefighters Grant Program in FY 2002, and an additional $190 million will be awarded by the end of calendar year 2002.[28] The administration has requested $3.5 billion for grants for first responders for FY 2003, but $2.6 billion requested for training and equipment for 18,000 local fire departments remained unfilled.[29] Also, funding for other critical areas of homeland security is seriously lacking, including port security, which has only received $92 million in funding in FY 2002 although needs exceed $2 billion.[30] With the nation spending over $100 billion a year for homeland security, and the needs of first responders so great, the proposed $3.5 billion for FY 2003, and $4.0 billion for FY 2004 is too small.[31]

However, much more than money is needed to prepare first responders to effectively deal with catastrophic threats. There has to be a crash program to educate, train, and exercise first responders. The *National Strategy for Homeland Security* lists this need as a major initiative. It says, "The Department of Homeland Security will under the President's proposal launch a consolidated and expanded training and evaluation system to meet the increasing demand."[32] The director of FEMA's Office of National Preparedness has identified this in more detail by stating how the Office of National Preparedness will establish an annual, nation-wide exercise program, with specific objectives and a corrective action program.[33] He also states how the Office of National Preparedness will establish national standards for compatible, interoperable equipment, a national mutual aid system, up-to-date personal protective equipment, and efforts at planning and coordinating all these initiatives.[34]

But while the need to educate, train, and equip first responders was identified in the first homeland security strategy, no one has proposed how this can be accomplished quickly and effectively. There is currently only one federally charted center that trains first responders to cope with WMD events.[35] Called the Center for Domestic Preparedness and located in Anniston, Alabama, it was created in 1998 and trains only 15,000 first responders annually.[36] Again, time is of the utmost essence given terrorists' autonomy to strike at their time and place of choosing. Indicators and warnings continue to point towards further terrorist attacks. CIA Director George Tenant has repeatedly warned Congress, as he did in

October 2002, that the terrorist threat is as grave now as it was just before the September 11, 2001, attacks.[37]

So this leads us to the second proposed fix to the plight of first responders: the federal government needs to utilize the leadership, organizational, and operational expertise of the U.S. military to assist FEMA's Office of National Preparedness in establishing Red Flag, Joint Readiness Training Center (JRTC), and National Training Center (NTC)-style training centers in all fifty states. These could be called "Homeland Security Training Centers." Using the technical expertise of the Center for Domestic Preparedness and the command and control, teamwork, and leadership training provided by Red Flag and its sister service equivalents, the Homeland Security Training Centers could be an enormous asset in homeland security. We will first look at why the U.S. military should be involved in this effort and the possible role of the newest unified command, NORTHCOM.

Why the U.S. military?

President Bush has used the term "Global War on Terrorism" to characterize the post 9/11 security environment. Clearly, it is a two-front war, with one front the homeland and the other overseas, whether it is Afghanistan, one of the axis of evil countries, or the fifty plus nations where Al Qaeda and other terrorists are active. In the latest *National Security Strategy*, the president says that to defeat terrorists, "we must make use of every tool in our arsenal—military power, better homeland defenses, law enforcement, intelligence, and vigorous efforts to cut off terrorist financing."[38]

The U.S. military has extensive experience dealing with many of the same problems first responders find themselves grappling with today. The chart below highlights this and shows how the U.S. military is at least a generation ahead of first responders dealing with these issues:

Table 7.1 U.S. Military – Civilian First Responder Comparison

(As of Nov 2002)	**U.S. Military**	**Civilian First Responders**
Organization-changing events	Vietnam; Desert One	Oklahoma City Bombing 9/11; anthrax attacks
Organizational Constructs	Goldwater-Nichols Act Unified Command Plan	Homeland Security Strategy; Department of Homeland Security

Coordination concepts	Jointness; multinational & interagency/total force ops	Interagency, inter-governmental operations; federalism
Cultural mindset for cooperation	Teamwork—jointness	"Tribalism"[39] Interagency competition
Interoperable communications	Good	Poor[40]
Command and Control	9 Unified Commands; Combatant commands	87,500 governments; Federalism; emergency scene unified C2--poor[41]
Personnel	1.4 million active duty; 1.3 million Guard and Reserve	11 million police, fire, medical, and emergency preparedness workers[42]
Education and Training	Extensive; advanced degrees, technical training; frequent professional military education	Varies greatly across the country. Infrequent; lack of standardization. WMD training poor.
Planning	Crisis Action Planning; Deliberate Planning	Uncoordinated Federal Response plans; Prior to 9/11, only 4 states had plans[43]
"Warfighting" Training & Exercises	Red Flag, National Training Center, Joint Readiness Training Center; Chairman of the Joint Chiefs of Staff exercise program	County level technical training by career—police, fire, etc. Interagency training? Center for Domestic Preparedness; few other specialized schools. Few large scale exercises[44]
Result	Desert Storm, Allied Force, Operation Enduring Freedom, Operation Iraqi Freedom successes	Next attack?

Source: Table developed by author

As this chart portrays, the world's most professional, experienced, successful, and powerful military has grappled with many of the problems first responders are grappling with today. With the urgency of improving first responders' preparedness, why should they reinvent a wheel the U.S. military has made for the last twenty-five years? As any veteran who has served on a civilian school board can attest, the leadership, teamwork,

organization abilities, and follow-through abilities of military personnel are often far superior to those of many civilians. As Secretary of Defense Rumsfeld said:

> When an event occurs in the United States, however, while everyone knows that the Pentagon is not in the business of providing an armed force for the United States, but when an event occurs, we get the phone call. And why do we get the phone call? Well, because the Department of Defense is considered the Department of Defense. They know that they've got troops, they've got people who respond, they're organized, and they can be of assistance."[45]

This is not in any way to denigrate civilians in general, but to underscore the impact of extensive education and training. The military has proven time and again in the last twenty years that it can quickly meet many challenges, especially those to national security. With the snail-like pace of training of first responders since 9/11, it is time for FEMA's Office of National Preparedness to get assistance from the U.S. military. Mayor Martin O'Malley of Baltimore summarized this situation when he said:

> For the first time in nearly 200 years, the front is right here at home. And to date, it's where we've seen the greatest loss of life. Yet we have insufficient equipment, too little training, and a lack of intelligence sharing with federal authorities.[46]

In fact, the Council on Foreign Relations Task Force recommends that the National Guard get actively involved in training civilian first responders, triple their number of WMD-Civil support teams, and get additional funding for more capabilities to assist local authorities in the event of a catastrophic terrorist event.[47] However, these recommendations are unrealistic in light of the incredible high optempo of active duty, guard, and reserve forces in their current commitments overseas and because of the magnitude of the needs among civilian first responders. The U.S. abandoned the two theater war strategy prior to 9/11 because of shortfalls in personnel and equipment, yet we find ourselves fighting a dual war now! The report also does not mention the possible role of

NORTHCOM, but the Homeland Security Strategy and the National Security Strategy do.

NORTHCOM and its Role in training First Responders

The mission of NORTHCOM, which stood up on October 1, 2002, is to plan, organize, and execute homeland defense and civil support missions.[48] Its area of operations includes air, land and sea approaches and includes the continental U.S., Alaska, Canada, Mexico, and the surrounding oceans out to 500 miles and parts of the Caribbean.[49] This is the first time a unified command is assigned the entire U.S, and it relieves Joint Forces Command of its responsibilities for homeland defense.[50] NORTHCOM's web site says, "If and when local and federal agencies need additional support—in the form of equipment, expertise, plans, organization, communication, and training—the men and women in uniform are prepared and ready to lend a helping hand."[51] Additional information on its web site indicates NORTHCOM is currently planning, "interconnected and complementary relationships and plans to support first responders."[52] But it does not go into any detail about these plans.

NORTHCOM and the DOD have been very careful in explaining the command's role, primarily because of the sensitivity of civil-military relations, especially when it comes to employing troops on U.S. soil, and because of the *Posse Comitatus* Act. This act prohibits U.S. military personnel from interdicting vehicles and aircraft; conducting surveillance, searches, pursuit and seizures; or making arrests for civilian law enforcement authorities.[53] And NORTHCOM is very clear about the chain of command—it does not liaison directly with the Department of Homeland Security; DOD conducts interagency liaison on behalf of the command.

These sensitivities and the potential assistance that NORTHCOM can provide in helping train first responders were illustrated at a DOD press conference announcing the new Unified Command Plan on April 17, 2002. Secretary Rumsfeld said NORTHCOM will, "provide for a more coordinated military support to civil authorities such as the FBI, FEMA, and state and local governments."[54] When asked what NORTHCOM would be in charge of, he firmly replied, "No, it's not in charge of anything. It is a supporting activity, as any activity that the Pentagon does today is a supporting activity."[55]

But indicative of the many possibilities that NORTHCOM can provide to civilian first responders, General Myers said that NORTHCOM is much more than an organizational reshuffling, and that all the support the Department of Defense provides to civil authorities will now be under one command.[56] As an example he used Joint Task Force-Civil Support that is responsible to civil authorities for chemical, biological, radiological, nuclear, and major conventional explosives events. General Myers said that many of these WMD units are in the Guard and Reserve, the implementation plan for NORTHCOM is not completed, and that training will have to be looked at.[57]

As of this writing, NORTHCOM does not have an active role with the Office of National Preparedness except for working with them on securing FEMA participation in NORTHCOM exercises.[58] It is the recommendation of this chapter that NORTHCOM immediately begin discussions with the Office of National Preparedness via the Department of Defense on the feasibility of the FEMA creating Homeland Security Training Centers in each state. Active duty, Guard, and Reserve personnel can provide assistance in creating curriculum training material, especially regarding leadership, command and control, interoperability, communications, and jointness, but above all in organizing these facilities to train the maximum numbers in the minimum time. However, civilian contractors and veterans should operate these centers, not the U.S. military because they simply do not have the personnel to do so.

Why Red Flag, Joint Readiness Training Center, National Training Center-style training?

One does not need to be a first responder to realize that specialized training is required to deal with catastrophic terrorism. The Center for Domestic Preparedness with its emphasis on WMD training clearly shows this, but it has its limitations. First, Center for Domestic Preparedness training does not involve a major accident response scenario, which is typical of catastrophic terrorism.[59] Second, only 15,000 students are scheduled to be trained in FY 2003.[60] And third, a greater emphasis on command and control needs to be added in order to effectively manage a large disaster. This new era of WMD, with the potential of thousands, even tens of thousands of casualties—or worse—requires thorough and frequent training taught by experts. Dr. Joseph Waeckerle, chairman of

the American College of Emergency Physicians' Task Force on Domestic Preparedness Against Weapons of Mass Destruction, emphasizes four points for first responders: educate, train, test, and sustain.[61] In addition to technical training, there is a need for first responders to learn command and control, communications, interagency coordination, crisis decision-making, teamwork, planning, and other skills that can best be taught not just by sitting passively in a classroom, but by practicing. Most state and local governments simply don't have the expertise or capability to teach these vital skills, much less to teach them to tens of thousands in a realistic environment.[62]

While some are advocating for greater involvement of the Guard and Reserve forces, their resources are limited, especially with record numbers of mobilizations fighting the Global War on Terrorism. Simply relying on the Reserve Component to deal with catastrophic terrorism would be a major mistake because they are stretched too thin.

The solution would be to use existing training schools such as Red Flag, Joint Readiness Training Center, and National Training Center, as models for the Office of National Preparedness to establish, with NORTHCOM's guidance, Homeland Security Training Centers. These would be larger and more team-integrated versions of the Center for Domestic Preparedness. This training could consist of several days of classroom instruction followed by "live fire" exercises. A cross section of first responders from the same city or municipality representing police, fire, emergency preparedness, medical, public affairs, utility, and others would practice terrorist scenarios involving chemical, biological, radiological, high explosive, and even nuclear weapons. The added benefit of this training would be to help standardize procedures nationwide, allowing even greater interagency coordination.

The success of the U.S. military in the Gulf War and every contingency since has been partially attributed to realistic training accomplished on a frequent basis. As one analyst said, "To a great extent, the massive tank and air-to-surface battles of the desert war [Desert Storm] were won at the Army's National Training Center in the Mojave Desert."[63] The Joint Readiness Training Center is another example of live training that has had a huge impact on effectiveness. Created in the late 1980s, all infantry brigades in the U.S. Army must participate in this three week exercise every two years to be certified combat ready. As you read

this chapter, there is a brigade at the Joint Readiness Training Center practicing urban warfare in a simulated chemical-biological warfare environment.

Another example of the value of this type of training was during ENDURING FREEDOM. The author of this chapter led a 95-person Tanker Airlift Control Element at the Joint Readiness Training Center in April 2001. This Tanker Airlift Control Element worked with Canadians and the 1st Brigade of the 10th Mountain Division, and seven months later we worked with some of the same Canadians at Kandahar and the 10th Mountain at Bagram Air Base near Kabul. The success of our missions to Afghanistan was attributed in part to our annual training at the Joint Readiness Training Center.

Summary

The immediate establishment of Homeland Security Training Centers in each state is vital for the following reasons:

- Current first responder training is severely inadequate despite the growing threats.
- Only 15,000 can be trained a year at the Center for Domestic Preparedness; 50 Homeland Security Training Centers could train approximately 750,000 annually, still far short of the eleven million first responders nationwide, but a big improvement.
- Training could be standardized nationwide, and the latest information could be disseminated from these locations to the 87,500 local governments.
- The enormous expertise and experience of the U.S. military could be leveraged quickly to its civilian counterparts, especially in areas where civilians are lacking. These include command and control, teamwork, leadership, and mass casualties.
- The U.S. military would be relieved of some, but not all, of the homeland security mission, freeing it to fight the Global War on Terrorism overseas.

- Federalism would be reinforced by building one Homeland Security Training Center for each state and by directing each state to organize and operate its own center.
- Politically, this would be very astute, since the President, members of Congress, state governors, and local officials could all claim credit.
- State Homeland Security Training Centers could become a focal point for coordinating equipment, additional training, and funding for homeland security, helping state and local officials sort through the maze of homeland security requirements. Also, these could become logical extensions of the new Department of Homeland Security.
- Homeland Security Training Centers would fit logically into the current state structures for homeland security. Each state has a homeland security director, and the Council on Foreign Relations report recommends each state establish a 24-hour command center.[64]
- These training centers could be quickly created from existing state and local facilities, standardized by the feds, and would be an early "win" for the newly created Department of Homeland Security.

Conclusion

The Global War on Terrorism is ongoing, and we've been told by our national leaders that it will take years more to fight. A key part of this war involves well-trained and equipped first responders to effectively handle terrorist attacks. In this age of WMD proliferation, the question is not if these weapons will be used on the homeland but when. To effectively deal with the unthinkable, the eleven million first responders must be trained adequately and very quickly.

The two solutions to this problem include greatly increasing funding for state and local governments, and establishing Homeland Security Training Centers in each state based upon the very successful models in the U.S. military. NORTHCOM should provide the Office of National

Preparedness technical assistance and advice in establishing these schools to accelerate their implementation because time is of the essence. The homeland security challenge facing the Nation requires innovative training and the ability to rapidly train and equip the country's first responders to handle a terrorist event, especially one involving WMD. This need was aptly summarized by the Council on Foreign Relations task force report:

> America's own ill-prepared response could hurt its people to a much greater extent than any single attack by a terrorist. America is a powerful and great nation, and terrorists are not supermen. But the risk of self-inflicted harm on America's liberties and way of life is greatest during and immediately after a national trauma.[65]

The clock is ticking. Action is needed. And eleven million first responders are waiting.

Notes

1. The White House, *National Strategy for Homeland Security* (Washington, D.C.: Office of Homeland Security, July 2002), *iii.*

2. Ibid., vii.

3. Ibid., x.

4. David H. Rosenbloom and Robert S. Kravchuk, *Public Administration: Understanding Management, Politics, and Law in the Public Sector* (New York, NY: McGraw Hill, 2002), 116.

5. *National Strategy for Homeland Security*, *viii.*

6. Ibid., 42.

7. Bruce Baughman, Director, Office of National Preparedness, *Office of National Preparedness*, (House, Transportation and Infrastructure Committee, 11 April 2002), 1.

8. Ibid., 2.

9. John Mintz, "Report: "U.S. Still Vulnerable," *The Washington Post*, 25 October 2002, 1.

10. Ibid., 1.

11. "Warren Rudman and Gary Hart, A Year After 9/11, "America Still Unprepared For Terrorist Attack, Warns New Hart-Rudman Task Force on Homeland Security," (New York, NY: Council on Foreign Relations, 25 October 2002), 2.

12. Ibid., 2.

13. "Experts discuss future of homeland security," Bio-Terrorism.Info, 21 October 2002, 1.

14. Ibid., 1.

15. Bruce Baughman, Director, Office of National Preparedness, "Office of National Preparedness," (House, Armed Services Committee, 5 March 2002), 2.

16. "Mutual aid agreements: Support for first responders outside major metropolitan areas," FDCH Regulatory Intelligence Database, 27 March 2002, 1.

17. Ibid., 1.

18. "Fighting Terrorism, and Lassitude," *The New York Times*, 29 October 2002, 1.

19. John Ashcroft, Attorney General, "Homeland Security," (Senate, Appropriations Committee, 2 May 2002), 1.

20. Ibid., 1.

21. William Langewische, "American Ground: Unbuilding the World Trade Center, *Atlantic Monthly*, October 2002, 99.

22. Ibid., 99.

23. Ibid., 99.

24. Marilynn Larkin, "Mixed Response to 9/11 Anniversary Among NYC's First Responders," *Lancet*, 7 September 2002, 730.

25. Richard J. Stillman II, *Public Administration Concepts and Cases*, (New York, NY: Houghton Mifflin Company, 2000), 129.

26. *National Strategy for Homeland Security*, vii.

27. Rosenbloom, 29.

28. "Bush Administration Puts Unprecedented Resources into Preparing and

Protecting the Nation's Firefighters," FDCH Regulatory Intelligence Database, 16 October 2002, 1.

29. Ibid., 2.

30. Mintz, 1-2.

31. *National Strategy for Homeland Security*, 63.

32. Ibid., 45.

33. Bruce Baughman, Director, Office of National Preparedness, *Office of National Preparedness*, (House, Armed Services Committee, 5 March 2002), 2.

34. Bruce Baughman, Director, Office of National Preparedness, *Office of National Preparedness*, (House, Transportation and Infrastructure Committee, 11 April 2002), 2.

35. Dr. Roger Golden, "Field Trip Report for Center for Domestic Preparedness," Air War College Elective: Chemical and Biological Warfare Issues for the USAF," 7 Sep 02, 1.

36. Terry Quarles, Department of Justice, e-mail, 13 Nov 02.

37. Mintz, 1.

38. *The National Security Strategy of the United States of America*, The White House, Washington, D.C., September 2002, iii.

39. Langewische, 99.

40. Rudman, 11-12.

41. Rudman, 11-12; Stillman, 283.

42. U.S. Northern Command, "First Responders, on-line, Internet, 29 October 2002, available from http://www.NORTHCOM.mil/.

43. John Ashcroft, Attorney General, "Homeland Security," (Senate, Appropriations Committee, 2 May 2002), 3.

44. Rudman, 12.

45. Donald Rumsfeld, "Special Briefing on the Unified Command Plan," *DefenseLink*, U.S. Department of Defense, 14.

46. Seth Fiur, "Hart-Rudman Report Confirms Mayors Concerns on Homeland Security,"

Washington Outlook, 4 November 2002, n.p., on-line, Internet, 18 November 2003, http://www.usmayors.org/uscm/us_mayor_newspaper/documents/11_04_02/Hart_Rudman.asp.

47. Rudman, 22.

48. U.S. Northern Command, "Who We Are—Mission, on-line, Internet, 29 October 2002, available from http://www.NORTHCOM.mil/

49. Ibid.

50. Donald Rumsfeld, "Special Briefing on the Unified Command Plan," *DefenseLink*, 2.

51. Ibid., "First Responders—Role of NORTHCOM."

52. Ibid.

53. Ibid., "Who We Are—Operating With The Law."

54. Rumsfeld, 2.

55. Ibid., 18.

56. Ibid., 13.

57. Ibid., 14.

58. Lt Col Todd K. Chamberlain, NORTHCOM liaison to Joint Staff, e-mail, 7 Nov 02.

59. Interview with Mr. Mike Culver, Air War College, 12 Nov 02.

60. Terry Quarles, Department of Justice, e-mail, 13 Nov 02.

61. Steve Brown, "Partnership Stresses First Responder Training in Community Preparedness," *AHA News*, 29 April 2002, 3.

62. Richard J. Stillman II, *Public Administration Concepts and Cases*, (New York, NY: Houghton Mifflin Company, 2000), 283.

63. Norman Friedman, *Desert Victory: The War For Kuwait*, (Annapolis, Maryland: Naval Institute Press, 1991), 244.

64. Rudman, 12.

65. Rudman, 5.

CHAPTER 8

Homeland Security: Strategic, Operational, and Tactical Partnerships

James Chambers

Translating the National Strategy

> *Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur.*[1]
>
> —The National Strategy for Homeland Security

Since September 11, 2001, many local law enforcement professionals have become somewhat apprehensive about projecting a positive response to the threat of terrorism. Most are anxiously looking to the federal government for direction and the all-important funding of new units and other activities that may become necessary in the national defense effort.[2] In July 2002, the Office of Homeland Security published its *National Strategy for Homeland Security* whose purpose is to "mobilize and organize our Nation to secure the U.S. homeland from terrorist attacks."[3] As President Bush states in his introductory letter, "it is a national strategy, not a federal strategy."[4] Admittedly, "this is an exceedingly complex mission that requires coordinated and focused effort from our entire society—the federal government, state and local governments, the private sector, and the American people,"[5] but one that must be done and done well.

In this effort, the yeoman's share of the responsibility rests on the state and local governments' law enforcement professionals. State and local law enforcement agencies have been, and always will be, the first line of defense in the protection of life and property within their

community.[6] Because of this, it is imperative that leaders in state and local law enforcement operationalize the stated and implied tasks listed in the *National Strategy* and translate those into tactical doctrine and procedures (response plans) for the men and women who "man" the American Front. Once these tasks are identified and plans are developed or revised, leadership must also establish a list of requirements or resources needed to meet those challenges.

Requirements and resources needed to counter our threats will likely include more efficient systems/organizations at the federal and state levels and high cost communications and training programs at the state and local levels, i.e., information sharing, communication interoperability, and first responder training. Seventy-seven percent of the 13,500 law enforcement agencies serving U.S. states, counties, cities, and towns have 24 or fewer sworn officers.[7] For these jurisdictions to successfully meet the challenges they are likely to face in the near- and long-term, they will require financial augmentation from the federal government.

Stated and Implied Tasks at the Operational Level

Operational level tasks link strategy and tactics. The *National Strategy's* objectives are clearly stated tasks, while others may not be stated but implied. In other words, they are implied because they are necessary to do in order to achieve the desired goal. The stated and implied tasks I have gleaned from the *National Strategy*, ones for which I believe law enforcement leaders can organize, train, and equip at the operational and tactical levels are: **Prevent, Respond to,** and **Recover from** terrorist attacks. Each of these tasks carry their own set of implied tasks. One implied task of "prevent" is the existence of an effective intelligence system. An implied task of "respond to" could be the existence of a communications system capable of interoperability with numerous jurisdictions and other emergency services. An implied task of "recover from" could well be the existence of a facility and infrastructure capable of sustaining an Emergency Operations Center (as well as a trained and available staff) for 24-hour operations for 14 days.

From these stated and implied tasks, a response plan can be developed or revised. Many agencies already have plans in place for various contingencies. Some natural disasters or large sporting event plans can easily be modified for response to a mass casualty situation. For

those jurisdictions that are without response plans, they must extract the stated and implied tasks applicable to their area's vulnerabilities and operational/incident management capabilities and create them. From this public safety plan, shortfalls in capabilities and resources can be identified and prioritized. Through the established financial grant process or through future funding programs, federal or state funding should be requested to eliminate vulnerabilities. In some areas, coalition law enforcement/emergency services will likely best serve the public, both operationally and fiscally, especially in the 77 percent of the 13,500 jurisdictions mentioned above.

Actions since 9/11

Since September 11, 2001, there have been many positive changes at all levels of government. President Bush signed into law an act creating the Department of Homeland Security—the largest governmental reorganization since 1947. The Department of Homeland Security Reorganization Plan transferred agencies from standing departments and reassigned them to the Department of Homeland Security; U.S. Customs, Border Patrol, and the Coast Guard to name a few. In January 2003, former Pennsylvania Governor Tom Ridge was confirmed as the first Secretary of Homeland Security.

Agencies within other Departments also made significant internal changes in an attempt to better meet their responsibilities. FBI Director, Robert S. Mueller III, outlined several changes in January 2003's *Police Chief* magazine. Some of those he mentioned include: the creation of the Office of Law Enforcement Coordination; the initiation of a pilot program in Saint Louis, Missouri, called the Joint Terrorism Task Force (JTTF) Information Sharing Initiative; and a new FBI Intelligence Bulletin sent to more than 17,000 law enforcement agencies weekly. The FBI's creation of joint terrorism task forces has proven to be an effective method of addressing the terrorism threat, while providing a means for the pooling of resources and the sharing of information with state and local agencies.[8] Director Mueller stated:

> Twenty-one new Joint Terrorism Task Forces (JTTF) have been started since September 11, 2001, bringing the total to 56. We have stood up a new national JTTF at FBI

> headquarters to complement the work of local task forces. It includes two local police officers as well as representatives from two-dozen federal agencies.[9]

However, the terrorists are capable of moving faster than our bureaucracy. Faster and more frequent changes are needed to prevent future successful attacks. If, in the immediate shadow of the terrorist attacks, the process by which we nominated and confirmed Secretary Ridge took almost a year and a half, how long will other "bold and necessary steps"[10] take as the memory of September 11th fades into history? As a Nation, we have a tendency to focus on the here and now, seldom studying the past and even more rarely planning for the future. Our political system, as a whole, reflects society in this manner.

Use the armed forces antiterrorism funding as a case in point. The ebb and flow of funding has been determined by crisis. After tragedies like Khobar Towers and the U.S.S. *Cole* attacks, money designated for antiterrorism programs flowed in great significance. Once spent and Congressional interest was focused elsewhere, the Department of Defense (DOD) relied on the amount appropriated in the annual budget—typically only a fraction of the money appropriated after a crisis.

Great changes usually begin with great catalysts. I submit the creation of Department of Homeland Security, albeit a wise strategic move, would have never been possible without an attack on our Nation's home front. Knowing how our political system operates, law enforcement/emergency services must continue to lobby for the systems and infrastructure that will achieve Department of Homeland Security's premier strategic objective—to prevent terrorist attacks within the United States—even if we only get an 80 percent solution.

Partnerships for Prevention

> *Every terrorist event, every act of planning and preparation for that event (if conducted inside the United States) occurs in some local law enforcement agency's jurisdiction. No agency is closer to the activities within its community than the law enforcement agency that has the*

> *responsibility and jurisdiction for protecting that community.*[11]
>
> —D. Douglas Bodrero, Senior Executive and Manager,
> State and Local Anti-Terrorism Training,
> Institute for Intergovernmental Research

Each community leader who undertakes the Herculean task of preventing, responding to, and recovering from terrorist attacks in their community knows "the most important focus is on prevention" and for him/her to be successful, it "requires strengthening, to the best of our abilities, our intelligence gathering systems."[12] A report from the National Commission on Terrorism stated in June 2000:

> Good intelligence is the best weapon against international terrorism. Obtaining information about the identity, goals, plans, and vulnerabilities of terrorists is extremely difficult. Yet, no other single policy effort is more important for preventing, preempting, and responding to attacks.[13]

Prevention, in this context, can be broken down further to include interdiction and mitigation. Interdiction, the most desirable form of prevention, is the complete stoppage of a planned terrorist attack at a point between the planning and execution phases. Whether interdiction occurs by employing an unmanned combat aerial vehicle such as the RQ-1 "Predator" against Al Qaeda operatives in Yemen; or by a Cullman County, Alabama, deputy sheriff's patrol conducting a routine traffic stop and finding a trunk load of explosives destined for a terrorist operation, the key is to make interdiction *intentional.* We must have a criminal intelligence system that will provide that capability.

If we fail to interdict terrorist acts, we must succeed in mitigating their effects. Though heavily reliant on a formal intelligence system, mitigation is also reliant on vulnerability assessments conducted by local governments. Something as simple as a well-placed set of concrete barriers at a hospital access point or an intrusion detection system with sensors and cameras at a chemical plant can mitigate a potentially catastrophic attack. Knowing vulnerabilities and the consequences of an attack will also allow plans to be crafted and spending to be prioritized showing the federal or state governments that funding your projects would

be the best use of the taxpayers' money. *Intentional* interdiction and mitigation requires a formal national intelligence system.

Intelligence System Requirements

In December 2001, then International Association of Chiefs of Police (IACP) President Bill Berger testified before the Senate Governmental Affairs Committee on the role of local law enforcement in homeland security. Berger stressed that state and local law enforcement agencies are crucial to success in the war on terrorism.[14] He further stated that there are 700,000 officers who patrol the streets daily with intimate knowledge of their community and implying they all have a part in gathering and using intelligence information to prevent terror in our country. What intelligence gathering agency would turn down the opportunity to have 700,000 intelligence gathering agents? In January 2003, FBI Director Mueller praised the success of local police involvement in gathering intelligence information. "Local officers have passed along tips and reports of suspicious behavior that have ultimately turned up terrorist activities. Recent months have made it clear that defeating terrorists requires a full partnership: local, state, federal, and international law enforcement working hand in hand like never before."[15]

In early 2003, even with all the landmark reorganizations and institutional changes, we have not created a national intelligence system that meets the requirements established by the IACP in the below paragraph:

> Berger stressed that in order to make use of this intelligence-gathering capability, federal, state, and local law enforcement agencies must develop an efficient and comprehensive system for the timely sharing, analysis, and dissemination of important intelligence information. The IACP believes that failure to develop such a system, and to provide guidance to law enforcement agencies in how intelligence data can be gathered, analyzed, shared, and utilized is a threat to public safety and must be addressed.[16]

Joint Regional Information Center

In June 2002, "IACP identified several barriers that currently hinder effective exchange of information between federal, state, and local law enforcement agencies:

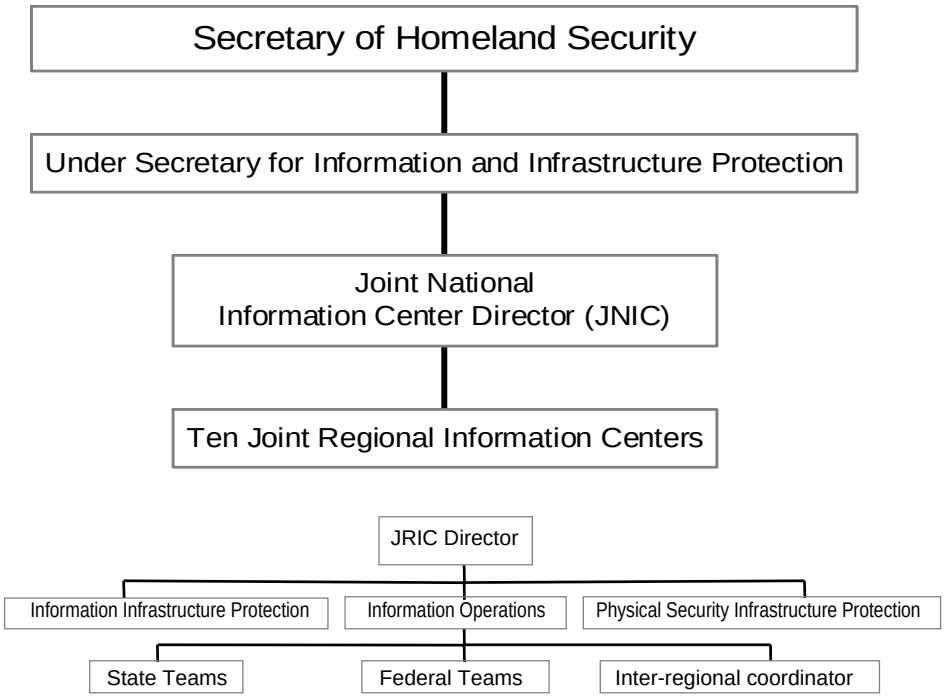
- The absence of a nationally coordinated process for intelligence generation and sharing.
- The structure of the law enforcement and intelligence communities.
- Federal, state, local, and tribal law and policies that prevent intelligence sharing.
- The inaccessibility and/or incompatibility of technologies to support intelligence sharing."[17]

Regardless of the steps that have been taken, some of these barriers still stand in the way of maximum information sharing. To alleviate these, I propose the following organization.

Organization

Create a Joint National Information Center (JNIC) under Department of Homeland Security's Undersecretary for Information Analysis and Infrastructure Protection (see Figure 8.1). Likely housed in Washington, D.C., the JNIC would oversee the backbone of the formalized information system, the Joint Regional Information Centers (JRIC). JRIC's organization would conceptually resemble the organization of the Department of Defense's unified command. A unified command is a command with a broad continuing mission under a single commander and composed of significant assigned components of two or more Military Departments.[18] Most unified commands are responsible for a specific region in the world—United States European Command for instance. JRICs would employ representatives from several federal agencies and be responsible for a specific region of our nation.

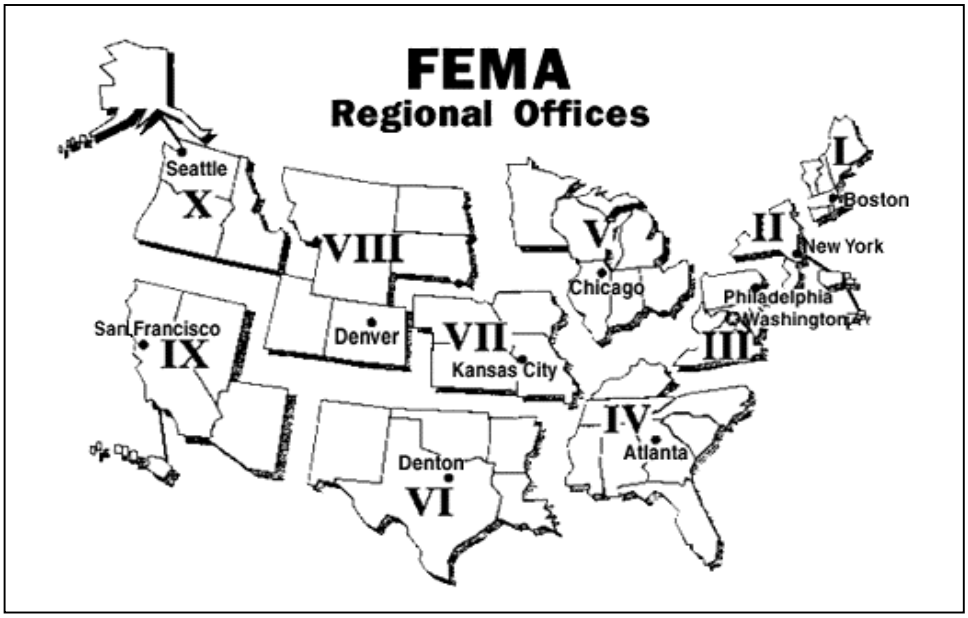
Figure 8.1 Proposed Joint National Information Center Construct



Source: JNIC and JRIC Concepts Proposed by Author

Department of Homeland Security, in creating this information system, should divide its area of operations into regions to make the volumes of information more manageable. Decreasing the input quantity would increase the output quality. The ten regions that the Federal Emergency Management Agency (FEMA) has established works well for my example and would likely work well operationally. *[Editor's note: As the Department of Homeland Security (DHS) incorporates FEMA into its Emergency Preparedness and Response Directorate, FEMA will become synonymous with DHS.]*

Figure 8.2 FEMA Regional Offices



Source: Federal Emergency Management Agency home page, on-line, Internet, available from http://www.fema.gov/regions/.[19]

Each JRIC would be organized to respond to local (city, county, state), national, and international intelligence gathering, analyzing, and dissemination needs. Local needs would be the responsibility of the **state teams** (Figure 8.1). A state team would exist for each state within the region and would consist of trained analysts dedicated to collecting and disseminating information to and from that state as well as other applicable state teams, federal agencies, and the inter-regional coordinator. In Figure 8.2, using Region IV as an example, there would be eight state teams. The size of each state team would vary depending on the workload, i.e., Florida *may* generate more information than Tennessee.

To address the national needs and international connections, other federal agencies such as the Departments of Justice, Energy, Defense, Interior, and the Central Intelligence Agency, to name a few, would assign employees to the JRICs. Workload would also determine which Department's personnel would have to be permanently assigned to the

JRIC or whether it could function like an emergency operations center where members are on call. The raison d'être of the JRIC would demand a permanent assignment of state teams and certain Department of Justice workers.

Operations

The scope of the JRIC should not be limited to terrorism activities only, but should include all criminal activity that may cross state, regional, or international borders. Why? Terrorism is, for the most part, an international organized crime similar in structure to a South American drug cartel or the Russian Mafia. Like all international crime organizations, international terrorism is dependent on what the military call lines of communications (LOC). A LOC is "a route, either land, water, and/or air that connects an operating military force with a base of operations and along which supplies and military forces move."[20] Criminal organizations that "trade" internationally often depend on the same LOCs, i.e., arms and explosive dealers, money launderers, human smugglers, etc. Evidence suggests Middle Eastern terror organizations have already contacted South American cartels.[21] The JRIC's resources should be used to exploit the similarities of international criminals. The cross flow of information would be significant as would the benefits reaped if timely information was disseminated to the proper agencies.

The information sharing cycle is a multidirectional process that could begin at any level and at any agency. As previously mentioned, there are 700,000 police officers employed by local agencies, all of which are experienced in gathering intelligence. Due to the nature of their work, these officers are experts at human intelligence (HUMINT). When a beat officer "works a snitch" for information and builds that informant as a reliable source, that is the purest form of HUMINT. Typically, this information is sent through the existing state system to the agencies currently responsible for intelligence gathering, analysis, and dissemination. In the proposed construct, state agencies would forward the information to their respective state teams in the JRIC. Sending this information forward would not preclude their own analysis and dissemination to local departments. Most states likely have a system in place that would be complemented by the JRIC system. For example, the following is a mission statement from the New Jersey State Police's

Intelligence Bureau. "The mission of the Intelligence Bureau is to diminish and control the capacity of criminal organizations to influence New Jersey's society, economy, and government."[22] This mission statement fits in well with the intent of the JNIC/JRIC concept, including breaking the LOCs of organized crime. Some states may have to modify their current organizations and information flow to meet the JRIC guidelines, but the payback will be well worth it.

Devil's advocates may groan that the federal government has just added another layer to the information/intelligence bureaucracy. They may also argue it would be quicker to just send the information to the affected state. With today's technology, the additional layer should not prevent State A from sending State B information at the same time State A sends it to the JRIC. JRIC would need this information in the regional system because State A may not realize that State G in another region may have corroborating information or even a better defined threat. The inter-regional coordinator's job in the JRIC is to make sure the information flow is completely seamless between all regions.

The success of this type of network was recently seen in the Washington, D.C. sniper case. Information sharing between more than a dozen jurisdictions in 6 states and 1,600 law enforcement officers, aided by the FBI's immense computer database helped solve this shooting spree. There is no doubt in my mind that this partnership was a key factor in getting the snipers off the streets and saving lives.[23] Unfortunately, we solved this crime in the respond mode, not the prevent mode. We cannot afford to be in the respond mode for a weapon of mass destruction (WMD) incident. A formalized system similar to the JRIC would increase our probability of interdiction.

Benefits

There are resounding strategic, operational, and tactical benefits to a consolidated information-sharing system. Currently, there are numerous organizations producing a substantial amount of information. The Regional Information Sharing System (RISS) program is an intelligence-sharing network with a goal of assisting state and local criminal justice agencies.[24] RISS is funded by the U.S. Department of Justice, Bureau of Justice Assistance.[25] The El Paso Intelligence Center (EPIC) is another example of an information-sharing program. EPIC is staffed by 15 federal

agencies. Others, such as the Law Enforcement Intelligence Unit, the state operated Law Enforcement Intelligence Networks, and the High-Intensity Drug Trafficking Area Investigative Support Center also exist and offer information to an already overworked investigator at your medium sized police department.

Consolidating the federally funded agencies gives local agencies a one-stop information shopping capability. With the right focus, trained intelligence analysts at a single JRIC-type center would decrease the quantity and increase the quality of information that flows to the officer on the beat. This would allow the local investigator or patrol officer to spend more time on the street and less time in the communications room. Regionalization of the information-sharing system carries the same benefit. Prior to September 11, intelligence-gathering agencies were overwhelmed with unfocused information. I submit this was a large contributing factor to the terrorists' success. The regional concept divides and conquers the immense amount of material.

The JRIC concept also evens the playing field between the "haves" and "have nots." Some agencies have a robust intelligence system that works well within their community. Some have a robust system that connects to other agencies as well. Other law enforcement agencies also need to benefit from that information, and the JRIC provides that conduit. The "have not" agencies, whether from lack of funding, leadership, or lack of perceived need, have no system in place. Given proper funding, the JRIC would provide national guidance on minimum requirements and effectively meet those needs.

Finally, the JRIC system would allow the FBI's sworn officers to focus on gathering information and acting on disseminated information. I debated internally on which agency, the FBI or Department of Homeland Security, should direct the JNIC system. The Department of Homeland Security has no paradigms to change and no bureaucratic inertia to overcome. The Department of Homeland Security seems best suited to create a new organization. By giving the analysis and the conduit responsibilities to Department of Homeland Security, more FBI agents can be put on the street. Also, the FBI has authority that would best be used in the enforcement arena.

Development of a comprehensive information system, coupled with well trained, dedicated law enforcement professionals will no doubt

increase the probability of interdicting planned terror activities. However, in our free society, security absolutes are very rare. Community leaders must demand a JRIC-like system from the federal government, but they must also plan for that system to occasionally fail. To do otherwise would result in potentially catastrophic consequences.

Planning to Respond and Recover

> *Reducing a community's vulnerability to attack requires, among other things, analyzing a locality to identify likely targets and working to improve security at these locations. Completely protecting every reservoir, parking garage, mass transit terminal, large building, and other likely targets within a jurisdiction is not possible.*[26]
>
> —IACP's Leading from the Front: Law Enforcement's Role in Combating and Preparing for Domestic Terrorism

The terrorist tries to find the softest target to get the most results while expending the fewest resources. The law enforcement agency must assess the risk to particular targets within its jurisdiction and attempt to harden the ones most likely to be attacked.[27] With planning, much of the chaotic activity usually produced by these kinds of events can be avoided.[28] Plan formats are readily available on the Internet. One option is to localize FEMA's Federal Response Plan, (FRP) accessible at http://www.fema.gov/rrr/frp/. This is a very in-depth plan that covers all areas of concern for a critical incident, including necessary support functions, and in part describes "the array of Federal response, recovery, and mitigation resources available to augment State and local efforts to save lives."[29] The FRP is a great starting point to develop a plan for any contingency. *[Editor's note: The Federal Response Plan is currently undergoing a thorough review and update by the Department of Homeland Security and is expected to be released as the National Response Plan in late 2004.]*

Mitigation

Successful prevention of a criminal terrorist act is not limited to intervention. Mitigation tactics, techniques, procedures, and technologies (TTPT) that decrease the terrorists intended effect by reducing loss of lives or structural damage should also be categorized as a successful prevention. Though TTPT need to be jurisdictional-specific to maximize mitigation, sharing with or borrowing from other agencies is highly encouraged. It will lessen efforts and time spent in a vacuum developing your own information. Regardless of jurisdictional similarities, minor adjustments will likely be needed. With that said, I do, however, believe certain steps in the mitigation process are applicable to every community, i.e., conduct assessments, create or revise response and training plans, exercise, and evaluate.

Vulnerability Assessments comprised of Consequence Assessments and Physical Security Assessments should be conducted in each jurisdiction. Methods for conducting Vulnerability Assessments are readily available on the Internet or through contacts in other agencies. The Department of Defense is a prolific assessor. The Defense Threat Reduction Agency (DTRA) conducts one assessment called the Joint Staff Integrated Vulnerability Assessment (JSIVA). The JSIVA is a five-day long installation assessment that examines threat assessment, mitigation techniques, and response capabilities.

- A terrorist options specialist looks at current threats and threat levels, the threat assessment process, and operations security.
- Two security operations specialists review operational plans, personal protection procedures, and security forces manning, training, and equipment.
- A structural engineer interfaces with base engineers and planners, surveys selected structures, reviews architectural and structural drawings, and performs quantitative analysis of blast effects to establish effective standoff distances.
- An infrastructure engineer focuses on the installation's supporting infrastructure such as water, power, and

communications protection against terrorist incidents. The infrastructure engineer also determines if there are any potential single-node points of failure.

- An operations readiness specialist focuses on the installation's preparedness to respond appropriately to a terrorist attack employing explosives, chemical, biological, nuclear, and radiological weapons. The operations specialist also reviews public affairs, medical, emergency operations center, legal, and communications programs.[30]

Results from JSIVAs are provided to installation leadership for corrective action. Some actions can be corrected through procedural changes, some through physical security installment such as barriers and intrusion detection systems, while others are unable to be addressed due to lack of funding. Vulnerability Assessments allow leadership to identify their vulnerabilities and create a prioritized spending list. Higher headquarters, either through annual budgets or additional Congressional appropriation, will often fund installation projects from their priority list.

Using the same process of assessing the vulnerabilities, identifying monetary shortfalls, and creating a prioritized list, local communities could reap the same fiscal benefit from their state or federal government. An excellent case in point on how preparation yields financial rewards is found in Louisiana.

In December 2002, FEMA granted "nearly $2 million to Louisiana for state and local responders and emergency management to become better prepared to respond to acts of terrorism and other emergencies and disasters."[31] Over the years, Louisiana has suffered from severe natural disasters in the form of hurricanes, floods, and tornadoes. With those come all the logistical challenges associated with a large population in the coastal region. For years, Louisiana has mitigated these effects by planning for warning, evacuation, shelter, and response procedures and funding equipment that supports those procedures. In November 2002, I visited the Louisiana Office of Emergency Preparedness, Emergency Operations Center to see their operation.

Using the Louisiana Emergency Assistance and Disaster Act of 1993, which established standards, requirements, and funding, the leadership in the Louisiana Office of Emergency Preparedness has done a

tremendous job organizing, training, and equipping the state's emergency management system. The Emergency Operations Center is very well arranged and rivals most military command centers I have seen, including the United States Central Command's Combined Air Operations Center at Prince Sultan Air Base in the Kingdom of Saudi Arabia. Their communications system, for instance, connects with 42 towers, making it capable of connectivity with all parishes (counties) in the state.[32] Although mainly used for natural disasters, this Emergency Operations Center is capable of managing any emergency, manmade or natural.

After September 11, 2001, the Louisiana Office of Emergency Preparedness expanded its existing infrastructure and focused on terrorism and WMD. Once they assessed their operation for that additional mission, they revised their response plan, identified deficiencies, and applied for a FEMA grant to fund corrective actions. The effort and money spent in the early years of emergency management did not go unnoticed. Louisiana reaped benefits because of their hard work and dedication to making their communities safer. In the following quote from the FEMA press release, notice the focus in plans at the local level.

> Of the nearly $2 million grant, $1.5 million will be provided for updating state and local plans and procedures to respond to all hazards, with a focus on weapons of mass destruction. The updated plans will help address a common incident command system, mutual aid agreements, equipment and training standards, interoperability protocols, critical infrastructure protection, and continuity of operations for state and local governments. *At least 75 percent of the grant amount is required to go to local governments.* The funds will assist local governments develop comprehensive plans, linked through mutual aid agreements, outlining the specific roles for all first responders (fire service, law enforcement, emergency medical service, public works, etc.) in responding to terrorist incidents and other disasters.[33]

Louisiana took advantage of all the money and effort they placed into their emergency management system. This grant money is currently

available to any community through FEMA. With the stand-up of Department of Homeland Security, coupled with constituents calling for funds to thwart possible terrorist incidents, I am positive future funding for like homeland security projects will be available. To capitalize on these funds, communities should assess their vulnerabilities, create or revise their response plans, identify shortfalls associated with their plans, and prioritize their needed resources.

Consequence and Physical Security Assessments

The Center for Civil Force Protection examines the consequences and physical security. There are four major categories in the Consequences Assessment that need to be addressed: loss of life, loss of revenue, loss of vital infrastructure, and loss of vital resources.[34] Obviously, loss of life would outweigh any consequence and should be given a higher value in calculating where to focus mitigation funding. Schools, hospitals, and large office buildings may fit into this category. The term *may* is used because there are so many other variables in each category. For instance, a large facility such as a school or office building may not be occupied during the hours of darkness. That's a significant factor. The hospital may receive additional weight in the consequence scale because your response plan is dependent on that hospital being available for use as the trauma hub in the case of a mass casualty event. Because of the complex, interwoven network and the multiple variables involved, a Vulnerability Assessment is not a one-person job and also not a job for law enforcement alone. It requires a team with members from all disciplines in the community.

When factoring consequences during a Vulnerability Assessment, place physical security in the plus column. Physical Security Assessments measure each system or facility's detection/assessment, delay, and response capabilities.[35] In the hospital example above, proper physical security measures would reduce the loss of life and/or infrastructure consequences. Physical Security Assessments often lead the assessor to ask a string of questions. Does the chemical plant in town have a security plan? Does corporate security or a private agency administrate it? Is my agency capable of responding to hazardous material incidents or will the corporation take that action? Are the exit routes capable of handling the amount of traffic exiting the cordon while allowing response vehicles access? When answered, questions like these will lead to measures to

mitigate negative effects of terrorist incidents as well as industrial accidents. Capability Assessments, when combined with Physical Security Assessments, begin the lessons learned loop that should be used to revise existing plans and further pinpoint where your money should be spent.

Exercises and Evaluations

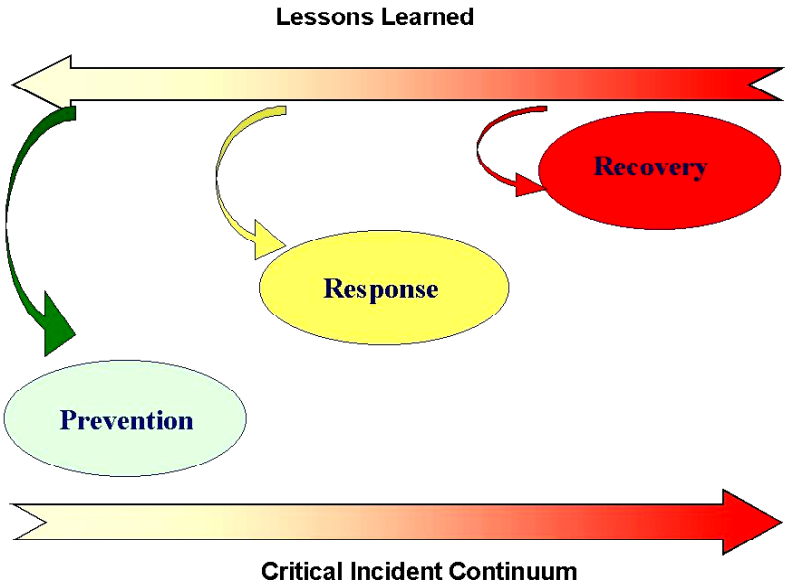
Over the last 25 years, emergency management training, as well as component-specific training, (law enforcement, fire, and medical) has kept stride with the needs of the community. State, federal, or private industry has always had visionary leadership to forecast future training needs. For most agencies, the shortfall has not been availability, but funding to support their training programs. Community leaders must fund or seek funding to continue these vital training programs. Well-trained responders are more confident and competent. Should an incident occur, the investment in training would pay huge dividends in lives saved.

An area that may not be as familiar to jurisdictions is exercising and evaluating their existing systems. Exercising and evaluating are as much a part of Vulnerability Assessments as studying consequences and physical security. Communities should conduct multidisciplinary exercises to identify vulnerabilities. Each community must determine which agencies need to be involved. In the previous example, the Louisiana Office of Emergency Preparedness Emergency Operations Center has a workspace for a representative from the hotel and restaurant industry. Their presence and connectivity with local hotels along the hurricane evacuation route provides valuable information to decision-makers. If your jurisdiction has the same concern, they must be included in the exercise. The entire system's efficiency is multidisciplinary dependent. Those communities that have conducted pre-incident exercises based on well-developed community response plans and have actually faced critical incidents have discovered that planning and exercising substantially improves their personnel's performance. Exercises work out relationships and problems before an incident occurs.[36] Exercise results also add information to your lessons learned loop.

When conducting these exercises, community leaders should consider inviting experts from other jurisdictions to observe and evaluate their plans and execution of their plan. The ideas, viewed from the outside, may identify additional vulnerabilities overlooked by the host. It's highly

likely these vulnerabilities may be overcome by simple procedural changes. Leaders who engage in this bold approach may be risking ego bruising as others will probably be critical of systems different from their own. Communities who ask others to evaluate their operation should remember that the criticism is intended to provide a different approach to an issue that can be dismissed or adopted by the community leadership. Evaluation, whether self-conducted or assisted by an outside agency, is a continual process. As depicted in the Critical Incident Continuum in Figure 8.3, it provides valuable information for every task.

Figure 8.3 Critical Incident Continuum



Source: Author's Model

Funding the Fight

Chief Ed Flynn of the Arlington County, Virginia, Police Department said, "While billions of dollars will, and should, be spent on federal-level preparedness and response to terrorism, one fact remains clear: the first responders to these acts will be beat cops—and they will need the

leadership of their chiefs to do the job right."[37] Training and equipping the beat cop to do the job for which they have been assigned is a leadership responsibility. For most local departments, training and equipping for terrorist prevention, response, and recovery requires funds over and above what most local departments are allocated annually. Federal assistance is vital to protect the lives and infrastructures. Two of the responsibilities of the Department of Homeland Security Director of the Office for Domestic Preparedness include:

- Coordinate preparedness efforts at the Federal level, and work with all state, local tribal, parish, and private sector emergency response providers on all matters pertaining to combating terrorism, including training, exercises, and equipment support, and
- Direct and supervise terrorism preparedness grant programs of the Federal Government (other than those programs administered by the Department of Health and Human Services) for all emergency response providers.[38]

The Department of Homeland Security has a tremendous opportunity to create a funding system that will insure funds and grants reach those who protect America's Front, and provide good stewardship of those allocated funds. Rather than creating their own system for this funding, the Department of Homeland Security should look at the funding system of the Department of Defense. When money is allocated from the Defense Budget to the Services, it is assigned a Program Element Code that identifies a specific mission. For instance, the Program Element Code for air base defense is 27588. Money allocated under that Program Element Code is for the sole purpose of air base defense programs and equipment. The system does allow money to transfer to other missions, but significant justification is required. Homeland Security Program Element Codes could include such programs as First Responder Training; Communications Systems; Hazardous Material; Biological, Agricultural, Chemical Abatement; Counterterrorim Task Force (SWAT), and many more.

The following is an example of how the system could function in the Department of Homeland Security. Pascagoula, Mississippi, after assessing their industrial complex and revising their response plan, may

need three additional Hazardous Material response vehicles to mitigate the damage an attack or accident could cause. Federal money is allocated for those vehicles under a Hazardous Material Program Element Code with the understanding that the money can only be spent on those vehicles. Meanwhile, the five jurisdictions within Jackson County, Mississippi decide to form a coalition and pool their resources to create a Hazardous Material response team. As a coalition, they only need one more vehicle to mitigate damage at the industrial complex, but they find their communications interoperability is insufficient for that coalition to operate. They request part of the original allocation to be transferred to the Communications Program Element Code. They justify their request by showing multiple benefits that serve emergency management in a much broader sense than just the industrial complex; i.e., the communications system is located in a coalition Emergency Operations Center and can be used for any manmade or natural disaster. The Department of Homeland Security would likely approve the request to change the color of money because it is more efficient and helps multiple jurisdictions with one allocation.

The basis for my proposal stems from information received in the United States Air Force Counterproliferation Center's Homeland Security Seminar. A representative from a Federal agency discussed his experience in dealing with local governments. He said most local governments expressed their lack of confidence in their state agencies' ability to pass along the Federal money to them. In order for the funding system within the larger Homeland Security system to be effective, local agencies must trust their state-level brethren. Also, because of the enormity of the undertaking, the Department of Homeland Security needs state governments to administer their money. The division of labor helps with the span of control. State agencies must be trusted by both the Federal and local governments to properly administer homeland security dollars. A Defense Department-like program with accounting trails and Government Accounting Office audits would insure proper appropriation and would instill trust in all parties.

Emergency Management Coalitions

Coalition warfare is commonplace in the history of warfare itself. Various reasons exist as to why these coalitions formed. Today, coalition warfare exists mainly for diplomatic or political reasons. Emergency

Management Coalitions should exist for the same reasons they have existed in historical warfare, however, one of the main reasons is fiscal efficiency. As previously mentioned, 77 percent of the law enforcement agencies have 24 or less sworn officers. They operate on a shoestring budget. Joining forces and the creation of co-dependent jurisdictions would provide better use of the limited homeland security dollars.

Many states are now divided into districts. For instance, Georgia has eight, while Mississippi has three. Cities and counties within districts should consider forming emergency management or law enforcement coalitions. For example, take four adjoining counties. Each, depending on their vulnerability assessment, may require certain services to mitigate their vulnerabilities in case of a critical incident. In this example, the four counties may have the common needs: first responder training, interoperable communications, hazardous materials response, and Counterterrorism Task Force.

Each county would take one of the four needs as their responsibility. Let's say County A takes the responsibility for first responder training. That county, through their emergency management or public safety director, would request funds to send a member from each discipline (police, fire, emergency management services, etc.) to a first responder instructor training class. Once they were trained, they would train all members of all agencies within their coalition. State and Federal funds would be spent on just one county but they would get four counties worth of training in return. This example applies to all aspects of the Respond to and Recover from tasks. Additionally, the example is also not just limited to the coalition in the example; memorandums of understanding could easily be reached with adjoining coalitions, including ones in adjoining states. The possibilities, with the right leadership, are endless.

Conclusion

> *We face an adaptive enemy. Empowered by modern technology and emboldened by success, terrorists seek to dictate the timing of their actions while avoiding our strengths and exploiting our vulnerabilities.*[39]
>
> —National Strategy for Combating Terrorism

In concluding my discussion on strategic, operational, and tactical partnerships, I weigh my points and ideas against the goals and objectives of the *National Strategy for Combating Terrorism*. Although the complete integration of all goals and objectives are vital for successful homeland security, I will concentrate on the fourth goal—Defend U.S. Citizens and Interests at Home and Abroad—and its objectives:

- Implement the *National Strategy for Homeland Security.*
- Attain domain awareness.
- Enhance measures to ensure the integrity, reliability, and availability of critical physical and information-based infrastructure at home and abroad.
- Integrate measures to protect U.S. citizens abroad.
- Ensure an integrated incident management capability.[40]

The *National Strategy for Homeland Security* is the approved roadmap by which we as a nation will protect our American way of life. The stated tasks are clear and the implied tasks as they pertain to each community are easily extracted. Federal agencies responsible for Homeland Security must create new systems or modify existing systems to produce maximum effects while minimally taxing (fiscal and otherwise) the American people and our infrastructure. Systems that provide real-time, accurate threat information to the agency or agencies that have the greatest potential for incident prevention and that properly fund local governments so they can alleviate or mitigate their vulnerabilities are two examples. Vulnerabilities are identified and prioritized through assessments. They can be conducted locally, by other agencies, or by a contractor, but must be accomplished.

State and local governments, using the *National Strategy for Homeland Security* as the basis for their operational and tactical plans, coupled with threat information and known vulnerabilities, can further develop detailed plans, prioritized requirements lists and request Federal funding assistance for resources beyond their financial capability. All financial requests should be linked to the goals and objectives of the *National Strategy for Homeland Security*. The International Association of Chiefs of Police President, Chief Joseph Samuels, Jr., has brought

national attention to funding priorities and advocates for Federal assistance to states and local governments. "It is critical that our members have the tools and resources needed to meet public expectations of us for safety and security. Securing Federal financial assistance and resources for state and local law enforcement will be one of the three priorities."[41]

Information and funding systems like those proposed in this text are vital in attaining integrated domain awareness. "Domain awareness is dependent upon having access to detailed knowledge of our adversaries distilled through the fusion of intelligence, information, and data across all agencies."[42] The Joint Regional Information Center provides domain awareness plus. The Joint Regional Information Center construct is designed as an information conduit, not terrorist related information only. International and interstate criminal lines of communication are like high occupancy vehicle lanes for all to use. To field an information system that fails to include all like information would be like removing a step from a math formula and still expecting the correct answer.

To better explain how an incomplete system is a formula for failure, I will use a historical case in point—the Law Enforcement Assistance Administration funding in the 1960s. This program was designed "to provide state and local law enforcement agencies with modern tools to fight crime but was disestablished in 1982 amid criticism that it had frittered away billions of dollars while crime rates rose."[43] On the surface it looks as if the idea and funds behind the idea were flawed, but consider the following information.

The criminal justice system is much more than just law enforcement. The criminal justice system consists of education, enforcement, the courts, and corrections. The Law Enforcement Assistance Administration only provided funds for law enforcement. As law enforcement efficiency improved, it created backlogs in the courts and overcrowding in the prisons—a funnel effect.

As court dockets filled, lesser crimes were often handled through plea-bargaining, with the criminal getting a lesser punishment. Likewise, the state prisons and county jails suffered from overcrowding. This drove United States courts to establish guidelines for prisons and jails and levy fines for noncompliance. Since states and counties could not afford the penalty for violating federal court mandates, work release programs were created instead of raising taxes to build more prisons. In many cases,

prisoners were released before serving half of their sentence and relocated into halfway houses and worked in the community. Crime rose, in this case, because of law enforcement's effectiveness—funding a component vice the entire criminal justice system.

Finally, ensuring an integrated incident management capability, considering the variety of jurisdictions within the United States, may be the most costly of the objectives. "An effective, integrated response requires incident management planning, enhanced interoperability, and coordination, based on and supported by rapid and effective decision-making."[44]

Federal guidance will be necessary to ensure integration. The Department of Homeland Security will need to establish minimum requirements for each jurisdiction type. For instance, a municipality with a population from 50,000 – 100,000 people must have the capability to communicate with all emergency management agencies within their county and bordering counties.

From this Federal guidance, local communities will establish their operations requirements. Using the above example, the required capability could mean a new central communication system or just reprogramming the existing equipment. Cost will vary with each jurisdiction. Resourceful governments will establish coalitions as mentioned in this text. Some less populated regions may have no other recourse but to bear the sole brunt of the required minimum standard. A funding system, as mentioned previously, where money is categorized and checks and balances exist to ensure the money allocated is spent properly, not only facilitates this objective, but builds confidence at every level of government from Congress to the constituency.

Although each citizen should do their part to prevent terrorism, those of us who have chosen public service as our profession carry a tremendous responsibility—organizing, training, and equipping the men and women who man the American Front. Together with these men and women, "we must take the battle to the enemy, disrupt his plans and confront the worst threats before they emerge. In the world we have entered, the only path to safety is the path of action. And this nation will act."[45]

In the wake of the September 11, 2001, attacks, there was no hesitation to *react*. As the ripples from that sensational event fade into a vast ocean of competing priorities, we must be able to articulate our strategic, operational, and tactical goals and objectives necessary to

prevent or mitigate future loss of life. We must act to prevent and mitigate because we cannot afford the consequences of waiting only to reaction.

Notes

1. Office of Homeland Security, The *National Strategy for Homeland Security*, July 2002, 2.

2. Philip M. McVey, "An Effective Homeland Defense Partnership," *Police Chief*, April 2002, 174.

3. Homeland Security, *National Strategy*, 1.

4. Ibid., n.p.

5. Ibid., 1.

6. D. Douglas Bodrero, "Law Enforcement's New Challenge to Investigate, Interdict, and Prevent Terrorism," *Police Chief*, February 2002, 43.

7. International Association of Chiefs of Police, *Criminal Intelligence Sharing: A National Plan for Intelligence-led Policing at the Local, State, and Federal Levels*, (Alexandria, VA: August 2002), 10.

8. Bodrero, 48.

9. Robert S. Mueller, III, "From the Director: Teamwork is Our Future," *Police Chief*, January 2003, 8.

10. Homeland Security, *National Strategy*, n.p.

11. D. Douglas Bodrero, "Law Enforcement's New Challenge to Investigate, Interdict, and Prevent Terrorism," *Police Chief*, February 2002, 43.

12. W. Ronald Olin, "Why Traditional Law Enforcement Methods Cannot Win the War on Terrorism," *Police Chief*, November 2002, 30.

13. National Commission on Terrorism, *Countering the Changing Threat of International Terrorism*, (Washington, DC: June 2002).

14. Gene Voegtlin, "IACP Testifies on Local Law Enforcement Role in Homeland Defense," *Police Chief*, February 2002, 8.

15. Robert S. Mueller, III, "From the Director: Teamwork is Our Future," *Police*

Chief, January 2003, 8.

16. Voegtlin, 8.

17. Gene Voegtlin and Jennifer Horne, "IACP President Testifies on Department of Homeland Security, " *Police Chief*, August 2002, 8.

18. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 12 April 2001, 446.

19. Federal Emergency Management Agency home page, on-line, Internet, available from http://www.fema.gov/regions/.

20. Joint Pub 1-02, 245.

21. Name withheld due to academic freedom policy, Air War College, Montgomery, Ala., 10 January 2003.

22. New Jersey State Police Homepage, n.p., on-line, Internet, November 2002, available from http://www.njsp.org/about/itelb.html.

23. Mueller, 9.

24. Bodrero, 45.

25. International Association of Chiefs of Police, *Criminal Intelligence Sharing: A National Plan for Intelligence-led Policing at the Local, State and Federal Levels*, (Alexandria, VA: August 2002), 8.

26. International Association of Chiefs of Police, *Leading from the Front: Law Enforcement's Role in Combating and Preparing for Domestic Terrorism*, 10.

27. Philip McVey, "An Effective Homeland Defense Partnership," *Police Chief*, April 2002, 176.

28. International Association of Chiefs of Police, *Leading from the Front: Law Enforcement's Role in Combating and Preparing for Domestic Terrorism*, 10.

29. Federal Emergency Management Agency, "Federal Response Plan," n.p., on-line, Internet, December 2002, available from http://www.fema.gov/rrr/frp/frpintro.shtm#purpose.

30. Defense Threat Reduction Agency, "Joint Staff Integrated Vulnerability Assessments Fact Sheet," July 2002, n.p., on-line, Internet, November 2002, available from http://dtra.mil/news/fact/nw_jsiva.html.

31. FEMA. On-line, internet, available from http://www.fema.gov/regions/vi/2002/r6_03_12_01la.shtm.

32. Visit November 2002, Brief, Baton Rouge, LA.

33. FEMA. On-line, Internet, available from http://www.fema.gov/regions/vi/2002/r6_03_12_01la.shtm.

34. Center for Civil Force Protection, "Community Vulnerability Assessment Methodology," Presented by Nick Nicholson, PhD. Sandia National Laboratories, National Institutes of Justice, Slide 19. On-line. Internet, November 2002. Available from http://www.nlectc.org/ccfp.

35. Ibid., Slide 21.

36. IACP, Leading, 10.

37. Ibid.

38. Department of Homeland Security, Reorganization Plan, November 25, 2002, paragraph 2,B, 3,c. On-line, Internet, January 2003, available from http://www.dhs.gov/dhspublic/.

39. *National Strategy for Combating Terrorism*, 24.

40. Ibid. 25-27.

41. Joseph Samuels, Jr., "President's Message: The Challenge Before Us," *Police Chief*, November 2002, 6.

42. *National Strategy*, 25.

43. William L. Schwabe, *Improving Crime-Fighting Technology in Law Enforcement*, 2001, n.p., On-line, Internet, November 2002, available from http://www.fathom.com/story122018.

44. *National Strategy*, 27.

45. George W. Bush, June 2002, quoted in the *National Strategy for Combating Terrorism*, 11.

CHAPTER 9

The Psychological Impact of Terrorist Attacks: Lessons Learned For Future Threats

Judith J. Mathewson

Setting the Stage for Panic and Terror

> *"Crises" can help us discover much about ourselves and enrich our lives. If 'disaster' enriches our lives with gifts that would otherwise have been taken for granted, is it really a disaster? Or is it a gift in disguise?*[1]
>
> —Elisabeth Kubler-Ross

Virtually every epoch in American history makes mention of one or more significant disasters - fire, floods, hurricanes, tornadoes, volcanic eruptions, snowstorms and earthquakes are commonplace. Other disasters are human-made, caused by people through mishap or neglect, such as a work accident, apartment fire, or with deliberate intention, such as terrorism.[2] A disaster is roughly defined as any natural or human-induced event that causes damage to physical, social, psychological or economic structures so as to require extraordinary assistance from outside the immediate impact area.

Terrorism, on the other hand, is something relatively new to American history, especially mass casualty terrorism. So, how do we define terrorism? Terrorism is defined as the use of violence by fanatical extremists as a mode of governing or opposing governments by intimidation.[3] It is coercion of the civilian population, or any segment thereof, in furtherance of political or social objectives.[4] Its aim is to immobilize the civilian population with fear and anxiety. Terrorists terrorize by using threats or physical destruction to kill and maim innocent people, create sensationalism and chaos, and gain instant

publicity for the terrorist's cause. The terrorist acts are unprovoked and intentional, causing overwhelming fear. These acts evoke feelings of helplessness in individuals; terrorists randomly target innocent and defenseless groups of people.

The battlefield is not the land upon which the attacks take place, but rather, it is the mind - the psychology - of those who survive.[5] The events of September 11, 2001, added a domestic reality to the term terrorism that all Americans had hoped would never be experienced. It has been estimated that somewhere between 9 percent and 35 percent of those directly exposed to traumatic events such as disasters and terrorism will develop significant posttraumatic psychological distress and perhaps posttraumatic stress disorder (PTSD).[6]

Psychotherapy alone, no matter how brief, seems inadequate to effectively respond to the psychological needs of both civilian and military personnel in the wake of terrorism and disasters. As a result, acute psychological crisis intervention, sometimes called "psychological first-aid," as well as other forms of emergency mental health interventions have been recommended to address the earliest psychological needs subsequent to disasters and acts of terrorism.[7]

Both types of disasters, natural and human-made, can elicit fear, anger and worry in victims, their families and friends and could lead to psychological symptoms of anxiety and depression. Research has shown that human-made disasters are more psychologically pathogenic than are natural disasters. Terrorism may be the most pathogenic of all due to its unpredictable and unrestrained nature.[8]

This chapter will describe the phases of terrorist attacks and examine the psychological impact of terrorist events on Americans, focusing on military members and civilian State Department employees. It will evaluate training programs and emphasize the importance of resiliency training to prepare individuals for future attacks.

To begin, it is important to understand the three fundamental phases of the terrorist attack: first, the pre-attack/pre-crisis phase, secondly, the acute event itself and third, the consequence management/reconstruction phase. These three phases have been identified in response to major disasters throughout the world over the past 20 years, according to Dr. George S. Everly and Jeffrey T. Mitchell, Ph.D., founders of the International Critical Incident Stress Foundation, Inc. They created this

structure for understanding the phases of terrorism and to prepare primary target populations and emergency services.[9]

The pre-attack, pre-crisis phase is the time period prior to the actual attack. During this phase, both threat assessment and prevention are very important and are performed by law enforcement, military, and the intelligence resources available. The military does this well by incorporating such considerations into its exercises and force protection strategy. The civilian sector is not so well prepared. Current events show that the civilian community needs to design and implement disaster exercises to identify possible threats and vulnerabilities and to educate its personnel on possible safety concerns. Phase two implements the plan designed from phase one. Doctors Everly and Mitchell believe that the better prepared the American population is for a terrorist event, the less severe the overall impact of the attack.[10]

As an example of all three phases of the attack, a young electronic warfare officer (EWO) learned a few lessons about terrorism that have stayed with him for many years. Talking about his experience brought back many painful memories for him. In Greece, during the late 1980's, there was animosity against the United States and the Air Force mission in an unprotected area near the city of Athens. Yet, the aircrew was not prepared for a car bomb that detonated near its bus, which was traveling the same route from the hotel to the base and back for the prior six months. When the EWO's bus was attacked, he was stunned and cut by shards of glass, but intuitively tried to assist the injured Greek bus driver. Later, he felt extreme anger towards a fellow Air Force member who sprinted away after the attack without assisting anyone else.[11] Although the EWO was later awarded a Purple Heart for his injuries, he felt frustrated since there was no follow-up counseling or training done, Critical Incident Stress Management (CISM) didn't exist at that time.

"Those airmen who requested to return to the United States were called 'wimps' by their commander," the victim explained. "By definition, one is not prepared for a terrorist attack – out of the blue. It is not like going into battle – a person is just doing his job when the attack occurs – changing his life forever."[12] As a result of this attack, the buses transporting the aircrews are now armored and personnel wear protective flak vests.

Conversely, at the Pentagon, there had been numerous fire and evacuation drills prior to the 9/11 attack; many permanent staff military and civilian personnel were accustomed to quickly and quietly evacuating the building due to these practice drills. It was quite different from the World Trade Center attack, where people jumped to their deaths from the building due to panic and chaos.

The second phase of the terrorist attacks is the acute event management phase. This phase persists as long as event assessment, containment, rescue and recovery efforts continue. During this time, fire suppression, communications, law enforcement, rescue and emergency personnel perform their respective functions. Techniques such as crisis management briefings, defusings, demobilizations, and crisis counseling within the CISM system are implemented.[13] This phase is one where counselors trained in trauma care can assist the emergency first responders and the victims during these crucial first hours.

Although research shows that it is important for first responders to rest, drink water, and take care of one's own needs after doing dangerous rescue work, many fire fighters, police, EMTs and security personnel push themselves to their limits and can become emotionally and physically worn-out. Caregivers need to pace themselves and each other and establish 8 to 10 hour work shift rotations to keep from becoming a psychological victim of a terrorist event.

The research done by the American Red Cross shows that there were more than 237,000 mental health contacts related to all three terrorist attacks from people in New Jersey, Connecticut, Massachusetts, California and several other locations. The Pentagon, as of 6 June 2002, had 8,136 mental health contacts – to include victims and first responders.[14] Current studies show that 52 percent of the World Trade Center first responders have suffered from both mental health issues and respiratory problems over eighteen months to years later.

The third phase is the consequence management and reconstruction phase. During this time, frustration, shock, anxiety, grief, disillusionment, mourning, and depression fully emerge. Studies show that survivors in close proximity to a terrorist attack may not realize they need help and therefore won't seek it, despite suffering significant emotional distress. Some endure active post-disaster psychiatric symptoms, including post-traumatic stress, sleep disorders, memory problems, and major depression

for as long as 6 months. One reason is that those who were spared may feel so much "better off" than those who were not; they may minimize their own needs and feel guilty for having them. Or, they may be ashamed of what they're feeling, believing their distress indicates some sort of weakness or instability.[15] As a method of helping these individuals, the Employee Assistance Program at the Pentagon and Operation Solace from Walter Reed Medical Center offered valuable, voluntary stress management classes, did "walk about" mental health talks with individuals and were available for assistance and referrals for up to a year after the terrorist attack. This was a very realistic and "user-friendly" approach for both civilian and military personnel who needed help but may have been hesitant to ask for it. An 800 number was established for those who needed to call-in to receive telephone consultation for psychological and emotional support.

Without a sense of psychological closure, without the ability to move on in life, the terrorists would prevail.[16] Without the ability to successfully mourn our dead, memorialize heroes, and continue to grow as individuals, families, communities, and as a nation, our way of life would be disrupted and the terrorists would win.[17] The Department of Defense held a memorial service two months after the attack for families and co-workers at the Pentagon. The newly reconstructed Wing was dedicated a year later; the 1-year anniversary ceremony, controversial but necessary, was celebrated not only by those who work at the Pentagon but with a nationwide moment of shared silence on September 11, 2002. As life continues on, did the terrorist events provide some "lessons learned" to be implemented for our next attack?

War on Terrorism in the "Battlefield of the Mind"

> *People are never helped in their suffering by what they think for themselves, but only by revelation of a wisdom greater than their own. It is this which lifts them out of their distress.*[18]
>
> —C.G. Jung

Now that the different phases of terrorism have been described, it is important to take a closer look at what happens to people during their

instinctual "fight or flight" reactions to a terrorist attack. Why do people react differently to the same terrorist event? How can one person behave heroically and another run for his or her life? Different populations of people may also respond in different ways to terrorist events. But how these symptoms are expressed, recognized, and handled may determine how they affect people over the long-term, according to the RAND Center for Domestic and International Health Security.[19]

Research shows that for some people, the consequences of a traumatic terrorist event may be severe and persistent. For many others, the symptoms are likely to subside over time.[20] But even though the emotional responses are ephemeral, they could trigger important behavioral responses to terrorist events, in both the short and long-term. For individuals and groups alike, the behavioral consequences of terrorist victims could be either positive or negative.

Positive responses could include connecting more with others, taking a colleague to a counseling session, or just viewing the disaster site together as well as taking appropriate safety precautions and avoiding unhealthy or risky behaviors. Negative responses could include excessive alcohol consumption, increased anxiety, functioning less productively at work, or losing confidence in society and government. The consequences could vary depending on the characteristics of the people exposed to the trauma, the nature of the trauma to which they are exposed, the extent of exposure, and the nature and extent of support they receive afterward.[21]

We also know from psychological theory that different ways of perceiving and interpreting risk will influence people's emotional and behavioral responses to that risk. Thus, it is vital to consider how risk is communicated to the public, since this can influence the ability and willingness of individuals and communities to follow response strategies, precautions, and evacuation instructions.[22]

Terrorism, once a foreign concept, has now become too real for America. With a terrorist attack list including the Khobar Towers, the Nairobi Embassy, U.S.S. *Cole* attack, September 11, 2001, the subsequent anthrax attacks in the postal system, sniper attacks, and even a local, Alabama medical missionary killed in Yemen: tragedy has hit home.

Why, then, is it important to study human reactions to disaster or terrorism? Psychological studies show a link between experiencing terrorist events and later mental health issues for many victims of

terrorism; especially those who were injured, directly witnessed the death of others, or experienced the loss of family members or friends.[23] Rescue workers and caretakers of the injured and bereaved may also experience significant mental distress. In addition, even those who watched the horror unfold on their television screens may experience strong psychological reactions. During a terrorist attack, psychological casualties will virtually always outnumber the physical casualties.

It has been estimated that somewhere between 9 percent and 35 percent of those directly exposed to traumatic events such as disasters and terrorism will develop significant posttraumatic psychological distress such as anxiety, grief, anger, rage, insomnia, worry about loved ones and a reluctance to travel. However, some individuals have demonstrated their resiliency and focus upon what really matters in their lives in the aftermath of the attacks. Research from the American Psychological Association reveals that "It would be a mistake to assume that time is healing everyone's emotional wounds at the same rate."[24]

As an example, following the Sarin gas attacks in the Tokyo subway system, where 12 people died, and 900 received medical treatment, over 9,000 people presented with psychological complaints, a ratio of 1:10 in the local emergency room. This volume of "walking worried" patients with emergency symptoms, which were either real or perceived to be real, overwhelmed the medical system. Today in Japan, 18 percent of the people who responded to a survey (1,200 out of 5,000) said they still experience flashbacks from the Sarin attack. Another example is the Oklahoma City terrorist bombing where there were 168 fatalities, but 8,898 individuals pursued counseling, crisis intervention, or support groups; a ratio of 1:53.[25] Are community services available to handle those in need? Most community disaster programs do not address treatment and management of the large numbers of the "walking worried" on psychological support and mental health services.

While terrorism is not new, its prevalence against Americans is increasing. In January 2002, Al Qaeda documents revealed plans to attack power plants and transportation centers throughout the United States. As recently as December 2002, an Islamic radical terrorist in a Yemeni hospital killed three American volunteer medical missionaries. The attacker was quoted to say that he "would be closer to God if he killed the Americans."[26]

With these blatant threats and attacks increasing within the U.S. borders and against its embassies and people, it is important to respond with training to increase the hardiness of the individuals on the front lines of these crises: the U.S. military and employees of the State Department and CIA. Any effective response to such crises simply must mandate both psychological and physical intervention.[27] Nunn, Lugar, and Domenici's *Defense Against Weapons of Mass Destruction Act of 1996* mandates the enhancement of domestic preparedness and response to capabilities in the wake of attack against the United States using weapons of mass destruction (WMD).

Although a small component, provisions are made for psychological crisis intervention with both emergency responders and primary civilian victim populations. Red Cross Mental Health Specialist and Registered Nurse, Diane Myers notes that only about 5 percent of federally sponsored courses on responding to WMD and terrorism include mental health-related topics. According to the Department of Defense, the psychological response to WMD and terrorism must be a seamless continuum of care consisting of diverse emergency mental health technologies.[28]

Yet how do we get this training to the entire Department of Defense (DOD) system? One facet of care is Critical Incident Stress Management (CISM),[29] consisting of crisis interventions suited for individuals, small groups, large groups, families, and organizations. Follow-up and referral services for more formal psychological assessment and treatment are an integral part of this system. Other training, such as resiliency or hardiness, is vital for the psychological well-being of our military and State Department personnel.[30]

In order to ensure that this resiliency training will occur will take a concerted effort of the chaplains, the commanders who have seen the stress of battle and terrorism, family programs, the military and civilian mental health community, and the dedication of each of the members to participate and create his or her own personal survival plan.

Dr. Al Siebert, renowned author of *The Survivor Personality,* has done resiliency training with Navy personnel over the years. His research shows that individuals who are survivors listen and observe difficult people, are open to change, and have a faith in something or someone greater than themselves. After many interviews with former prisoners of war (POWs), he has found that survivors have some characteristics in

common: patriotism, a faith in God or higher power, an active imagination and willingness to be creative, and the ability to transcend one's own situation and pain. These qualities can be built into training for State Department personnel as well as military members to help them understand the importance of creating a positive state of mind, no matter what your circumstances.[31]

General Robbie Risner's book, *The Passing of the Night,* confirms these observations. Those who survived against all odds made a commitment to survive and were supportive of other people in the same situation. As a group, the survivors believed that they would be rescued and not forgotten by the United States. The concept of "united we stand" worked for the POWs of the Vietnam War. So what can we learn from their experiences?

Personal Accounts from Victims of Terrorism

> *All sorrows can be borne if you put them into a story or tell a story about them.* [32]
>
> —Isak Dinesen
>
> *If you're going through hell, keep going.*[33]
>
> —Winston Churchill

Human beings need to view the world as a predictable, orderly, and controllable place, psychologists indicate. The advent of terrorism was a concept outside the frame of reference of most Americans as it blared from our television sets on September 11, 200l. Trying to come to grips with wide-scale terrorist events can trigger immediate and long-term psychological repercussions for some individuals. If the fear of attacks becomes sufficiently crippling, the fright grows into a paralyzing sense of impending doom for a civilian population.[34] The aftereffects can lead to dread, vulnerability, grief and despair.

Or conversely, they can evoke determination and resolve, as when ordinary U.S. citizens go about their normal activities with a renewed sense of purpose and direction. This is an acknowledgement that a free society has the right to go about their usual routine. [35]

In preparing to write this chapter, I had the opportunity to interview a member of the State Department (DOS), the Central Intelligence Agency

(CIA) and numerous members of the Air Force and Army. Each of their experiences at the Khobar Towers, Nairobi Embassy, USAF Base in Greece, Chilean baseball game (consisting of American Embassy personnel) and Pentagon attacks are vastly different from each other. The common thread woven through each individual story was a normal response to an abnormal situation.

All fifteen subjects experienced terrorist attacks even though, initially, the threat didn't appear to be strong; their responses were due to their training or lack of training. Today, some continue to live with Post-Traumatic Stress Disorder (PTSD); time, family support, telling their story, and distance from the trauma site have been the most helpful for each of them. During interviews with five of the subjects, anxiety, intrusive images, guilt, and tear-filled eyes suggest strong emotional reactions to their experiences as terrorist targets. Due to these responses, it appears that the military, CIA, and State Department sorely need resiliency training for their personnel to help them "bounce back" from their traumatic experiences. Resiliency training now utilized by the U.S. Navy may be a key factor in creating healthier military and other government personnel who experience high-risk activities as part of their federal duty and careers.

In general, most survivors of extraordinary trauma undergo normal stress reactions for several weeks. Such reactions fall into four broad categories:

1. **Emotional reactions** – temporary feelings of fear, shock denial, grief, anger, resentment, guilt, shame, helplessness, and detachment from significant others in their lives.

2. **Cognitive reactions** – confusion, indecisiveness, worry, disorientation, difficulty remembering and concentrating, shortened attention span, self-blame and unwanted memories.

3. **Physical reactions** – tension, nausea, bodily aches and pains, change in libido, nervousness, sleepiness, insomnia, hyper-arousal symptoms like rapid breathing, sweating, being easily startled, and panic attacks.

4. **Interpersonal reactions** – distrust, irritability, withdrawal, isolation, feelings of abandonment or rejection, being judgmental, over-controlling or distant.[36]

Psychologists believe that how someone has coped with past crises will determine how they will handle newer ones. If individuals have successfully worked through stressful circumstances in the past, they may find coping easier. I interviewed a Pentagon survivor who has experienced many traumatic experiences as an Air Force Special Operations pilot. He was psychologically equipped to remain calm during the attack and assist those without training during the building evacuation.[37] Three other military survivors calmly left the building, called home to reassure family members, and realized there was nothing more they could do to help. They were encouraged to leave the area while medical personnel attended to the wounded and search and rescue teams could complete their tasks.[38]

As these interviews indicate, there is no "universal standard" pattern of reacting to inordinate stress. It is unclear how many survivors will develop chronic psychiatric illness and how many will resolve spontaneously.[39]

I also discovered that five Pentagon survivors who are military members had been in Kosovo and other wartime conflicts prior to this attack. The Pentagon attack was not a difficult or traumatic event for them since they had specific training in building evacuation, personal security plans and prior traumatic incidents they had experienced and overcome. The sniper attacks in the Washington D.C. area were more stressful for three of the subjects who had children or friends with children due to the possible injury of their own family and friends who live in the Capital City area.[40]

There's also no time clock to measure how long acute stress reactions are considered normal, or to signal when they become abnormal. The length of time required for recovery is an individual matter, influenced by the degree of exposure, personal characteristics, past history, concurrent circumstances and intensity of loss. When loss of life of a loved one or friend is involved, and/or substantial property damage is sustained, recovery will take longer.[41]

The RAND Corporation conducted a survey of U.S. households three to five days following the terrorist attacks of September 11, 2001. Television may have played a role in increasing the stress levels of adults:

those who watched the most television reported the most stress. This study also reported that almost 90 percent turned to others for social support: their religion gave them comfort as did group activities such as memorials or vigils, which can provide a sense of community.[42]

Four survivors of the Pentagon attack mentioned that they experienced some sleep disturbances, shock, and disorientation, but they were clearly told to return to the Pentagon on the following day and responded without anxiety. Another survivor was called back to the Pentagon at 11:30 p.m. that same evening, tasked by the Secretary of Defense to determine the cost of the U.S. going to war in Afghanistan in retaliation for the attack! At first, he was amazed that he had to return so quickly to the Pentagon. Yet, he knew his job was vital to national security; his committee worked for 5 straight days on a budget for the President and Congress to consider the cost of waging a war, to repair the Pentagon, and other homeland security measures.[43] This Air Force officer had a purpose and the threat of additional terrorism did not cloud his sense of duty.

Another military survivor who was severely injured during the Khobar barracks bombing in Saudi Arabia in 1996, where 19 Americans were killed, continues to undergo numerous surgeries for his eyes seven years later. This individual did not have an opportunity to talk to a chaplain or mental health officer about his experience since it was not available to him in Saudi Arabia at that time. He still serves in the U.S. Air Force today because, as he stated, "of his sense of duty." He is determined to know the building evacuation routes for each building he enters today.

In spite of the scars and cuts on his body, he finds comfort from the support of his family and a few fellow survivors he meets in the Air Force.[44] In spite of the lack of building evacuation exercises prior to the attack, the serious physical injuries he received and perceived lack of psychological support, he is a survivor.[45] What is his advice to other military members? He strongly recommends that individuals insist upon evacuation routes posted and practiced on posts and bases and if attacked, talk about it with professionals to help release some of the psychological terror and panic. His attackers were never brought to trial and he angrily stated that he believes the terrorists "got away with murder."[46]

Normal Versus Abnormal Reactions

> *A sign of health is that we don't become undone by fear and trembling, but we take it as a message that it's time to stop struggling and look directly at what's threatening us.*[47]
>
> —Pema Chodron

What else can we learn from survivors of terrorist events? Some survivors suffer from Post-Traumatic Stress Disorder (PTSD), a psychiatric disorder that can occur after life-threatening events such as combat, natural disasters, major accidents, terrorist attacks, or violent personal assaults such as rape.[48] PTSD victims may experience vivid flashbacks and nightmares, feel detached or estranged, have sleep and appetite disturbances, survivor guilt and hyper-alertness that significantly impairs their quality of life.[49] Most people exposed to trauma will experience some of the symptoms of PTSD in the days and weeks following exposure. Data suggest that roughly 8 percent of men and 20 percent of women will go on to develop PTSD, and nearly 39 percent will develop a chronic form of significant post traumatic psychological distress that may persist throughout their lifetimes.[50]

PTSD is identified by clear biological and psychological changes. It is often complicated by related disorders such as substance abuse, depression, memory and cognition problems, occupational instability, marital problems and divorce, family discord, and/or parenting difficulties. Personal loss of loved ones or friends and life threatening danger from intentional human violence are among the factors that increase the risk of lasting readjustment problems. These problems include: loss of home, valued possessions, neighborhood or community; exposure to gruesome death; exposure to toxic contamination; or intense emotional and physical demands from fatigue, sleep deprivation, or harsh weather.[51]

These are the conditions of military personnel in wartime situations, the CIA and State Department under attack, search and rescue workers who help disaster victims – fire fighters, police, emergency medical technicians – and they are at risk for secondary traumatization. Also known as vicarious traumatization, compassion fatigue, and burn out, the symptoms are similar to, but less severe than, full-blown PTSD.[52] Yet

they do affect the quality of life and careers of even those with considerable training and experience.

Nurses, physicians, and mental health professionals may also be adversely affected by an overdose of victim suffering. If one works with, cares for, or is exposed to the stories of many traumatized victims, it is important to anticipate the possibility of secondary traumatization and take steps to protect oneself at the first sign of trouble. Exposure to the images or stories of multiple disaster victims, one's sensitivity and empathy for their suffering and any unresolved emotional issues of one's own that relate to the suffering at hand can be major risk factors for secondary traumatization. Called "Soldier's Heart" during the Civil War, battle fatigue or "shell-shock" during World War I, it is anticipated to last for a small amount of time.[53] When an individual can't stop talking or thinking about the event to the point of preoccupation or obsession, the individual should be referred to a mental health professional for additional assessment.

An example of primary and secondary PTSD traumatization was the experience of a State Department survivor in attacks in Africa. As an engineer, the survivor evaluated the Beirut Embassy terrorist bombing and its aftermath in 1984. No critical incident stress debriefing (CISD) or other psychological support to any survivors following this tragedy. In 1998, this same engineer worked at the Nairobi Embassy when it was destroyed by Al Qaeda terrorists. During this attack, a truck bomb killed 224 people, to include 12 Americans, and injured over 5,000 Kenyans, according to Mental Health Services Chief, Dr. Harlan Wadley.[54]

The engineer was out of his office at the exact time of the bombing, but personally knew all the Embassy workers who died. He, by default, immediately became the leader of the search and rescue team at the bombsite and continued to search for survivors and the recovery of body parts for the 48 hours following the bombing. He did not rest, eat in a healthy manner, have adequate tools to complete the search or protect his own health. His respiratory functioning and lungs were damaged from smoke and chemical inhalation and his back and rotator cuffs were permanently damaged from lifting mangled pieces of the building, in a desperate attempt to find injured victims.[55]

For his own psychological survival, there was limited mental health assistance in Nairobi for personnel or their families: survivor guilt,

flashbacks, and fear of individuals who appeared to be of the same cultural background as the perpetrators still haunt this subject five years later.[56] This subject was able to attend the memorial services of those who died in the line of duty and traveled to New York for the trial and conviction of the perpetrators found guilty of this terrorist act. It was healing to attend the sentencing of the terrorists, but that did not erase the lingering psychological effects.

Numerous Nairobi Embassy survivors are more emotional, have undergone personality and behavior changes, and require anti-depressant medication for their PTSD symptoms.[57] Survivors were not monitored at their next assignment, Dr. Wadley added, and follow-up consultation during the following year was not encouraged; survivors were on their own. No protocol or standard of care had been established since psychiatrists were not trained in trauma counseling; the State Department now questions the wisdom of these actions since lawsuits claiming negligence by the Department persist to this day. As a result of the Nairobi attack, the State Department has initiated mandatory psychiatric counseling each year for survivors of attacks to determine the presence of any mental health issues.[58]

For survivors of terrorist events, there are many strategies for coping with extraordinary stress. These strategies have effectively reduced anxiety and improved the quality of life for the fifteen individuals I interviewed. First of all, the survivors realized that they were having a normal reaction to an abnormal event. They thought back to what worked in the past for them when they needed to overcome adversity. They created structure by sticking to their usual routine and activities. They kept a journal or diary; writing was a catharsis for their spirit.[59]

They prayed, attended worship services, or whatever deepened their faith. For example: in his book, *Return With Honor*, Scott O'Grady, USAF Captain shot down in Bosnia, stated that when he started praying, he discovered he wasn't doing a solo; he had joined a huge chorus; he could hear prayers for him from throughout the world. Afterward he said, "Those six days in Bosnia were a religious retreat for me, a total spiritual renewal."[60]

Other terrorist survivors stated that they worked in a garden to connect with the earth and experienced the great outdoors for fresh air and solitude after their trauma. They treated themselves to a therapeutic

massage, ate healthy foods, slept, and limited redundant media coverage. The survivors mourned their losses, acknowledged them, and then began their grief work. They practiced relaxation techniques and learned to meditate. They talked to others and shared their feelings; they became better listeners, too. And most importantly, they all agreed to keep a positive but realistic outlook – it takes time to heal. They postponed major life decisions to avoid potentially strong stressors, used humor to lighten their load, and spent quality time with family and friends.[61]

Granted, we are in uncharted territory, but our institutions of democracy are intact and we are taking steps intended to combat terrorism and restore security. Are we providing resiliency training to those who serve on the front line of defense?

Helping Lessen the Psychological Impact of Terrorist Attacks

> *Surviving means that you gain strength, courage and confidence by every experience in which you really stop to look fear in the face. You are able to say to yourself, "I lived through all this horror. I can take the next thing that comes along."*[62]
>
> —Eleanor Roosevelt

Survivors of torturous experiences have emphatically stated that the will to live cannot be taught. Survivor qualities must be developed beforehand so they can be relied upon when needed. Some of the ways that lead to survival, according to Dr. Al Siebert, include: suppress strong feelings and use common sense, adapt to the new reality, be able to function alone without asking for approval from other people, find humor, make a deep emotional commitment to keep going, plan for a pleasant future and try to maintain contact with others.[63]

Disaster research indicates that the fabric of communities and of society can provide resiliency and protection against psychological consequences. Probably the best protective factors are the communities in which victims live, work, and interact. It has been suggested that closing schools, churches, or other social institutions, quarantining individuals without letting them communicate with the outside world, can cause psychological harm.[64] The community must provide appropriate

information and reassurance while maintaining an ongoing surveillance of threats.

This may require an expansion of the concepts of emergency responders, trauma counselors, Red Cross volunteers, mental health institutions and universities. In the future, emergency response strategies need to incorporate each of these service-provider roles. For example, psychiatrists, psychologists, and health specialists are needed to address severe emotional and behavioral consequences of traumatic events, but have no specialized training in emergency response. Dr. Harlan Wadley from the State Department mentioned that all psychiatrists should have emergency response training, but few medical schools have developed curriculum to meet that need.[65]

Likewise, although primary care and emergency care workers are responsible for tending to the survivors of terrorist attacks, their priority is assessing and treating physical, not psychological injuries. Policymakers should consider ways to capitalize on the strengths of a broader range of social supports and institutions beyond the health care system. Deploying emergency mental health personnel to the site of the attack is insufficient. A broader capability is needed – to ensure an effective workforce during the threat of terrorism, to prevent mass panic that can seriously weaken the strength of our society and economy.[66]

To help lessen the psychological impact of terrorist attacks, Homeland Security policymakers should view employers, religious organizations, and schools as part of the response team and create roles for them in mitigating any potential long-term psychological harm. With proper planning, better prevention and optimum response strategies, Americans from many walks of life, policymakers, clinicians, emergency response workers and community leaders, can work together to minimize the psychological effects of terrorism and maximize the national resistance to it.[67]

How can diverse agencies work together following a terrorist event? An example of an impromptu but highly effective response strategy took place in Chile a few years ago. When a terrorist's bomb, concealed in a baseball bat at a public stadium exploded near the U.S. embassy team, a CIA agent prepared a special dinner for the following evening and insisted that all Americans from the Embassy and school attend. She quickly prepared food for the "mandatory dinner party." The embassy team and their families were able to "pick up the pieces" of their lives with a shared

meal, shared stories of sadness and threats against their lives. Thus, they were fortified by eating together and talking about their feelings and the previous day's attack.[68]

Response strategies for victims need to go into effect immediately following any type of terrorist event. By intervening as soon as their symptoms appear, physicians, psychologists, and other clinicians were able to help victims identify normal stress reactions and recommended steps to cope effectively. Counselors in the Washington DC and New York areas quickly responded with coping materials and resources for the first responder community and families of those who were injured or killed. Professional counseling organizations prepared information for schools and community gatherings nationwide to discuss how to talk to children and the elderly about anxiety and terrorism.[69]

Recommendations and Conclusions

In response to the terrorism of the September 11 attack, Doctors Everly and Mitchell recommend the following "Ten Commandments of Psychological Response":[70]

1. Never forget that the terrorist act is designed to create psychological instability. Death and destruction are merely a means to an end. Terrorism is psychological warfare.
2. DOD, DOS and civilian communities need to establish joint intervention hotlines and walk-in crisis facilities for those directly or indirectly affected by terrorism. Psychological support and restoration of a sense of community is essential.
3. Pre-incident psychological resiliency training and ongoing support during and after the terrorist attack is important for front line emergency personnel, CIA, FBI, DOS and DOD. Families need to be included in all aspects of these processes. The psychological state of mind of these personnel will have direct effects upon their ability to perform their necessary jobs during this stressful time and upon the physical and mental health of the targeted population.

4. Concerns about future attacks can heighten anxiety; correct information is power. Collaborate with mass media for the dissemination of accurate and ongoing information to all involved. Credible information calms the sense of chaos and provides rumor control. Age-appropriate reading and community activities help children cope with the situation. Limit continuous monitoring of television and radio coverage of the event, particularly around children who may have difficulty seeing vivid pictures of the event.
5. Take steps to re-establish a sense of physical safety for the public. Widely publicize these efforts for children, the elderly and those who are sick.
6. Establish a network of local political, educational, medical, economic, and religious leaders to calm fears, provide crisis intervention and instill hope.
7. Re-establish normal communication, transportation, school and work schedules as soon as possible. The longer and greater the disruption, the greater the public's perceived risk and lack of safety.
8. Symbols are a means of re-establishing community cohesion. Just as terrorists target locations that symbolize a part of America they despise, a community can use flags, bumper stickers, and billboards as a sign of unity.
9. Initiate rituals to honor the dead, the survivors, and rescuers. Provide opportunities for those not directly affected to help with donations of money, food, clothing, blood, etc. Communicate that to carry on and succeed in life honors the dead. Otherwise, the terrorists are victorious.
10. Do no harm. Don't interfere with people's natural recovery mechanisms or interfere with tactical assessment and rescue efforts.[71]

These ten recommendations create a nationwide standard of care for the survivors of terrorist attacks and their caregivers.

In schools and the military, most disaster plans are designed by an individual or a committee and are never exercised with all key components including the local area, community, state and other agencies. It will take a conscious effort to practice these plans before an attack occurs in the near future.

Military Disaster Exercises include four phases in the disaster plan: threat/risk assessment of the area; secondly, mitigation, or diagnosis of the problem areas, prioritizing the needs; third, response, or test the plan, having checklists and role cards to remind individuals of their responsibilities during and following an attack; and last of all, recovery – the return to the pre-disaster state to re-evaluate the weak areas. Role and responsibilities of all participants are planned and executed for each of the four phases.

Following the disaster response exercise, continuous staff training should be included for additional areas needing attention while working together with all key agencies fighting terrorism. This is the first time that the U.S. has developed a response plan to include the military, local, state and federal levels for terrorist attacks. Agencies such as the Red Cross, Homeland Security, Federal Emergency Management Administration (FEMA), religious communities, and media all play a vital role. When these agencies can assist personnel in creating a personal survival plan, it will include ways to: regain emotional balance, adapt and cope with the immediate situation; thrive by learning and find the gift in each bit of adversity, no matter how unfair it seems. One can learn to survive and thrive by converting disaster into good fortune, Dr. Siebert states.[72]

How can this training be accomplished? Hardiness and resiliency programs are already in place and utilized by various U.S. military survival schools, according to Lieutenant Colonel Frank Heyl, USAF (Retired). Survival skills taught to pilots would benefit those on the front line against terrorism as we fall victim to attack.[73] Scott O'Grady is an example of one who utilized his survival skills in a grim situation. He stated, "For the record, I don't consider myself a hero. I was in the wrong place at the wrong time. As I huddled in those woods, I was a scared guy named Scott, getting by on his wits, not a fighter pilot. How people fare in survival situations is predicted by their strength, their determination and their power of will."[74]

The military needs additional stress management, survival and resiliency training in addition to that taught by Operation Solace, The National Guard's Trained Crisis Responder Program, and the Navy's Survive and Thrive training. Classes must be taught during orientation or basic training and at other times in one's career for the real test of life. Training can be created by psychologists, psychiatrists, and survival experts in both the military and civilian communities in order to develop psychological toughness in military members and DOS employees, a necessity in today's terrorist environment. Having a survivor speak of his or her experience would drive the importance home to class participants.

This type of training has not reached all branches or members of the military and is inconsistently taught to State Department employees. Psychological survival and resiliency training must be institutionalized for all branches; research shows that individuals with resiliency skills are less likely to succumb to divorce, substance abuse, depression, violence, suicidal tendencies and other problems when they develop an inner nature of survival skills. People can develop positive attitudes, ways of coping with adversity and skills to help them work through rough experiences without becoming psychological casualties. A positive attitude, Dr. Siebert states, is far more important for survival than having a "Rambo" survival knife.[75] As a former Marine of World War II described his own survivor personality: "All one needs is the will to survive – and the skill to cooperate with others, be dependable and self-disciplined."[76]

Notes

1. Elizabeth Kubler-Ross. On-line. Internet. Available from http://www.livinglife fully.com/adversity2.html.

2. National Guard Trained Crisis Responder (TCR) Course: Terrorism and Disaster Response, 7.

3. U.S. Department of Justice, 1996, 3.

4. Ibid.

5. National Guard Trained Crisis Responder (TCR) Course: Terrorism and Disaster Response, 19.

6. Ibid., 8.

7. Ibid.

8. Dr. Al Siebert, *The Survivor Personality*. New York: Perigee Publishing, 237.

9. *International Journal of Emergency Health*, 2001, 3(3), 133-135.

10. Ibid.

11. Interview with survivor of terrorist attack in Athens, Greece.

12. Ibid.

13. Everly and Mitchell, *National Guard TCR Course: Terrorism and Disaster Response*, 19.

14. American Red Cross Disaster Mental Health statistics from the 11 Sept terrorist attacks. (e-mail).

15. Wilson and Harel, *Human Adaptation to Extreme Stress: From Holocaust to Vietnam.* New York: Plenum Series, 58.

16. Everly and Mitchell, *National Guard TCR Course: Terrorism and Disaster Response*: 27.

17. Ibid.

18. Carl Jung quote on adversity. On-line. Internet. Available from http://www. livinglifefully.com/adversity2.html.

19. RAND Center for Domestic and International Health Security. *The Path of Greatest Resilience.* On-line. Internet. Available from http://www.rand.org/publications/rand review/issues/rr.o8.02/resilience.html.

20. RAND Center for Domestic and International Health Security. On-line. Internet. Available from http://www.rand.org.

21. Conversations in Care. *Communicating during a crisis*. On-line. Internet. Available from http://www.conversationsincare.org/web book/chapter03.html.

22. Human Behavior and WMD Crisis/Risk Communication Workshop.

23. K. Nader. "Terrorism: September 11, 2001, Trauma, Grief and Recovery." On-line. Internet. Available from http://www.giftfromwithin.org

24. American Psychological Association. On-line. Internet. Available from http://www.apa. org.

25. *National Guard TCR Course: Terrorism and Disaster Response*, 20.

26. *Montgomery Advertiser*, December 27, 2002.

27. *National Guard TCR Course: Terrorism and Disaster Response*, 21.

28. Department of Defense, 2001 report on WMD.

29. Terrorism and its after effects. On-line. Internet. Available from http://www.nimh.nih.gov.

30. Ibid.

31. Quote from Isak Dinesen. On-line. Internet. Available from http://www.living lifefully.com/adversity2.html.

32. Quote from Winston Churchill. On-line. Internet. Available from http://pprsites.tripod.com/pprquotes/PPR-Quotes-DifficultTimes.htm.

33. Wilson and Harel, *Human Adaptation to Extreme Stress: From Holocaust to Vietnam.* New York: Plenum Series, 136.

34. Interview with Lt Col Tracy Amos. Air War College, Dec 2002.

35. Interview with Lt Cols Deborah Gibbs and Denise Schultz; Air War College, Dec 2002.

36. Deployment Health Clinical Center. On-line. Internet. Available from http://www.pdhealth.mil/wot/fact_sheet1.asp.

37. Interview with Lt Cols Denise Schultz and Devin Cate; Air War College, December 2002.

38. RAND Corporation. On-line. Internet. Available from http://www.rand.org.

39. Interview with Lt Col Tony Thompson, Air War College, Dec 2002.

40. Interview with TSgt Andre Stanton, Hill AFB, Dec 2002.

41. Ibid.

42. Dr. Frank Ochberg, 9-11 Anniversary Reactions. On-line. Internet. Available from http://www.giftfromwithin.org.

43. Interview with Lt Col Tony Thompson, Air War College, Dec 2002.

44. RAND Corporation. Helping Each Other Cope. On-line. Internet. Available from http://www.rand.org.

45. American Psychology Association. On-line. Internet. Available from http://www.apa.org.

46. Interview with TSgt Andre Stanton, Hill AFB, Dec 2002.

47. Quote from Pema Chodron. On-line. Internet. Available from http://www.livinglifefully.com/adversity2.html.

48. Dealing with Trauma. On-line. Internet. Available from http://www.suu.edu/ss/wellness/trauma.html.

49. John P. Wilson: *Human Adaptation to Extreme Stress: From the Holocaust to Vietnam*, 135.

50. Post Traumatic Stress Disorder: New Treatment. On-line. Internet. Available from http://www.focusondepression.com.

51. Interview with Dr. Harlan Wadley, U.S. State Department, Dec 2002.

52. Ibid.

53. Ibid.

54. Interview with Lee Reed, State Department employee, Air War College, Dec 2002.

55. Ibid.

56. Ibid.

57. International Society for Traumatic Stress Studies. On-line. Internet. Available from http://www.istss.org.

58. *The Path of Greatest Resilience*. On-line. Internet. Available from http://www.rand.org.

59. Al Siebert, *The Survivor Personality*. New York: Perigee Publishing, 224-228.

60. Ibid.

61. Ibid.

62. Eleanor Roosevelt quote. On-line. Internet. Available from http://pprsites.tripod.com/pprquotes/PPR-Quotes-DifficultTimes.htm.

63. Dr. Al Siebert, *The Survivor Personality*. New York: Perigee Publishing, 95.

64. Scott O'Grady, *Return With Honor*. New York: Doubleday, 1995, 111-113.

65. Hopkins Study Dispels "Panic" Myth. On-line. Internet. Available from http://www.jhsph.edu/Press_Room.

66. National Guard Trained Crisis Responder (TCR) Course, 27.

67. Interview with Dorothy LeBois, CIA employee, Air War College, Dec 2002.

68. Ibid.

69. National Guard Trained Crisis Responder (TCR) Course: Terrorism and Disaster Response, 27.

70. Ibid, 28.

71. Dr. Al Siebert. *The Survivor Personality*, New York: Perigee Publishing, 266.

72. Ibid.

73. Frank Heyl, Phone interview, 10 Jan 03.

74. Scott O'Grady, *Return With Honor*. New York: Doubleday: 1995, 111-113.

75. Dr. Al Siebert, *The Survivor Personality*, New York: Perigee Publishing, 176.

76. John P. Wilson: *Human Adaptation to Extreme Stress: From the Holocaust to Vietnam*, 136.

CHAPTER 10

Canada And The United States - Defense Cooperation In U.S. Northern Command?

David B. Millar

Introduction

> *Our friendship has no limit. Generation after generation, we have traveled many difficult miles together. Side-by-side, we have lived through many dark times, always firm in our shared resolve to vanquish any threat to freedom and justice.*
>
> —Jean Chrétien, Prime Minister of Canada
> September 14, 2001

In the aftermath of September 11th, it became apparent that North America was no longer insulated from the threats that it had once assumed would never reach its borders. Canadians were equally startled as they came to recognize, literally for the first time in their lives and in the history of their country, that their freedom and safety were in jeopardy. This revelation is particularly poignant in a nation that tends to take its national security for granted, relying almost exclusively on its benevolent neighbor to ward off threats. This ambivalence, however, quickly evaporated following the terrorists attacks as Canadians came to realize that a threat upon the United States was ostensibly a threat to Canada. Security took on a wholly new emphasis and the calls to come to the defense of the United States and North America were resounding. The sudden outpouring of nationalism brought to the forefront the historic ties between the two nations annunciated over 62 years ago when President Roosevelt and Prime Minister King created the first defense arrangements that would eventually lead to the Canada/U.S. North American Aerospace

Defense Command (NORAD) Agreement. Today, in recognition of the enormity of the threat to North America and in fulfillment of its obligations to the U.S., the Canadian Government has undertaken sweeping security measures analogous to the U.S. initiatives on Homeland Security. Indeed, the majority of the measures have been in concert with the U.S. and the most notable have been consecrated publicly as a further attestation of the bond between the two nations. Yet, there has been one striking exception; none of the measures include a military response. The U.S. has established Homeland Defense with U.S. Northern Command (NORTHCOM) as its flagship against terrorist threats to North America. However, there has not been a similar pronouncement by Canada to join the U.S. initiative by contributing forces to the kind of collective defense that has historically united the two nations in times of crisis. Although it would seem intuitive that Canada would accept a U.S. offer to participate in continental security, using the opportunity to broaden its existing NORAD contribution, NORTHCOM stood up on October 1, 2002, without contribution from Canadian land, sea, or air forces. Why didn't Canada provide military forces to the newly constituted NORTHCOM in light of the threat to its own security?

The U.S. has naturally taken the lead to protect itself from terrorism and, as a result, has thrown a security blanket over North America under the auspices of Homeland Defense. Canada is implicated because its territory is included within the proclaimed security zone and, by default, so is its sovereignty. The dilemma for Canada became whether to formalize an arrangement with the U.S. to assert control of its sovereignty by assigning forces to NORTHCOM, or to abstain from participation because to do otherwise would completely relegate Canadian sovereignty to the exclusive control of the United States. Canada elected the latter course of action because its sovereignty is more important than its physical security.

The purpose of this chapter is to show in light of today's strategic environment that Canada's decision not to participate in NORTHCOM may in fact jeopardize its sovereignty. First, it is important to provide the background on Homeland Defense vis-à-vis the Canada/U.S. relationship and set the stage of the debate between sovereignty and security that Canada faced when offered to participate in NORTHCOM. Then, this analysis elucidates the priority Canada places on sovereignty by

describing the broad security initiatives undertaken following September 11th, which noticeably preclude the military. The lack of military involvement is explained by showcasing Canadian misgivings towards NORAD and national missile defense, which serve as a precursor to understanding the relevant issues pertaining to NORTHCOM. Further, this chapter describes the circumstances surrounding Canada's decision not to contribute forces and posits that the decision was based on a presumption the U.S. would continue to honor Canadian sovereignty despite the Homeland Defense mission. It will be shown, however, that the U.S. attitude towards its bilateral and multilateral agreements is changing and that the U.S. Government is prepared to act unilaterally to protect its own national interests above those of other nations. Finally, this analysis concludes that Canada should join NORTHCOM to preserve its sovereignty and security, alongside the United States.

U.S. Northern Command (NORTHCOM) and the Canada/U.S. Relationship

NORTHCOM

On October 1, 2002, the Deputy Secretary of Defense, Mr. Wolfowitz, along with the Chairman of the Joints Chiefs of Staff, Gen Meyers, inaugurated the much heralded NORTHCOM, the newest of the six unified commands within the Department of Defense. The new command is a bold step forward and plays a key role in the war on terrorism alongside the President's recently approved Department of Homeland Security.[1] The implications of NORTHCOM for Canada are equally bold and potentially far-reaching as, for the first time in its history, Canadian territory is consolidated under U.S. unilateral command and control.

Although the creation of NORTHCOM raised the ire of Canadians and remains the focus of media attention and government debate, creating a new unified command is routine within U.S. parlance. As a matter of course, the Chairman of the Joint Chiefs of Staff is charged with the responsibility of routinely reviewing the Unified Command Plan to adapt command and control of U.S. military forces around the world to the evolving security environment. From its inception in 1947, the Unified

Command Plan was created from the success of World War II where command of U.S. operations and forces overseas was centralized under a single commander who was responsible to the Joint Chiefs of Staff. The most characteristic feature of the Unified Command Plan is its geographic orientation. Over the years, successive reviews of the Unified Command Plan have debated the best way to subdivide the world, whether along geographic or functional lines and whether along joint or service lines. Despite a number of perturbations, the orientation has been primarily geographic.[2] This latest review reaffirms the geographic orientation and for the very first time in history includes a command that encompasses the U.S. homeland. Despite the outward similarities to the existing commands, there are unique aspects pertaining to NORTHCOM that set it apart.

NORTHCOM is very different from its sister commands, namely in terms of its relationships, mission, roles and authorities, assigned forces, and area of responsibility. The creation of the new unified command is a part of the larger U.S. effort to defend against terrorism. A two-pronged approach has been undertaken which comprises Homeland Security and Homeland Defense. Homeland Security falls under the auspices of the President's Department of Homeland Security approved by Congress in November 2002. The Department unifies the various separate agencies responsible for domestic security and safety under one centralized command and control organization. The new department is responsible for border and transportation security; emergency preparedness and response under the Federal Emergency Management Agency; chemical, biological, radiological, and nuclear countermeasures; and information analysis and infrastructure protection. On the other hand, Homeland Defense falls under the auspices of the Unified Command Plan with NORTHCOM as the lead Department of Defense agency to command all military forces needed to protect the U.S. against attacks emanating from outside the country. In addition, the Command also serves as an adjunct to the Department of Homeland Security, when called upon.[3]

Historically, defending America's national security interests has been accomplished using forces operating in designated strategic areas overseas. Following September 11th and the creation of NORTHCOM, North America ostensibly became a strategic area with forces operating within the U.S. This implies that military force could be used for internal, domestic security matters. However, following the Civil War, the Posse

Comitatus Act was proclaimed to strictly prohibit such use of the military. Nevertheless, the imperative to combat terrorism is so pervasive that the President and Congress are prepared to exercise the special exigencies within the Act to permit the use of the military in support of NORTHCOM's roles.[4]

NORTHCOM has two distinct roles. The most unique, and the one to which the exigencies of the Posse Comitatus Act will be applied, is civil defense. The role of NORTHCOM in civil defense is very specific; military force will only be invoked upon direction of the President or the Secretary of Defense and if so, it will be subordinate to civil authorities in a supporting role. For the most part, the Department of Homeland Security and its agencies across the U.S. are expected to respond to domestic crisis, in particular, the Federal Emergency Management Agency, which would be the lead agency. In contrast, NORTHCOM's primary mission is homeland defense that encompasses deterrence, prevention, and prosecution of threats and aggression aimed at the U.S. The preponderance of effort and resources will be dedicated to this mission.

However, this will be a challenge because very few forces have been assigned to the new command. The Joint Force Headquarters-Homeland Security, the Joint Task Force-Civil Support, and the Joint Task Force 6 constitute the permanently assigned forces. Consequently, the staff of 700, in its headquarters at Peterson Air Force Base in Colorado Springs, is relegated to monitor and plan for potential, direct attacks against the U.S. In case of attack, other forces will be assigned on an as-required basis depending upon the nature of the emergency.[5]

These unique aspects surrounding the creation of the new Command posed significant challenges to NORTHCOM's viability and, according to its officials, permitted some latitude to consider innovative solutions, such as including forces from the surrounding nations.[6] NORTHCOM's Area of Responsibility (AOR) encompasses the continental territory of the U.S., Alaska, Mexico, and Canada, and extends 500 nautical miles into the surrounding waters emanating from the continent.[7] By definition, the new unified command exercises control of U.S. forces operating in its AOR, which includes Canadian territory. What Canada initially perceived as an encroachment upon its sovereignty instead unfolded into an offer to participate in the defense of North America against terrorism. When Secretary Rumsfeld spoke to the Canadian Senate and House Armed

Forces Committee in February 2002 and acknowledged the success of the NORAD relationship in protecting the air sovereignty of the U.S. and Canada, he posited that:

> [H]e would welcome Canadian participation with both the sea and the land elements, but that it would be up to Canadians to determine whether it was in their national interest to participate...[8]

Such an offer should not have come as a surprise given that command and control of U.S./Canada sovereign air space has been maintained under the auspices of the NORAD Agreement since 1958. Nevertheless, NORTHCOM's established boundaries and roles provoked a certain reticence among Canadian Government officials who have always suspected the NORAD agreement as an abrogation of Canadian sovereignty. The suggestion of a deeper relationship within NORTHCOM served to further exacerbate their concerns about sovereignty.

Sovereignty versus Security

The Combatant Commander of NORTHCOM and NORAD is one in the same person. Indeed, NORAD provides air and space support for the Homeland Defense mission; however, by definition, only those resources and forces owned and operated by the U.S. fall under NORTHCOM's purview. In other words, the Canadian Forces equipment and personnel associated with NORAD are theoretically not a part of the NORTHCOM order of battle, nor are they considered as assigned forces. The same argument has been applied to space and the detection and tracking of ICBMs. This line-in-the-sand has been delineated to placate the perception of any unsanctioned use of Canadian Forces assets. However, in all practicality, if part of NORTHCOM's mission is to deter possible air threats from entering the U.S. and the threat happens to be in Canadian sovereign air space, which ostensibly is within NORAD's purview, intuitively, Canadian Forces assets will be used to engage the threat. As a matter of fact, since September 11th, Canadian Forces CF-18s have been involved in the air intercept of suspect commercial aircraft destined for the U.S., oblivious to whether a NORAD or NORTHCOM mission. The line-in-the-sand is somewhat blurred in the eyes of

Canadian Government officials by the wedding of NORTHCOM and NORAD under the same commander.

Another concern is potential U.S. reaction to a threat emerging from within Canadian sovereign territory. For all intents and purposes, NORTHCOM is responsible for potential threats emanating within the Area of Responsibility that are aimed directly at or pose a threat to the United States.[9] In the case of threats from within Canadian land, sea, and air approaches, U.S. assigned forces will in all likelihood be directed to prosecute them before entering into the U.S., without necessarily seeking the Canadian Government's approval. The ramifications to Canadian sovereignty are significant. Ostensibly, the U.S. becomes the benefactor of Canadian sovereignty under the aegis of the NORTHCOM mandate to protect the U.S. against air, space, land, and sea threats from within the Area of Responsibility. Historically, Canada chose to participate in NORAD to obviate such a circumstance. As an equal partner in the bilateral arrangement, Canada reaped the benefits of being included in the spectrum of capabilities the U.S. military has to offer while, at the same time, asserting command and control over its contribution of equipment, resources, personnel, and, above all, its sovereignty.[10]

At the time of the offer from Secretary Rumsfeld, these concerns and the arguments for and against became further inflamed by the media and incited a public debate in Canada over the potential sublimation of Canadian sovereignty. However, the aggressive schedule set by the United States to declare the new Command operational imposed an artificial constraint within Canada that limited the debate of the pros and cons. Consequently, the initial reticence expressed by government officials quickly turned into reluctance to accept more than the status quo. The government's cautious approach is best understood by examining the events that have characterized the U.S./Canada relationship.

Canada and the U.S.

It has been opined that Canada and the United States are practically synonymous. Both share the same values and ideals at home and abroad, the economies are inextricably linked, the cultures and people are indistinguishable for the most part, and the two countries depend on one another for their mutual security. Some two hundred treaties and agreements legally bind the two nations together and underscore the extent

of the relationship. Economically, $475 billion worth of trade is exchanged annually between the two countries involving over 2 million employees in each country. Canada represents one quarter of U.S. exports, and it imports more goods from the U.S. than the entire European Union and three times more than Japan. The United States is Canada's largest foreign investor, and Canada is the leading market for 38 U.S. states. With the signing of the North American Free Trade Agreement in 1994, the two countries became inseparable economically and culturally to the extent the border is seamless with over 200 million people crossing each year.[11] Militarily, Canada and the United States share a long tradition of cooperation in defending the continent and in fighting side-by-side for the goals and values of freedom and democracy that both uphold. The two countries have fought together in the World Wars, Korea, the Gulf, and in Kosovo. Not just in war, but also in peace, the two countries are seen as one in their peacekeeping endeavors around the world. In terms of defending the North American continent, Canada and the United States are bound together through the NORAD agreement originally signed to act as a shield against the Soviet manned-bomber threat.[12] The symbiotic relationship has been nurtured over time; however, it has not been without hardship, and when examined more closely, reveals a different perspective.

A Relationship in the Making

Canada can be characterized as a nation that has been in continual pursuit of being recognized as a sovereign, independent power by the rest of the world, and in particular, by the United States. However, these ideals have often been curtailed because of a reliance on others for economic prosperity and security. Likewise, the perennial sovereignty movement within French-Canada and the threat of cessation has tempered the Canadian Government's ability to present a strong, unified voice. As a consequence, to achieve domestic appeasement, the government has had to be more conciliatory in its deliberations in its bilateral and multilateral arrangements thus creating the impression that Canada is reluctant to act definitively or aggressively in matters of import. Overall, each of these factors has had a profound influence on shaping how Canada conducts its policy and decision-making, especially in regard to the U.S. and matters

involving security. The degree of influence can be best understood through historic lenses.

Upon its creation as a nation, Canada fell under the British Empire as one of its new colonies in July 1867. Responsible for its domestic affairs, Canada, like the other British colonies, deferred to the Empire for its international relations and foreign affairs. Yet, one of Canada's first aims would be to seek independent recognition of its abilities to govern itself both domestically and internationally. This became a single pursuit of Canada's first Prime Minister, John A. Macdonald, who recognized that independence would have to be gradual and, therefore, he sought a policy to remain subordinate to the empire but not subservient.[13]

While Britain and the rest of the world were building up their arsenals of military strength, Canada pursued its domestic economic interests. A country with vast resources, the key to its power would be its economic potential, not its military capability. After all, the Empire and the Royal Navy were Canada's security guarantee, allowing the leadership to focus on the economy. For Macdonald, this was Canada's opportunity to become worldly recognized through trade, and he concluded the first Canadian trade agreement with France in 1893, not surprising given Canada's French-Canadian origins.[14] Trade with the U.S. continued to expand during this time along with Canada's protection of its industrial growth through tariffs. The unintended consequence was the almost overnight expansion of U.S. ownership of industry within Canada to offset the tariffs. For Canada, this meant stronger economic relations with the U.S. and less dependence on Britain, both economically and in terms of foreign policy.[15]

Canada continued to pursue an independent foreign policy and political equality with Britain by objecting to participate in her imperialistic ambitions and skirmishes. During the Sudan crisis of 1884-1885 when Britain called for assistance, Macdonald remained defiant and did not offer military support where Canada had no interests.[16] This would become a recurring trend for future Prime Ministers. At the time of the Boer War in 1899, Britain appealed to the colonies for assistance. Then Prime Minister Sir Wilfred Laurier was opposed to providing military support. Yet, under a recent euphoria of British sentiment following the Diamond Jubilee, his government was compelled to order 1,000 troops to war with the caveat that the British Government was not to

construe this as a precedent for additional support.[17] This posturing was not only a means to distance Canada from the Empire, but was also necessary to placate the rising anti-British sentiment being expressed by the growing movement of the French-Canadian nationalists in the province of Quebec.[18]

Much to the surprise of the allies, Canadians quickly rose to the call of arms providing half a million soldiers in World War I. The sudden support for Britain was more in recognition of the world crisis than an emotional response to a threat to the Empire. Yet, to continue its insistence on controlling its destiny, the Canadian Government was adamant that it had a part in the decision-making of the war and in the eventual peace negotiations.

Again, these demands were to assert Canada's desire for greater autonomy and also to placate the growing unrest of the French-Canadian population who saw Canadian contribution to the war, especially after conscription was enacted, as a sign of support for imperialism.[19] In the end, Canada was successful at getting a seat at the negotiating tables, surprisingly, despite strong objection from the United States. It was thought the objection was related to Canada's diminutive stature in the realm of high-power diplomacy, although in actual fact, the U.S. was more concerned about an imbalance of British votes.[20]

Nevertheless, the apparent disagreement that Canada perceived did not deter it from asserting itself in the deliberations over President Wilson's League of Nations initiative. Canada became infamous at the fifth League Assembly in 1924 when Canadian Senator Dandurand described Canada as "a fireproof house, far from inflammable materials" in his objection to Article X and collective defense. Although causing considerable consternation among the League delegates, the Senator's analogy accurately portrayed the view of Canadians at this time. In the end, Canada dropped its opposition once the requirement for collective defense became optional. Despite the initial euphoria at the outset of the war, in the aftermath, the Senator's bold assertion reaffirmed the growing isolationist views that would characterize Canadians and Canadian Government policy leading into World War II.[21]

In World War II, the government exercised caution based on its previous lessons learned. In order to appease French-Canadians, the government initially authorized a limited contribution thereby avoiding

conscription. As well, to avoid being over committed, Canada indirectly supported the war effort through initiatives such as training aircrew in Canada under the British Commonwealth Air Training Plan and by providing war materiel and foodstuffs.[22] This approach achieved a balance between Canada's perception of its international moral obligations and its recurring domestic politics. As a consequence, at the end of the war, Canada was not a part of the high-level negotiations and was relegated to 'middle-power' status; a turning point in solidifying Canada's future international role.

Canada had always believed in peaceful resolution of conflict through international committee. In this sense, the United Nations suited the Canadian ideals. Although not a member of the Security Council, Canada did secure the agreement that non-members would be represented at the Security Council when use of force was being contemplated, thus allowing Canada to assert its views against the use of military means to resolve disputes. This backbench approach to international diplomacy was reflected in Canada's early involvement with the U.N., as well. Canada was demonstrative in the creation of the International Monetary Fund and the International Bank for Reconstruction and Development. Canada also played a constructive part in the creation of the International Civil Aviation Organization.

Its middle power status combined with its growing reputation as an international mediator had an infectious influence on Canadians who began to realize the need to affect international peace and security in order to ensure prosperity at home.

As such, Canada sought a niche to be able to assert itself. Peacekeeping became that niche in November 1956 when the U.N. General Assembly approved the Canadian plan to create a United Nations force to intercede between Israel and Egypt over the Suez Canal. Canada from this time became synonymous with U.N. peacekeeping activities in the Congo, between Turkey and Greece, and to the end of the Cold War.[23] This was the role that the Canadian people preferred and that guided policy decision-making into the future. The first real tests were the Korean War and the Cuban Missile Crisis.

During the lead-up to the Korean War, Canada was opposed to the U.S. involvement fearing an escalation of tension between Russia, China, and the rest of the world. As a result, Canada would not commit its forces,

initially, in support of the U.S. intervention. Similarly, during the Cuban Missile crisis in the early 1960s, when the superpowers edged toward nuclear war, Canada initially reneged on its NORAD commitment by not bringing its forces to full alert as the Americans had directed. Instead, Canada appealed to the U.N. for an independent verification of U.S. allegations of the missile sites in Cuba. In both cases, U.S. reaction was extremely critical of the Canadian Government's position on such profound issues, particularly in light of the close relationship between the two countries.[24] These types of incidents, over time, created cracks in the relationship that would be manifest in the way Canada tends to look at security issues differently than the U.S. This was specifically borne out in the dispute between the two nations over the Vietnam War.

Canada was faced with a dilemma that would once again pit its national interests against its closest relationship, the U.S. By this time, 81 percent of foreign investment in Canada was American.[25] Economically dependent on the U.S., tied by a plethora of bilateral agreements, and sharing similar ideals and interests as shown through partnership in NATO and the United Nations, the United States looked to Canada for support in Vietnam, at least in principle. However, the Canadian Government upheld its ideals of peace through negotiation and Prime Minister Pearson took a firm stance against U.S. intervention at a speech in Philadelphia. Not surprisingly, this infuriated the United States leadership. At a follow-on discussion at Camp David, President Johnson grabbed the Prime Minister by the lapel and berated him for his views. Anti-American sentiments quickly grew and were matched by anti-Canadian sentiments, as draft dodgers were welcomed to Canada in protest of the war.[26] A cooling-off period ensued. From the experience, the Canadian Government learned it had to walk a tightrope between its pursuit of middle power ideals and the realities of being dependent upon the United States for its economy and security.

Since the nation's early beginnings, the Canadian Government has continually sought to exercise its sovereignty through independent foreign policy. To do so, Canada portrayed itself as anti-conflict and anti-military, and chose to place emphasis on international trade and commerce to achieve peace and prosperity. Although this is somewhat an over simplification as attested by the patriotic support during the World Wars, Canada became labeled as such by a world whose main instrument of

policy was military power. Canada sought to seek independence by differing from the norm.

This was fostered by a philosophy of isolationism on the part of the Canadian people, in particular French-Canadians, by the government and its policies, and physically by Canada's geographic remoteness from the world and proximity to its benevolent and powerful neighbor. Canada distanced itself from the Empire by skillfully solidifying its relationship with the United States through lasting trade, commerce, and defense agreements, which nicely fit the Canadian ideal of harmony through economic prosperity. At the same time, it provided Canada with a blanket of U.S. protection.

Canada had unwittingly manipulated itself into another dependency that once again influenced its decision-making both domestically and internationally. Canada's emergence as a foremost peacekeeping nation is a stellar example. Not only did this role give Canada international recognition, it also provided the opportunity for greater foreign investment thus decreasing the dependency on the United States. It also had the advantage of promoting Canada's altruistic belief in security through universal economic cooperation beyond the Canada/U.S. border.

At home, peacekeeping was a suitable compromise to Canada's non-warlike tendencies and its commitments to international, collective peace and security. Most importantly, peacekeeping gave Canada a visibly different role because, by this time, Canada had become indistinguishable from the United States. Both English-Canadians and French-Canadians came to recognize the advantages of using international institutions to protect their values and ideals as Canadians, distinct from the Americans, as a form of sovereignty. Finally, peacekeeping was more befitting the modest size and relative capability of Canada's military. Overall, Canada could believe it was more independent from the influence of the United States, a perception that it tries to portray, to this day, in its decision-making on security matters.

What can be concluded from this historical analysis? First, the evidence is irrefutable that Canada's quest for its national identity as an autonomous and self-determining nation has been a singular preoccupation throughout its history. As a result, sovereignty has literally become a paranoia of the government's, especially on issues pertaining to the United States whom Canada is so economically dependent. Another prevalent

fact is that Canada does not consider its military as a key instrument of its national security. From this perspective, it becomes clearer how the offer from Secretary Rumsfeld to participate in NORTHCOM posed a dilemma for the Canadian Government. It was faced with devising security initiatives that would demonstrate to the United States its resolve against terrorism and, at the same time, safeguard its sovereignty.

Canadian Security Initiatives

> *"The government and people of Canada consider the attacks on New York and Washington to have been an attack on North America."*[27]

> *"The United States and Canada will work together to combat the menace of terrorism, and to protect the security of our citizens. We talked about the need for doing what will work in the long term, not merely what might make us feel good in the short term."*[28]

Security Problems

The extensive security initiatives undertaken by the Canadian Government since September 11th have largely been aimed at ensuring the continued free-flow of commerce, trade, and movement across the border so vital to its economy. The measures that have been implemented span the spectrum of federal agencies and are almost in lockstep with the U.S. initiatives.

Following the attacks, initial reports suggested that the terrorists had entered the United States through Canada. It has been a longstanding argument that the Canadian borders and approaches are too porous and that its immigration laws are too permissive. This became an immediate focus of attention in Canada as it quickly became apparent that there were a number of serious deficiencies.[29] Along the 5,526 mile border between the two countries, a large percentage of Canada's customs agents are university students hired on a temporary basis. At the border crossings themselves, there was little in the way of state-of-the-art technology to inspect containers and baggage entering the United States. As a result,

only one-third of the vehicles were ever properly screened. Likewise, there was no integration between Customs and Royal Canadian Mounted Police computer systems that would allow identification of potential suspects trying to enter the United States, nor was there any link to the U.S. Customs computer system.

At the airports, although adequate security measures were in place to screen passengers and baggage, the concern focused on the employees. Background checks on personnel and the control of ramp passes were not standard in all airports. However, the most glaring deficiencies existed at the seaports on the east and west coasts where upwards of 60 percent of the goods being off-loaded are destined for the United States. Because of budget constraints, the port authority had cancelled the contract for policing the docks, and instead, placed the responsibility upon the customs and security agents who were unqualified and ill prepared to do the job. As a result, there was no way of controlling the crime, smuggling, and gang activity that has become commonplace at portside. Concern was also expressed over the legitimacy of the numerous dockyard companies as it was suspected that many were havens for criminal activity.

At the federal level, the deficiencies were also prominent. Both the Royal Canadian Mounted Police and the Canadian Security Intelligence Service, similar to the Central Intelligence Agency, lacked the resources to conduct both domestic and international policing because of reductions in budget and resources. It was apparent that border, port, immigration, policing, and intelligence would need to be addressed urgently and that the efforts should be coordinated in conjunction with the U.S. initiatives to enhance its own internal security.[30]

Security Initiatives

It was recognized that increased security came at the expense of freedom of action and efficiency. With Canada's reliance on the United States as its largest trading partner, it could ill-afford overly stringent measures that could significantly hamper the $1.9 billion free-flow of trade between the two countries every day.[31] Unrestricted movement of people and goods is critical to the economic prosperity of both countries, in particular Canada. Accordingly, a practical compromise between the existing deficiencies and complete militarization of the air, land, and sea approaches had to be found.

The changes that were implemented within a relatively short time were far reaching. On December 12, 2001, Deputy Minister of Foreign Affairs, John Manley, and U.S. Homeland Security Director, Tom Ridge, signed the Canada-U.S. Smart Border Declaration. The features include: integrating personnel security systems to be able to share information on suspects crossing the border; coordinating information and efforts pertaining to refugees, the issuance of visas, and the sharing of crew and passenger manifests; development of a Canada/U.S. system to permit free-flow of no-risk personnel by creating 14 integrated border enforcement teams; collaboratively developing and implementing state-of-the-art technology for screening and inspection of cargo; sharing between the respective law enforcement and intelligence agencies information through common technology and working more closely together in the identification and apprehension of criminals/terrorists; and establishing joint teams of customs agents stationed at the major Canadian and U.S. ports to enhance inspection and security.

At airports, the Air Transport Security Authority authorized plain-clothed police officers to patrol airports and to fly on Canadian domestic flights.[32]

With respect to anti-terrorism and immigration, the Canadian Government implemented the Anti-Terrorism Act on December 24, 2001, and the Immigration and Refugee Protection Act on June 28, 2002. The intent of the Anti-Terrorism Act is to prevent terrorists entering Canada, to establish greater latitude for the federal courts to prosecute, to convict, and punish terrorists rather than deporting them to their native countries, and to work more closely with U.S. counterparts in the isolation of terrorists and terrorists groups. The changes to the immigration laws and the anti-terrorism act deny potential terrorists refugee status and impose significant penalties for those involved in procuring, selling, or falsifying documents.[33]

In response to the deficiencies in the policing and intelligence agencies, additional resources were given to the Royal Canadian Mounted Police and the Canadian Security Intelligence Service to train, equip and deploy personnel domestically and internationally in anti-terrorist operations. A greater focus was placed on inter-service cooperation between the two agencies and their counterpart agencies in the United States. Personnel were also hired to provide additional port security and coastal surveillance.[34]

In total since the terrorist attacks, the Government of Canada has allocated $7.7 billion to enhancing security. This represents 1 percent of its gross domestic product and is significant in its monetary value and in its symbolic value.[35] Monetarily, the size of the contribution reflects the government's commitment to security, and it is recognition of the degree to which internal security within the nation had been allowed to lapse. Symbolically, it renewed Canada's commitment to the United States by coming to the aid of its neighbor, friend, and ally in a time of crisis. The dispatches between the President and the Prime Minister that started on September 24, 2001, up to the most recent on September 9, 2002, were reminiscent of the Franklin Delano Roosevelt and William Lyon Mackenzie King era when the cooperation between the two countries was at its highest. The common cause then was Germany and World War II.[36] Today, the cause is terrorism, and in the words of the Prime Minister, "our relationship has never been stronger."[37]

Nevertheless, conspicuous by its absence is any semblance of relative military contribution to the overall security initiatives. Other than increasing the NORAD alert posture and assigning an additional $200 million annually to disaster response and nuclear, biological, and chemical threats, the military contribution is disproportionate to the government's focus on other areas and symbolically disproportionate to the U.S. military initiative to create a Command exclusively dedicated to homeland defense.[38] It is almost perplexing, in light of the tradition of cooperation in defending the continent alongside the U.S., that the Canadian Government is not asserting its military in a more demonstrative role beyond the existing arrangements. Add to this the unofficial acknowledgement that Canada benefits more from its defense relationships with the U.S. than it contributes. For instance, Canada is an equal partner in NORAD although it contributes only 10 percent of the equipment, personnel, and resources.[39] In this sense, Canada has an obligation to reciprocate in some fashion out of deference to the United States.

This sense of obligation stems from the first public pronouncement of any U.S. President regarding Canadian security. President Franklin Roosevelt stated in August 1938: "that the people of the United States will not stand idly by if domination of Canadian soil is threatened..." Prime Minister Mackenzie King reciprocated by stating: "that hostile powers would not be allowed to base operations against the United

States from Canada."[40] The impetus of the threat of German invasion at that time is not unlike the threat of terrorism today.

Likewise, the outward expression of support to the United States that led to the creation of the Permanent Joint Board on Defence then is not unlike the outpouring of support following September 11th. Families housed over 23,000 people stranded on 330 flights that had been diverted to Canada from the U.S. On September 14, 2001, the Prime Minister declared a national day of mourning when 100,000 people came out to the memorial ceremony held in the nation's capitol. Subsequently, over 10,000 Canadians traveled to New York to lend their support.[41]

It should not come as a surprise, considering the historical pattern of behavior that has characterized Canadian decision-making on security matters affecting its sovereignty, that Canada's reaction to a military contribution was relatively benign. The official response to Secretary Rumsfeld's offer was very succinct and deliberately released the same day as the Pentagon's announcement of the planned creation of NORTHCOM:

> While the creation of a 'Northern Command' may have potential implications for existing continental security arrangements, it is too early to speculate on what those might be…At this stage, discussions do not include the possible creation of a new joint command with standing forces attributed to it.[42]

As previously alluded, the decision also reflects in part the short notice between when the offer was made and the stand-up of NORTHCOM. Accordingly, although the statement precludes military forces, it implies the possibility of a future military contribution once "implications for existing continental security arrangements" have been fully assessed. What are the implications and how do they affect Canadian sovereignty and military participation in NORTHCOM?

North American Aerospace Defense Command (NORAD)

The implications of NORTHCOM are predicated on the history of the NORAD relationship and the manifestations of Anti-Ballistic Missiles (ABM).

The NORAD agreement is the centerpiece of the United States/Canada continental security arrangements. However, its implications permeate beyond just the military relationship. Signed in 1958 as a consequence of World War II and concerns over continental security, the NORAD agreement was formulated by the Military Cooperation Committee under the aegis of the Permanent Joint Board on Defence.[43] The agreement culminated a decade of partnerships and agreements that saw equipment, personnel, technology, and territorial sharing between the two countries in order to secure one another's defense. The defense industry, trade, and economic benefits that resulted from the collaboration were equally beneficial to both countries in both the long and short term.

Nevertheless, the agreement was not met with euphoria throughout Canada. Characteristic of its aversion to superpower dominance, those who were sovereignty conscious were skeptical that the agreement was yet another step in solidifying the 51st state. Indeed, the permanent presence of American strategic and tactical aircraft on Canadian soil; the installation of radar sites throughout Canada manned by U.S. military personnel; the construction of various facilities in Canada funded by U.S. security interests; and finally, the approval of over flight by bombers laden with nuclear weapons, gave the appearance of significant U.S. presence that constituted, in the minds of many, an invasion of Canadian sovereignty. These concerns were somewhat mitigated early on by the way Canada depicted the NORAD agreement on the international stage.

Concerned that the agreement could be viewed overseas as an inward-looking mechanism to isolate North America from European allies, Canada was careful to assuage any such concerns by promoting the agreement as a reflection of its commitment to collective security, similar to NATO. This rumination allowed Canada to remain true to its foreign policy ideals while convincing itself that it was not completely abrogating control to the United States. Nevertheless, despite the elaborate rationale, skepticism towards NORAD would resurface every 5 years upon the anniversary of its renewal. [44]

The agreement is complex. It melds both the President and the Prime Minister into a unified command and control arrangement and ostensibly gives each equal authority over decision-making within their respective countries. For instance, the Prime Minister can decide not to

prosecute a target in Canada although the U.S. feels it poses a threat to them; recall the Cuban Missile Crisis. The Commander of NORAD reports to both in the daily execution of air defense over Canada and the United States. His second in command, responsible for daily operations, is a Canadian who exercises direct control over the three NORAD regions: Alaska, Canada, and Continental U.S. In the Canadian region, the Canadian Commander has a U.S. deputy who is second in command and oversees all NORAD activities in Canada.

Today, Canada contributes approximately 268 people, working in the United States at NORAD facilities. In terms of Canadian equipment, NORAD has at its disposal: a network of radars; 4 squadrons of CF-18s; access to Canadian satellite resources; and access to command and control facilities. Over the years, the relationship has grown so close that the two sides are indistinguishable except for the color of uniform.[45]

In its initial stages, the threat to North America constituted the manned bomber capable of carrying both conventional and nuclear weapons. The NORAD role was to detect incoming aircraft using a series of land-based radars, and intercept and destroy them using United States and Canadian aircraft stationed throughout North America.[46] Canada was a willing partner in this role, which was very much related to potential breach of its own sovereignty, and it contributed the bulk of the fighter aircraft to intercept the Soviet bomber sorties that would routinely fly over the pole into Canadian air space to test NORAD's rapid reaction capability. In a sense, Canadian territory became the early warning of impending Soviet attack on the United States.

The advent of the ICBM shifted the emphasis away from the manned bomber and air defense to the early detection and warning from space of potential nuclear attack. U.S. funding, equipment, and infrastructure were realigned to meet the new priority and the focus became satellites instead of aircraft. Canada's participation dwindled. Its inability to afford the cost of the technology was a contributing factor, but more importantly, its foreign policy stance on non-proliferation was the most serious impediment to participation in this aspect of NORAD.

Ballistic missile defense further challenged the Canadian Government's advocacy of arms control and put Canada squarely in the middle of its bilateral obligation and its broader foreign policy objectives. Characteristically, the latter was upheld during the 1968 NORAD renewal

when Canada renounced participation in any aspect of ballistic missile or ballistic missile defense systems, thereby resigning itself to the air defense role only.[47]

The next major evolution of the NORAD agreement was reflected in the 1981 renewal. Two factors influenced amendments that would reinvigorate Canada's involvement. The first was that deterrence had been firmly ensconced within U.S. and Soviet doctrine. One of the outcomes was a resurgence of air defense against the manned bomber in recognition that the cruise missile threat was as pervasive as the ballistic missile threat. This led to a redefinition of the roles to include: aerospace warning comprised of the detection, validation, and warning of attack from air or space; and aerospace control comprised of detection, identification, intercept, and destruction of targets within North America's sovereign air space.

The other major factor was the consummation of an Anti-Ballistic Missile (ABM) Treaty between the U.S. and the Soviet Union. The agreement all but eliminated the deployment of a national system except for mutually agreed nodes. Non-proliferation and deterrence became the mainstays once again. For Canada, this resolved the original conundrum. In the end, both outcomes were entrenched in the renewal and Canada agreed to remove its objection to ballistic missile defense and to accept the change to North American Aerospace Defense Command, from North American Air Defense Command, as the new name for NORAD.[48]

What followed was a complete modernization to bring the new NORAD into the 21st century. The United States replaced outdated radar sites with a series of long-range and mid-range radars positioned throughout Canada's north overlooking the northern approaches. Airborne Early Warning was integrated into the air defense net and all command and control facilities were upgraded to be fully interoperable between Canada and the United States. Forward operating bases and over-the-horizon radars were also constructed in the farthest reaches of Canada. In concert, the U.S. continued to pursue advances in missile and space technology, the most notable being the Strategic Defense Initiative. Canada was offered an opportunity under the pretext of NORAD to assist in the research and development of the program; however, this was too reminiscent of the 1968 debacle.[49] Accordingly, Canada refrained from participation by reasserting its objection to missile defense systems of any kind.

National Missile Defense

Canada's contribution to NORAD has not been consistent. In fact, it has waned twice over the implications of missile defense, and each time, the relevance of NORAD itself came into question. The ensuing debate always focused on two sides of the sovereignty debate: the proponents who argued that membership in NORAD enhanced Canadian sovereignty through membership in a larger, more encompassing umbrella of defense with shared responsibility and control; and the opponents who reiterated that membership undermined Canadian sovereignty because of U.S. controllership. The most recent debate preceded the May 2001 renewal and national missile defense, the "son of ABM," became the center of attention.

Upon the recommendation of the Permanent Joint Board on Defence, Canada initiated the renewal process a year in advance with the aim of having the new agreement in place before the 2001 Presidential Elections; otherwise, there could have been a gap while awaiting review by potentially a new administration. As it turned out, the premonitions were serendipitous as the Republicans replaced the Democrats in the White House. However, there was also a downside to deliberating the renewal too early.

The Permanent Joint Board on Defence recommended to both governments that the agreement be renewed unchanged for another five years. As with all previous renewals, the Canadian Government wanted to examine the changes to the international security environment and to the trends of globalization that could have implications on the agreement. Accordingly, a Parliamentary Committee comprised of members from each of its official federal parties convened to interview witnesses from across the military, foreign affairs, and academia. At issue was the Clinton administration's renewed interest to deploy a robust national missile defense system to address the burgeoning ICBM threat from rogue nations. Extensive research, development, and testing had been underway leading up to the NORAD renewal. On the horizon, however, was the election that, depending on the outcome, could result in either deployment of national missile defense or a policy reversal in light of its enormous cost and implication to the ABM Treaty and proliferation. Regardless of the outcome, the implications of national missile defense to NORAD and

the new ICBM threat resurrected old arguments in Canada.[50] Among the military, foreign affairs, and academia, there were two distinct proponents: those in favor of participation in national missile defense and those seemingly against it.

National missile defense is a U.S.-sponsored program to deploy a fixed number of missile defense units to defend against a limited intercontinental ballistic missile threat. Whereas in the past, the United States relied on its nuclear arsenal as a deterrent against the Soviet Union, the end of the Cold War and the rise in nations with a nuclear capability gave impetus to be able to defend against a limited nuclear attack, either intentional or accidental. Deploying a national missile defense capability would give the United States another option other than launching a retaliatory nuclear strike. It was also rationalized that although rogue nations may not necessarily use their missiles directly against the U.S., the threat of using them could dissuade the U.S. from intervening in regional conflicts. A national missile defense capability would obviate this sort of brinkmanship.[51] Conceptually, national missile defense would rely on NORAD detection and tracking systems, integrated into a limited number of deployed missile sites dispersed in Alaska and the U.S., to shoot down incoming missiles. Phase one of the plan envisages a system capable of intercepting a small number of warheads using 100 interceptors that would take five years to deploy once a decision was made. Additional radars would have to be installed in Alaska, Great Britain, and Greenland as part of the first phase. Phase two would comprise additional interceptors and radars to provide redundancy, and would be operational five years hence.[52] Given the seemingly adamant pursuit of this plan, the Parliamentary Committee focused its deliberations to better understand the shift in U.S. policy towards national missile defense in an effort to assess the implications to NORAD and future Canadian participation.

The motivation behind developing what was then called a ballistic missile defense system emerged from the Soviet long-range missile threat in the 1950s and 1960s. Because of the potential imbalance to the nuclear deterrent theory posed by the new technology, both the U.S. and the Soviet Union pursued an agreement to limit the capability so as not to give either side an advantage. In 1972, both signed the ABM Treaty that limited either side from building a nationwide missile defense system. Instead, each country was permitted to erect a local system to project a

specific area of interest. The Soviet Union constructed a system to protect Moscow that is still functional today; whereas, the U.S. decommissioned its system that was constructed around its ICBM silos in 1976. The treaty thus ensured ongoing vulnerability thereby leaving the deterrence theory of nuclear weapons intact. The next milestone in missile defense came during the tenure of President Reagan when he proposed the Strategic Defense Initiative in 1983. Analogous to Star Wars, the system used spaced-based technology to defeat missiles. However, events such as the end of the Cold War, the technological challenges, and the cost of the system prevented it from going beyond the drawing board. It was not until the 1998 report to Congress by the Commission on the Ballistic Threat to the U.S., chaired by Donald Rumsfeld, that ballistic missile defense was rejuvenated. [53]

The report concluded the ballistic missile defense threat was no longer from Russia, but instead potentially from accidental firing or rogue nations possessing intercontinental missiles. Nations such as China, Iran, Iraq, India, Pakistan, North Korea had developed and tested ballistic missile capabilities. For instance, North Korea tested the Taepo Dong 1 missile in 1998 and is working on the Taepo Dong 2 having a greater range. The Missile Defense Act was subsequently passed in the U.S. in July 1999, a year before the NORAD renewal discussions that declared the U.S. would deploy a national missile defense system "as soon as technologically possible."[54] The pronouncements represented a direct violation of the ABM Treaty and signaled the U.S.'s intent to abrogate its commitment. The shock waves were still reverberating when the Parliamentary Committee began its deliberations.

Canada has chosen to use its middle power status to promote its belief in non-nuclear proliferation through the international forums of the U.N. and NATO. Canada has always promoted a robust, multilateral, non-proliferation arms control and disarmament regime. The Canadian representatives from the Department of Foreign Affairs and International Trade have been demonstrative at the U.N., taking the lead in ratification of the Combined Test Ban Treaty, the Nuclear Non-proliferation of Missile Technology Treaty, and the Outer Space Treaty. It was thought that if the United States unilaterally defied the ABM Treaty and deployed national missile defense, it could result in the proliferation of Russian nuclear weapons to overwhelm national missile defense's capabilities and

thus spark a new arms race. From the Department of Foreign Affairs and International Trade's perspective, Canada's association with national missile defense through NORAD would be hypocritical given Canada's foreign policy and long-standing activism against proliferation. It would also undermine the government's international credibility: on one hand promoting stability through collective institutional cooperation to rid the world of nuclear weapons; while on the other hand, endorsing a system that would give the U.S. and Canada dominance over the rest of the world. Those in the Department of Foreign Affairs and International Trade anticipated that a similar face-saving predicament would befall Russia. Russia has had to acquiesce to the unification of Germany, NATO expansion, ratification of the Strategic Arms Reduction Treaties, and to the Comprehensive Test Ban Treaty. It was felt that nullification of the ABM Treaty could compel Russia to change its demeanor to reassert its presence nationally and internationally as a matter of reputation. Those in the Department of Foreign Affairs and International Trade were also very much aware of the importance of Canada's bilateral agreements with the U.S. and cognizant of the adverse economic, political, and security implications of fundamental disagreement. Accordingly, those in the Department of Foreign Affairs and International Trade moderated their view towards national missile defense by accepting that missile defense would not necessarily have to be incompatible with arms control and disarmament if a compromise was found between Russia and the U.S.[55]

On the other hand, the proponents of national missile defense in Canada are less overt; instead, choosing to articulate the benefits of close military association with the United States as the primary reason for strengthening the NORAD agreement. Their rationale is based on the threat to North America. As expressed in the Rumsfeld Report, rogue nations possessing an ICBM capability with nuclear, chemical, and biological warheads, represents a threat to United States security, and by proxy, either an indirect or direct threat to Canadian security. As an indirect threat, although the missile may be targeted against the United States, there is a potential for technological error whereby Canada becomes the target. Directly, a missile may be targeted against Canada to dissuade the U.S. from getting involved elsewhere, without having to directly attack the United States.

In terms of weapons of mass destruction, a detonation close to the border region could have equally devastating effects on Canada as the U.S. Therefore, supporters of national missile defense argue that the capability to defend against a threat from the air through offensive means has always been a hallmark of Canada's contribution to NORAD. During the era of the Soviet manned-bomber, Canadian Forces aircraft were the means to defeat the threat. This role persists today to a lesser extent due to the introduction of the ICBM.

The advent of technology has necessitated a shift in the means but not the requirement to defeat a threat. It is argued that national missile defense is the latest means and represents a logical manifestation of the fighter role and NORAD missions. Therefore, Canada should not contest the use of existing NORAD architecture to support the national missile defense mission nor should Canada exclude itself, as it has in the past, if national missile defense were to be integrated within NORAD. However, Canada's contribution should extend beyond the rhetoric of political backing and into the realm of actual participation in national missile defense for fear the current NORAD roles, and, therefore, Canada's contribution, become obsolete.

The historical precedence has already been established. Canada owned and operated long-range, high altitude, nuclear tipped BOMARC missiles to intercept Soviet bombers between 1960 and 1970.[56] This was at a time when Canada provided a more balanced contribution to the bilateral agreement. Back when the manned-bomber threat and later the missile threat were predominant, Canadian involvement and especially the territory upon which the early warning radars were based (Distant Early Warning Line, Mid-Canada and Pine Tree Lines) were essential to the early detection of a threat to the U.S. In this sense, Canada's physical contribution to the United States was invaluable. This is less the case today as technology moves the threat to the higher ground. Undoubtedly, Canada's intellectual contribution, demonstrated by the outstanding men and women in uniform who participate in the day-to-day operations, is immeasurable by any standard. Although it is significant in itself to the relationship, it can in no way offset the financial disparity that exists between the United States and Canada especially if the relevance of Canada's contribution is outmoded by technology.

There is also the self-conscious dilemma of continually being on the receiving end with little to show in return. Specifically, as a consequence of the NORAD relationship, Canada gains access to U.S. technology, information, equipment, and resources that are at the leading edge of the revolution in military affairs. The prominence that this affords Canada allows it to be more influential at the international level and to participate in peace and security discussions that have broader implications to its trade and commerce worldwide. The argument is that Canada accrues many first, second, and third order benefits through membership in NORAD and needs to ensure its contribution remains balanced, as is practical as possible, and relevant.

However, it is a known fact that the United States plans to deploy national missile defense regardless of Canadian participation. The current plans do not require use of Canadian territory, Canadian owned infrastructure, or equipment. The United States could adopt a go-it-alone attitude, especially if it becomes disillusioned with the one-sided approach to the agreement.[57]

The Parliamentary Committee was faced with these two opposing views. Not surprisingly, the debate was reduced to the implications on Canadian sovereignty should Canada decide to participate in national missile defense or to end its commitment to NORAD because it refused to participate in any form of national missile defense and was no longer providing a relevant contribution. The Department of Foreign Affairs and International Trade questioned whether NORAD was the best way of protecting Canadian sovereignty while the Department of National Defence reinforced that no other viable alternative would afford Canada the same protection or benefits.

As in the past, a stalemate resulted and an indecision regarding national missile defense became a decision to maintain the status quo and to renew the agreement as the Permanent Joint Board on Defence had originally recommended.[58] For all intents and purposes, this was a practical decision. National missile defense is still in its nascent stage; any timeline for deployment is notional. Also, the U.S. has not committed to integrating national missile defense within NORAD nor have they approached Canada to participate. Even if Canada was approached, it remains theoretically possible to isolate Canadian participation from the

detection, warning, and prosecution processes should this be the case and still remain a partner in NORAD.

In its totality, the Parliamentary Committee assessed that Canada would supposedly have sufficient time to observe the developments and decisions surrounding national missile defense before the next anniversary in 2006 and to reassess the strategic environment and the implications to the agreement. Canada approved the renewal in June 2000.[59] However, September 11th and the changing security environment suddenly resurrected these exact same arguments but this time in terms of the implications of NORTHCOM.

Obstacles and Attitudes to NORTHCOM

Three prevalent characteristics underscore Canadian decision-making about the implications of NORAD and national missile defense issues that are relevant to participation in NORTHCOM: sovereignty, process, and time.

Sovereignty is the largest impediment preventing Canada from participating in NORTHCOM. The debate dates back to the founding of Canada under the guise of the Royal Empire. Since that time, successive Canadian Governments have risen and fallen from power based on the public's perception of whether the country was too close or too distant from its benefactor. As described, this overarching theme influenced Canada's contribution in war, the formulation of its foreign policy, and ultimately how the nation defined its identity, both domestically, in terms of its culture and linguistic differences, and internationally, in terms of its part in contributing to global peace and security. These forces have shaped the Canadian psyche and dominate the debate of participation in NORTHCOM and whether Canadian sovereignty is more threatened by terrorists or by closer association with the United States.

The idealists argue predominantly on the political aspects of closer association with the United States. There is general agreement that the Canadian economy is dependent upon the U.S. economy and therefore, Canada should do its utmost to foster this aspect of the relationship. Witness the extensive efforts by the Canadian Government to instill confidence in the U.S. administration through its broad-reaching measures to secure its land and sea borders following September 11th.

It is also generally agreed that the plethora of other bilateral arrangements between the two countries, such as cultural, academic, research and development, and defense help foster the economic relationship. The idealists, however, draw a line on the relative importance of the military bilateral relationships with the U.S. relative to the overall economic relationship, arguing that the strength of the economic relationship pervades the military relationship, and not the other way around.

Idealists also contend that, although NORAD is a significant symbol of the close cooperation between Canada and the U.S., changes to the agreement, whether in favor or otherwise, historically have not adversely affected the economic relationship. The Cuban missile crisis and the inclusion of ABM exceptions within past NORAD negotiations, for example, did not denigrate economic cooperation. The economic relationship has surpassed the defense relationship to the point that the two are independent of one another.

The idealists are applying this same rationale to the argument surrounding Canada's participation in NORTHCOM. This does not imply that idealists have an irreverent view of the defense relationships with the U.S. and that NORAD and/or NORTHCOM would not serve Canadian interests. Instead, the idealists take a pragmatic approach by opting for the status quo, as has been the tendency within the NORAD agreement. In this way, Canada achieves the best of both worlds, while minimizing the implications to its sovereignty. The Prime Minister reaffirmed the stronghold of idealist thinking within in the Canadian Government when he referred to the Canada/U.S. relationship as:

> ...[A] relationship based on shared values of freedom and human dignity. A model to the world of civility and respect. And, in the context of globalization, a guide to how nations can develop strong friendships while retaining distinct identities.[60]

The fallacy of the idealist argument, however, is manifest in how they define sovereignty. Canadians have a tendency to portray themselves in contrast to Americans. This tendency originated from the historic perception that the United States leaders once wanted to absorb Canada into the Union. Over time, the annexation of Alaska, the interference with

Newfoundland joining the Canadian confederation, and the extensive development of U.S. installations on Canadian territory helped perpetuate paranoia in Canada.

As a result, Canadians began to portray themselves as not American. This attitude is prevalent today as the government tries to restrict the amount of American culture and advertising on Canadian television and in Canadian magazines for fear of Americanization. It is also the foundation for the idealist's contention that closer military association with the U.S. would further undermine Canadian sovereignty. Essentially, by placing Canadian land, sea, and air forces under a command relationship within NORTHCOM, some argue that Canada would relinquish control of its sovereignty to the United States, which would have untold consequences to its identity, independence, and self-determination.

The logic of the argument breaks down when you consider that the United States has no interest in absorbing Canada or any other nation, nor does it have any ambition towards controlling Canadian sovereignty. The fact that the United States has been sensitive to Canada's preoccupation with its sovereignty is reflected by its acquiescence towards an equal partnership in NORAD, despite the growing lopsidedness of Canada's contribution.[61] If the idealist contention were true, Canadian participation in NORAD would be proportional to its contribution.

Realists, on the other hand, argue that the two countries are more alike than not and that the creation of defense agreements has spawned cooperation and collaboration in a wide range of activities between the two countries. Strong fundamental agreements that bind the security of the two countries are the basis for lasting economic relationships. Likewise, Canada has used its defense relationship with the United States to promote its prominence in other international forums where military strength is recognized as a symbol of power and influence. Being closely aligned with the United States allows Canada an equal presence and representation of Canadian ideals and values. At the same time, other nations recognize this special relationship and will consult with Canada on matters relevant to the United States.

The NORAD agreement is the symbol to others of the close relationship between the two countries. The realist approach is to actively promote greater association with the United States to strengthen Canada's ability to control and maintain its sovereignty. Abstaining from

participation in NORTHCOM is tantamount to relinquishing control of Canadian sovereignty, in the realist opinion. National missile defense is held in the same regard and, therefore, participation in both national missile defense and NORTHCOM is essential. The concern for the realist is whether the United States will continue to indulge the perennial obfuscation surrounding Canada's commitment to collective defense of the continent or will the United States grow tired and simply forge ahead alone?[62] Recall in 1968 when Canada opted out of ABM defense because of its unwillingness to participate in any aspect of missile or space activity beyond that of warning and surveillance. The United States subsequently modified the Unified Command Plan and assigned ABM to the newly formed U.S. Space Command, relegating Canada to a position of spectator.[63] In fact, the decision has been made to assign national missile defense to U.S. Strategic Command. What are the implications on Canadian sovereignty from the realist perspective? Without a link through a potential NORAD/NORTHCOM accord, Canada will not be a part of a NORAD-like unified command and control arrangement that would provide some authority in the decision-making process. Until Canada works out the idealist and realist views, the sovereignty debate will continue to preclude Canada's future participation in substantive defense matters with the United States.

There are indications that Canada is undertaking a process to address sovereignty and the implications of its relationship with the U.S. There are five key indicators: the ABM Treaty; the recently commissioned study on the Canada-U.S. relationship; the results of the study on Canadian Security and Military Preparedness; the completion of the Defense Review initiated on September 1, 2002; and the potential federal election in 2004, all of which have an element of predictability as to their influence on the decision to participate in NORTHCOM.

Recall that one of the factors influencing participation in NORTHCOM is a decision by the United States on the ABM Treaty. The Department of Foreign Affairs and International Trade indicated that should Russia and the U.S. reach an accommodation on the ABM Treaty, that would avoid the possibility of nuclear proliferation, Canada would be more amenable to national missile defense. When President Bush announced his intention to withdraw from the Treaty in December 2001, President Putin reacted nonchalantly in light of the unilateral U.S.

announcement of commensurate reductions to its strategic nuclear arsenal.[64] As a result, the Department of Foreign Affairs and International Trade will likely relax its objection towards national missile defense and be more amenable to considering Canadian participation in both national missile defense and NORTHCOM.[65]

In January 2002, the government commissioned a parliamentary study to examine the future of Canada-U.S. relations. The purpose of the bi-partisan commission is to address a watershed of issues ranging from adopting the U.S. dollar as a common currency to greater economic integration, even beyond the bounds of the North American Free Trade Agreement. Headed by the Department of Foreign Affairs and International Trade, the mandate will be to create an institutional framework of the relationship to move beyond many informal liaisons that currently exist to more formalized agreements. One of the implied intents of the study is to show that Canadian sovereignty is not a function of the relationship with the United States, but instead, is defined by Canada's distinctiveness as a country. Therefore, the commission should conclude that, despite some paranoiac fears within Canada, the U.S. has no more intention of absorbing Canada than Canada has becoming the 51st state and, as a result, closer bilateral relations with the U.S. do not pose a threat to its sovereignty.[66]

The other two noteworthy indicators are the Canadian Security and Military Preparedness study and the Defense Review. The Canadian Security and Military Preparedness study was completed in February 2002 and was, in part, the catalyst for Defense Review launched on September 1, 2002. The Defense Review is to update the White Paper on Defense, last written in 1984, to reflect the changing security environment, prioritize the mission and roles of the Canadian Forces and realign resources, equipment, personnel, and budget to achieve the government's military objectives.[67]

The Canadian Security and Military Preparedness Report reaffirms the current trends of equipment obsolescence, inadequate funding, under trained personnel, lack of resources, and over commitment.[68] The Defense Review should provide the government of Canada with options to address these deficiencies. The underlying problem, as with any military, is funding.

In the past, Canada has relied heavily upon its alliances for collective defense as a means to defray otherwise enormous defense expenditures. This approach will undoubtedly be reaffirmed by the two reviews, and it should point to the significant opportunities that can accrue through additional integration of Canada/U.S. forces within a framework like NORTHCOM that encompasses land, sea and air forces.[69]

Finally, the federal election predicated to occur some time in 2004 will also be an indicator. Whereas the outcomes of the other indicators can be predicted with some confidence, the position of the political leaders on Defense is far less certain. Canada's penchant towards its military has not been stellar and, therefore, it has not featured prominently on the campaign trails of the past. However, the newly elected leader of the current government, Mr. Paul Martin, has called for the need for closer cooperation with the United States and has placed a spotlight on Canada's military by announcing a majority capital equipment purchase of helicopters. There is also general agreement amongst the political parties that the condition of Canada's military desperately requires attention. The pronouncements in the last six months by the U.S. ambassador to Canada have been instrumental in drawing the attention of all parties to the situation.[70] As a result, although not likely to be a campaign issue, the elected government will be faced with the same situation after the election as before and should continue with the same courses of action laid down by the government prior to the election.

By combining the predicted results of these five key indicators, it appears intuitive that Canada will eventually assign forces to NORTHCOM. It is regrettable that the process precludes an earlier decision. It seems that the military has in fact drawn this conclusion and has convinced the government to at least take some initial steps. Canada has surreptitiously indicated it will establish a cell in NORTHCOM Headquarters to observe, plan, and support coordination of United States and Canadian land and sea operations on a case-by-case basis.[71] Strategically, this is perhaps the best course of action in light of the government's anti-military predilection. At the same time, this approach provides a signal to the U.S. of Canada's interest and desire to remain actively engaged. Hopefully the U.S. will recognize the circumstances and continue to extend its benevolence and understanding towards the collective defense of the two nations while Canada takes the time to

complete its detailed review of the Canada/U.S. relationship over the next year or so. However, indications are otherwise; there are telltale signs that U.S. policy is changing and is becoming less benevolent.

NORTHCOM - U.S. Attitude

It is being purported that the U.S. attitude towards its bilateral and multilateral relationships is becoming more and more unilateral. In actual fact, the U.S. policy towards international relations is undergoing a noticeable change of direction and countries, such as Canada, need to take notice.[72]

At the multilateral level, the U.S. appears to becoming more obstreperous towards issues that are not within its national interests. For instance, the U.S. has not ratified the 1997 Land Mine Treaty to ban anti-personnel land mines, nor the creation of the International Criminal Court in 1998 to investigate and prosecute those who commit war crimes. This has created the impression that the U.S. is disengaging itself from international agreements.

In actual fact, the U.S. abstentions are for such valid concerns as the need to use landmines for force protection along the border between North and South Korea.[73] Likewise, the trepidation over the International Criminal Court is a reflection of the U.S. concern for its military members who are engaged in almost every international conflict and who, by the sheer consequence of U.S. military preponderance, may become the victims of their own benevolence.[74] At the bilateral level, the United States has renounced its participation in the ABM Treaty with Russia. Although the announcement did not instigate a negative reaction from the Russian President, as many onlookers predicted, it is being interpreted as a further indictment of a unilateralist approach, despite the pervasive threat of nuclear weapons from rogue nations described earlier.[75] This portrayal falls on the heels of U.S. pronouncements on the war on terrorism, the war in Afghanistan, the axis of evil, and the most poignant of all, the action in Iraq, all in the aftermath of September 11th.

Accordingly, the portrayal of a change in U.S. policy is accurate but is legitimized by the changing face of the security environment in which the U.S. finds itself; all the more reason for nations to take stock.

The most revealing evidence of the change is in the U.S. National Security Strategy that unabashedly enunciates the new U.S. unilateral approach:

> We will disrupt and destroy terrorist organizations by identifying and destroying the threat before it reaches our borders. While the United States will constantly strive to enlist the support of the international community, we will not hesitate to act alone, if necessary, to exercise our right of self-defense by acting preemptively...[76]

For Canada, the implications of the changing U.S. attitude must be assessed in the context of its bilateral relationship and its presumption that the United States will continue to remain ambivalent to the procrastination that has typified Canada's decision-making. The premonitions show that the U.S. will act unilaterally in face of a threat to its national interests and this could pose a greater challenge to Canadian sovereignty than participating in the security of North America as an active member of NORTHCOM.

Conclusions

The examination of the Canada/U.S. relationship and its historic underpinnings, and the description of the security initiatives undertaken by Canada following September 11th provide a perspective on how Canada ranks its sovereignty in relation to its security.

What then can be concluded about Canada's decision not to participate in NORTHCOM? To Canada, the heart of the debate of whether or not to assign land, sea, and air forces to NORTHCOM is not about United States control of Canadian Forces. NORAD is a perfect example of the effectiveness of combined forces under a unified command and control structure where Canadian Forces aircraft are commanded under the auspices of the U.S. combatant commander. Nor is the debate about the use of Canadian equipment, resources, and personnel by the U.S. Again, the precedence is replete throughout history where Canada and the United States have collaborated in such areas and Canada in particular has reaped the benefits.

The heart of the debate lies at the political level, within government, and the innate perception that contributing additional forces under the command of the United States will further erode Canada's sovereignty as opposed to enhancing it through collective security. Canada sees this as a greater threat than the threat of terrorism itself. The roots of the paranoia of becoming Americanized are historic, and, in large part, are self-aggrandized to the point of preoccupation when issues of defense cooperation are tabled. The debate of pros and cons often results in indecision that becomes a decision for the status quo.

This was the outcome within the limited time Canada had to consider the offer by Secretary Rumsfeld to participate in NORTHCOM. Instead, Canada opted to enhance its economic security by investing heavily in all other forms of border, port, and airport security to protect the flow of trade critical to the Canadian economy. The efforts were aimed at pacifying U.S. concerns about the permeability of Canada's defenses against terrorism, without having to commit military forces to NORTHCOM. It was presumed these initiatives, along with the historic defense agreements, would satisfy the United States. However, the existing defense agreements are no longer sufficient to protect U.S. interests, and there are growing signs that the U.S. is no longer prepared to be dependent on others for its security.

It appears the U.S. is reverting to a more unilateral approach in the pursuit of its national interests, especially involving terrorism. The latest National Security Strategy serves notice to countries like Canada that the United States is prepared to take preemptive measures without prior consultation. In other words, if the threat to the United States is imminent, then it will no longer regard Canadian sovereign interests in deference to its own, as Canada has historically presumed. In recognition of this fact, Canada has undertaken a broad range of initiatives to assess the future of Canada/U.S. relations with the goal of making improvements, including militarily.

Additionally, Canada has committed a small planning and coordination cell as an interface between the Canadian Forces and NORTHCOM while it undertakes the broader assessment of its relationship with the United States. Indeed, based on recent comments from the former Minister of National Defence, there are indications that Canada's mind-set towards sovereignty and security is changing:

> "Sovereignty means that we must be able to defend Canada and participate meaningfully in the defence of North America."[77]

Nevertheless, this may not be timely enough for the United States who is advancing Homeland Security and Homeland Defense at breakneck speed. Admittedly, Canadian sovereignty and security are enhanced through close association with the United States. If Canada wants to avoid being excluded from actively contributing to the defense of North America and, therefore, its own sovereignty, it needs to be in lock step with the United States by assigning forces in support of NORTHCOM.

Notes

1. Press Release, US NORTHCOM Public Affairs, 2 October 2002.

2. J.F. Schnabel, R.J. Watson, K.W. Condit, B. Fairchild, W.S. Poole, *The History of the Unified Command Plan 1946-1993* (Washington, D.C.: Historical Division, Joint Chiefs of Staff, 1995), 11-15.

3. U.S. Department of Defense Homeland Security, on-line, Internet, 30 September 2002, available from www.defenselink.mil/ specials/homeland.

4. Department of Defense, *The Joint Staff Officer's Guide JFSC Pub 1*, (Washington, D.C.: U.S. Government Printing Office, 2000), 1-28 - 1-45.

5. U.S. Department of Defense U.S. Northern Command, on-line, Internet, 30 September 2002, available from http://www.NORTHCOM.mil/index.cfm?fuseaction=s.whoweare&section=5.

6. General Eberhart, Commander NORAD and U.S. NORTHCOM, Staff briefing to Air War College (AWC) International Officers (IO), 10 September 2002.

7. U.S. Department of Defense U.S. Northern Command.

8. Government of Canada, *Canadian Security and Military Preparedness: Report of the Standing Senate Committee on National Security and Defence,* (Queen's Printer, Ottawa, Ontario, 2001) 66.

9. Eberhart, Staff briefing to AWC IOs.

10. Standing Senate Committee on National Defence and Veterans Affairs, *Canadian Security and Military Preparedness: Renewal of the NORAD Agreement*, Federal Government of Canada Proceedings Transcript, statement by LGen G. MacDonald, Deputy Commander in Chief NORAD, DND 23 March 2000.

11. Canada, Government of Canada - Statistics Canada available from http://canada.gc.ca/main_e.html.

12. D. Morton, *A Military History of Canada.* (McClelland & Stewart Inc, 1985), 239-247.

13. William Metcalfe, ed., *Understanding Canada - A Multidisciplinary Introduction to Canadian Studies* (New York University Press, New York, 1982), 492.

14. Ibid., 493.

15. Ibid., 116.

16. Ibid., 494.

17. Morton, 113.

18. Metcalfe, 117.

19. Ibid., 120 - 122.

20. Ibid., 124.

21. Morton, 176.

22. Ibid., 193 - 195.

23. Metcalfe, 498 - 502.

24. C.F. Doron, *Forgotten Partnership.* (The Johns Hopkins University Press, Baltimore, Maryland, 1984), 77 - 96.

25. Canada, Government of Canada - Statistics Canada.

26. L. Martin, *The Presidents and the Prime Ministers*. (Doubleday Canada Limited, Toronto, Ont., 1982), 1 - 15.

27. Government of Canada, *Canadian Security and Military Preparedness: Report of the Standing Senate Committee on National Security and Defence*, 63.

28. Jean Chrétien, Prime Minister of Canada, Parliament Hill, Ottawa, Canada,

September 24, 2001.

29. Government of Canada, *Canadian Security and Military Preparedness: Report of the Standing Senate Committee on National Security and Defence*, 135-143.

30. Ibid., 1-75.

31. Canada, Government of Canada - Statistics Canada.

32. The Smart Border Declaration, *Building a Smart Border for the 21st Century on the Foundation of a North American Zone of Confidence*, Ottawa, Canada, 12 December 2001.

33. Government of Canada, *Anti-Terrorism Act and the New Immigration and Refugee Protection Act (IRPA)*, Ottawa, Canada, 24 December 2001.

34. Government of Canada, *Canadian Security and Military Preparedness: Report of the Standing Senate Committee on National Security and Defence*, 135-143.

35. Government of Canada, *Budget 2001* Ottawa, December 10, 2001, 2001-118.

36. Martin, 115-146.

37. Jean Chrétien, Prime Minister, *On the occasion of the Canada-U.S. Border Summit*, Detroit, Michigan, 9 September 2002.

38. Government of Canada, Department of National Defence, *The Department of National Defence and Canadian Forces response to September 11, 2001, Operation Apollo – Canada's contribution to the campaign against terrorism* available at www.dnd.ca/menu/operations/apollo/index_e.htm.

39. D. Nicks, J. Bradley, C. Charland, *A History of the Air Defence of Canada, 1948-1997*, (Queen's Printer, Ottawa, Canada, 1997), 5-207.

40. Martin, 127.

41. Government of Canada, Department of National Defence, *The Department of National Defence and Canadian Forces response to September 11, 2001, Operation Apollo – Canada's contribution to the campaign against terrorism*.

42. Office of the Prime Minister of Canada, Ottawa, Canada,17 April 2002.

43. G. Lindsey, *Canada-U.S. Defense Relations in the Cold* War, ed J. J. Sokolsky, J.T. Jockel, *Fifty Years of Canada-United States Defense Cooperation The Road From Ogdensburg* (The Edwin Mellen Press, Lewiston, NY., 1992), 61.

44. Ibid., 61 - 67.

45. D. Nicks, J. Bradley, C. Charland, *A History of the Air Defence of Canada, 1948-1997*, (Queen's Printer, Ottawa, Canada, 1997), 5-207.

46. Lindsey, 60 - 65.

47. Ibid., 71.

48. D. Murray, *NORAD and U.S. Nuclear Operations* ed J. J. Sokolsky, J.T. Jockel, *Fifty Years of Canada-United States Defense Cooperation The Road From Ogdensburg* (The Edwin Mellen Press, Lewiston, NY., 1992), 209-235.

49. D. Cox, *Canada and Ballistic Missile Defense*, ed J. J. Sokolsky, J.T. Jockel, *Fifty Years of Canada-United States Defense Cooperation The Road From Ogdensburg* (The Edwin Mellen Press, Lewiston, NY., 1992), 240.

50. Standing Senate Committee on National Defence and Veterans Affairs, *Canadian Security and Military Preparedness: Renewal of the NORAD Agreement*, Federal Government of Canada Proceedings Transcript 23 March 2000.

51. Statement of The Under Secretary of Defense for Acquisition and Technology Honorable Paul G. Kaminski Before a Session of the House Committee on National Security Subcommittee on Military Research and Development and Subcommittee on Military Procurement on National Missile Defense, May 15, 1997.

52. Presentation by the Honorable John D. Holum Senior Adviser for Arms Control and International Security U.S. Department of State Conference on International Reactions to U.S. National and Theater Missile Defense Deployments Stanford University, March 3, 2000.

53. R. Handberg, *Ballistic Missile Defense and the Future of American Security*, (Praeger Publishers, Westport, CT, 2002), 1- 37.

54. Hearing before the Committee on Foreign Relations United States Senate 6 Oct 1998, *The Ballistic Missile Threat to the United States.* (U.S. Government Printing Office, Washington, D.C., 1998).

55. Standing Senate Committee on National Defence and Veterans Affairs, *Canadian Security and Military Preparedness: Renewal of the NORAD Agreement*, Federal Government of Canada Proceedings Transcript, statement by Mr. P. Heinbecker, Assistant Deputy Minister, Global and Security Policy, 23 March 2000.

56. Cox, 244.

57. Standing Senate Committee on National Defence and Veterans Affairs, *Canadian Security and Military Preparedness: Renewal of the NORAD Agreement*, Federal Government of Canada Proceedings Transcript, statement by Mr. D. Bon, Acting Assistant Deputy Minister, Policy, DND, 23 March 2000.

58. Ibid.

59. Ibid.

60. J. Chrétien, Prime Minister of Canada, address on the occasion of the U.S./Canada Border Summit, September 2002.

61. J.J. Sokolsky, J.T. Jockel, *Fifty Years of Canada-United States Defense Cooperation The Road From Ogdensburg*, (The Edwin Mellen Press, Baltimore, Maryland, 1992), 3.

62. Cox, 259.

63. Murray, 229.

64. Statement by President of the United States, *U.S. Withdrawal from ABM Treaty*, The White House, Office of the Press Secretary, 13 June 2002.

65. Standing Senate Committee on National Defence and Veterans Affairs, *Canadian Security and Military Preparedness: Renewal of the NORAD Agreement*, Federal Government of Canada Proceedings Transcript testimony by Paul Heinbecker Assistant Deputy Minister, Global and Security Policy, Department of Foreign Affairs and International Trade, 23 March 2000.

66. Mr. L. Yves Fortier, Former Canadian Ambassador to the United Nations, *Canada and Sovereignty*, lecture, Osgoode Hall Law School, York University, Toronto, Ont, 23 January 2002.

67. Government of Canada, Department of National Defense, *The Defense Review*, September 2002.

68. Government of Canada, *Canadian Security and Military Preparedness: Report of the Standing Senate Committee on National Security and Defence*.

69. Government of Canada, Department of National Defense, *The Defense Review*, September 2002.

70. U.S. Ambassador to Canada, Paul Cellucci has been supportive in trying to emphasize the need to bolster the Canadian military and its contribution to NORAD and NATO.

71. The Honourable John McCallum Minister of National Defence, lecture to the Toronto Board of Trade, Toronto, Ontario, on-line, Internet, 25 October 2002, available from http://www.forces.gc.ca/eng/archive/speeches/2002/oct02 /BOT_s_e.htm.

72. J.S. Nye Jr, *The Paradox of American Power*, (University Press, Oxford, New York, 2002), 154.

73. Ibid., 156.

74. Ibid., 160.

75. C. Krauthammer, The Bush Doctrine - ABM, Kyoto, and the New American Unilateralism, *Early Bird*, 4 June 2001.

76. U.S. Government, The National Security Strategy of the United States of America, September 2002, Chp 3, 6.

77. The Honourable John McCallum Minister of National Defence, lecture to the Toronto Board of Trade, Toronto, Ontario, 25 October 2002 available at http://www.forces.gc.ca/eng/archive/speeches/2002/oct02 /BOT_s_e.htm.

Contributors

Lieutenant Colonel Phillip A. Bossert is Chief of Exercises and Training for NATO's only deployable Combined Air Operations Center, Ramstein Air Force Base, Germany. A 1982 graduate of the United States Air Force Academy, he is a command pilot with over 3900 hours in CT-39B, C-21A, C-141B, and UV-18B aircraft. A veteran of Operations JUST CAUSE, DESERT SHIELD, DESERT STORM, AND ENDURING FREEDOM, he holds master's degrees in economics, military art and science, strategic studies, and public administration. He is a graduate of the United States Army Command and General Staff College, Armed Forces Staff College, and Air War College. Throughout his career Lt Col Bossert has served as an assistant professor and Air Officer Commanding at the Air Force Academy, Chief of Strategic Plans at Headquarters Air Mobility Command, Chief of the Programs Division at United States Transportation Command, and commanded the 821st Air Mobility Squadron. A prolific writer, he has published over 75 articles and 1 book, and won the Global Mobility Writing Award at Air War College for a paper describing his experiences commanding Tanker Airlift Control Elements in Afghanistan.

Lieutenant Colonel James Chambers is Chief of the Security Forces Operations Division at Headquarters United States Air Forces in Europe (USAFE), Ramstein Air Base, Germany. He is responsible for providing policy and guidance for security, law enforcement, and integrated base defense operations for over 2,700 USAFE security forces personnel. Lt Col Chambers is a graduate of the U.S. Air Force's Air War College, and holds a M.S. and B.S. in Criminal Justice from the University of Southern Mississippi. He is also a graduate of the Federal Bureau of Investigations National Academy and has studied at the British Academy of Forensic Sciences at the University of London. He is the recipient of the 1985 Larry Wilson Award as the outstanding graduate student in Criminal Justice for the University of Southern Mississippi.

Dr. Roger Dean Golden is currently Chief of the Matrixed Contract Support Division, HQ Standard Systems Group, Acquisition Directorate, Maxwell AFB—Gunter Annex, AL. Dr. Golden has 24-years experience in

DOD contracting as a price analyst, contract specialist, and procurement analyst. After beginning his career at Warner Robins ALC, he served in positions at HQ AFLC, AF Standard Systems Center, and the Defense Commissary Agency before moving in 2001 to his current position. He was honored as Top Contract Price Cutter for the Air Force in 1985 while in AF Logistics Command, and again in 1988 while in AF Communications Command. In addition to numerous performance awards, Dr. Golden has received over $23,000 in cash awards for cost saving suggestions. He also received the General Charles A. Horner Award for his professional studies paper at Air War College. Dr. Golden received his B.S. degree, *cum laude*, in mathematics from Bob Jones University, his M.S.A. in management from Georgia College, and his D.P.A. degree in public administration from the University of Alabama. He received the Master of Strategic Studies from the Air War College in 2003. Dr. Golden's "Mission Support Pricing—Telling the Whole Story" was published in National Contract Management Journal in Summer, 1987. Dr. Golden is a member of the Board of Directors for Alabama Special Olympics. He resides in Prattville, Alabama with his wife Diane and son Adam. His son Alex is a freshman at the University of Alabama in Birmingham.

Lieutenant Colonel Ralph G. Hensley, Jr., is the Chief of Doctrine, Training, and Readiness in the Joint Chiefs of Staff, J-8 Directorate, Joint Requirements Office for Chemical, Biological, Radiological, and Nuclear matters. Lt Col Hensley's previous assignments include Installation and Major Command Disaster Preparedness Officer, USAF Civil Engineer Readiness School and Recruiting Squadron Commander, Interservice Nuclear Weapons School Instructor, and Associate Director of the USAF Counterproliferation Center. He received his B.S. in Biology from Virginia Wesleyan College and M.A. in Business Management from Webster University. Lt Col Hensley is also a graduate of Squadron Officer School, Air Command and Staff College and Air War College. He has authored North Atlantic Treaty Organization Standardization Agreements and Air Component Command, Major Command, and installation nuclear, biological, and chemical emergency response plans.

Lieutenant Colonel James M. Jenkins is the NORAD/NORTHCOM Desk Officer at the Joint Staff, Directorate of Command, Control,

Communications and Computer (C4) Systems, Current Operations Division, the Pentagon. He is responsible for staff actions related to C4 aspects of crisis, contingency, and emergency situations; operational direction of MILSATCOM systems, coordination with DOD and non-DOD agencies regarding MILSATCOM access, and coordination with Combatant Commander J-6 staffs regarding operational and programmatic issues. Lt Col Jenkins is a graduate of the U.S. Air Force's Air War College, and holds a M.A. in Management from Webster University, and a B.G.S. from the University of Nebraska. He won the 2003 Air War College Armed Forces and Communications Electronics Association (AFCEA) Research Award for his paper entitled "Computer Network Defense: DOD and the National Response."

Lieutenant Colonel Judith J. Mathewson serves as the Alaska Air National Guard State Plans Officer for the Headquarters, Alaska Air National Guard, Fort Richardson, Alaska. She ensures senior leadership is advised of technical procedures and organization of strategic plans for the two Wings, which include over 2100 members in a C-130H Airlift Squadron, KC-135 Air Refueling Wing, HC130 and HH60 Rescue Squadron, Combat Communications Squadron and numerous support organizations. She retired from the Anchorage School District after twenty-three years as a certificated educator and counselor while performing her duties as a traditional Guard member. Lieutenant Colonel Mathewson facilitated graduate level courses at the University of Alaska Anchorage as adjunct faculty for three years. She also served as Lead Trainer, platform instructor and small group facilitator at the Department of Defense Equal Opportunity Management Institute (DEOMI) for nine years. She developed the Tragedy Assistance Program for Survivors, Inc. Youth Program for children of deceased military members and organizes a seminar for these children each Memorial Day. She trains Honor Guards from all branches of the military and counselors to work with these bereaved children and their surviving parent. Colonel Mathewson was instrumental in writing a grant for the Troops to Teachers program in the State of Alaska. She designed curriculum and provided counseling services for the Alaska Youth Corps Challenge Program for at-risk teenagers. Over 1500 cadets have graduated from high school or received their GED as a result of this successful program. An advocate for continuing education, Lt Col Mathewson coordinated the Alaska National Guard Tuition Scholarship Program, resulting in free tuition from the University of Alaska multi-campus system

for all Air and Army National Guard and Naval Militia personnel. Lieutenant Colonel Mathewson graduated from Air War College in-residence in May 2003 at Maxwell AFB, Alabama. She is a Trained Crisis Responder, Critical Incident Stress Management Team Member and a regular volunteer for Family Programs.

Commander L. Edward Mayer currently serves as a Special Assistant to the Chief of Naval Operations (Speechwriter). He is a submarine officer who served on both LOS ANGELES and OHIO Class submarines: Executive Officer, USS JEFFERSON CITY (SSN-759), Navigator and Operations Officer, USS BOSTON (SSN-703), Communicator, USS WEST VIRGINIA BLUE (SSBN-736). His shore assignments include Shift Engineer at S1C Prototype in Windsor, Connecticut where he trained Officers and Sailors reactor plant operations and in the Pentagon on the Staff of the Deputy Assistant Secretary of the Navy for Ship Programs where he oversaw acquisition of SEAWOLF and VIRGINIA Class submarines. Commander Mayer received his Bachelor of Science Degree in Chemical Engineering from Pennsylvania State University in 1987 and was commissioned at Officer Candidate School Newport, Rhode Island. Commander Mayer is a graduate of the Air War College and the Joint and Combined Warfighting School. He wrote this paper while taking an elective course from the Air Force Counterproliferation Center on Homeland Security.

Colonel David B. Millar is the Director of Engineering and Maintenance in 1 Canadian Air Division at Canadian Forces Base Winnipeg, Manitoba. He recently graduated from the U.S. Air Force's Air War College, and holds a M.A. in Strategic Studies and a B. Eng in Computer Engineering from the Royal Military College of Canada. While at the Air War College, he submitted a paper on the potential of greater defense cooperation between Canada and the U.S. under the auspices of U.S. Northern Command. Colonel Millar won the General Charles G. Boyd award for best paper in the areas of regional and international security analysis in 2003.

Lieutenant Colonel Brian S. Norman serves as Chief of Joint Manpower for Headquarters, United States European Command (USEUCOM), Patch

Barracks, Germany. He and his team provide comprehensive manpower management, organization and resource control services to support USEUCOM's mission. In his current position, Lt Col Norman has focused upon directing analytical studies and facilitating actions for USEUCOM Transformation, creation of the European Plans and Operations Center and optimizing theater organizations and manpower to sustain the Global War on Terrorism and foster security cooperation. Lt Col Norman has held a variety of challenging staff and operational jobs, including Chief, Management Engineering Division for Military Airlift Command, Commander of the 7200th Management Engineering Detachment, Instructor at the Ira P. Eaker School for Professional Development, Congressional Enactment Manager and Executive Officer for Plans and Programs, Headquarters Air Force and Commander of the 20th Mission Support Squadron. He holds a B.S. in Industrial Engineering from the University of Missouri and an M.S. in Systems Management from the University of Southern California. Lt Col Norman is a distinguished graduate of Air Command and Staff College and a graduate of Air War College. His career efforts to improve Air Force combat capability through engineering innovation have earned him honor as the only two-time recipient of the Air Force-level *Manpower Management Award for Professional Excellence*, officer category. Lt Col Norman has written several papers on homeland defense issues, including "The Emergent Care Dilemma: Implications for the Nation, Air Force, and Disaster Response" for the United States Air Force Counterproliferation Center. Lt Col Norman earned the 2003 Air Force Homeland Security Award for his paper entitled "Gulf of Mexico, Offshore Energy Structure at Risk?"

Colonel Michael W. Ritz is the Air National Guard Special Assistant to the Director, USAF Counterproliferation Center. He also serves as chief of intelligence for the California Air National Guard's 146th Airlift Wing. Since 1997, he's been a visiting professor at the Air War College, instructing in core courses and elective courses in visual media and scenario development. Enlisting in the Air National Guard in 1968, Col Ritz was a still and motion picture photographer and public affairs supervisor for more than nine years. Commissioned in November 1977, he served as chief of public affairs before assuming the duties of wing executive officer in 1994. Since early 1998, he's been his wing's chief of

intelligence. A visual media expert and military historian, he has a Bachelor's Degree in drama & motion pictures from California State University, Northridge, and a Master's Degree in military history from the University of Alabama. He's a resident graduate of Squadron Officer School, Air Command & Staff College, and Air War College. When not pursuing his military endeavors, Col Ritz is a screenwriter/filmmaker living in his hometown of Beverly Hills, California. His most recent screen works include: *All Blood Runs Red*, *Hats In The Ring*, *Blue Fire*, *The Cyclist*, and *The Roundtable*.

Commander Dario E. Teicher is the Chief for Security Cooperation Plans, U.S. Southern Command, under the SCJ5 Strategy, Policy and Plans Directorate. He is responsible for developing and executing the U.S. Southern Command Theater Security Cooperation Strategy in Latin America and the Caribbean as directed by the Secretary of Defense. CDR Teicher is a graduate of the U.S. Air Force's Air War College, and holds an M.S. in Telecommunications Management from Naval Post Graduate School and a B.S. in Computer Science from NY Maritime College. He is a 1999 graduate of the U.S. Army Command and General Staff College. Also, CDR Teicher is a graduate of the Joint and Combined Warfighting School, Senior Program, Joint Forces Staff College, where he was the recipient of the 2002 General Douglas McArthur Writing Award having coauthored "Operation Sea Lion: A Joint Critical Analysis."

Major James C. "Chris" Whitmire is the USAF Counterproliferation Center's Homeland Security Officer. He is responsible for directing, developing, administering, and lecturing CPC Homeland Security endeavors and is the co-editor of the CPC's first homeland security book. Maj Whitmire is a senior Air Force and American Airlines pilot with over 3,800 hours in military and commercial aircraft and holds a Master of Science in Structural Engineering as a Guggenheim Scholar from the Institute of Aerodynamic Flight Structures, Columbia University, and a Bachelor of Science in Civil Engineering from the United States Air Force Academy. He is the recipient of numerous leadership and airmanship awards and the 1990 George W. Kamenicky Award as the Outstanding Graduate in Civil Engineering for the United States Air Force Academy.

USAF Counterproliferation Center
Maxwell Air Force Base, Alabama

Providing Research and Education on
WMD Threats and Responses for the US Air Force