

INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

ProQuest Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

UMI[®]

**TERROR IN THE AIR:
BIOLOGICAL WEAPONS, TERRORISM, AND ASYMMETRIC
THREATS TO U.S. NATIONAL SECURITY
IN THE TWENTY-FIRST CENTURY**

By

**Brian Robert Calfano
B.A., Rider University, 2000**

THESIS

**Submitted in partial fulfillment of the requirements for
the degree of Master of Arts in Public Policy**

Robertson School of Government

Regent University

Virginia Beach, Virginia

2001

UMI Number: 1410852

**Copyright 2001 by
Calfano, Brian Robert**

All rights reserved.

UMI[®]

UMI Microform 1410852

**Copyright 2002 by ProQuest Information and Learning Company.
All rights reserved. This microform edition is protected against
unauthorized copying under Title 17, United States Code.**


**ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346**

APPROVAL SHEET

This thesis is submitted in partial fulfillment


of the requirements for the degree of

Master of Arts in Public Policy.



10.31.01

Brian Robert Calfano

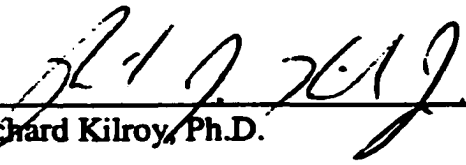
Approved October, 2001



Philip Bom, Ph.D.
Chairman



Joseph Kickasola, Ph.D.



Richard Kilroy, Ph.D.

**Copyright
2001
Brian Robert Calfano
All Rights Reserved.**

PREFACE

The research for this thesis began in October 2000. Initially, the scope of the research was limited to biological weapons and the challenges they pose to U.S. national security. Later, other asymmetric challenges, such as information warfare and chemical weapons, became areas of interest and research.

The pilot project for this thesis, consisting of research on bioterrorism, was presented at Old Dominion University's Graduate Program in International Studies Symposium in February 2001. In September 2001, the National Defense University publication, "Low Intensity Conflict and Law Enforcement," published a book review based on the pilot research.

In the summer of 2001, the role of the United States Intelligence Community in interdicting threats from asymmetric warfare became the second major area of focus of this thesis project.

By the time of the September 11th terrorist attacks on New York City and Washington, DC, most of the research, and a good portion of the writing, had been completed. The task of the time between September 11th and October 26, 2001 has been to reassess the validity of the original research and recommendations, and amend these positions where necessary. The result is a more balanced view of terrorism, asymmetric threats, and bioterrorism.

Writing in this very fluid period of national transition required the establishment of a cut-off point for research and writing – **October 26, 2001**. The story of terrorism and the challenges to U.S. national security will continue, and, hopefully, this thesis will provide some general guidance along the way.

ACKNOWLEDGEMENTS

This thesis, the people who helped make it a success, as well as the educational opportunity that provided it, would not have been possible without the constant Grace of God Almighty. Praise Him for His Son, Jesus Christ, our Savior and Lord.

Dr. Philip Bom has been my mentor, encourager, and teacher in so many ways. His love of music, scholarship, and the Reformed faith has been an inspiration and true encouragement to me, and will remain an asset for many years to come.

Dr. Richard Kilroy provided the guidance and opportunity to begin to explore this project back in October of 2000. I am profoundly grateful for his endorsement of my efforts, and for his constant willingness to remain interested in my academic and professional pursuits.

Dr. Joseph Kickasola has been an enthusiastic supporter of my efforts with this thesis, as well as a source of fresh ideas and insights into this very complex world.

Special thanks to Dr. K. Alan Snyder whose initial encouragement led me into the Master's program in Public Policy, and whose emphasis on the true principles of government are a continued source of personal enrichment.

A person could not ask for a better friend than Karen Johnson. Her presence in my life is true gift from God.

Sheldon Hudson is a true friend and a great mind through which to assess the validity of one's ideas and presuppositions, and a valuable proofreader.

Dr. David Rebovich, of Rider University, is the man responsible for me entering into the study of Political Science and Public Policy.

Dr. Kevin Oessenich, of Philadelphia Biblical University, has been a cherished friend, advisor, and source of warm encouragement throughout my graduate program.

My sister, Debra E. Calfano, of Cook College of Rutgers University, provided invaluable technical assistance with the scientific portions of this thesis.

Extra special thanks goes to my friend Tony Shea. Tony willingly read no fewer than 30 drafts of this thesis over the last year in order to provide editing assistance. Only a true friend would show such insanity!

Gratitude to Rich VanDerHorn, Carol Burres, John and Helen Yansak, Tyron Harris, Mark Buttich, Kimberly Luyben, Milt and Rita Havens, Bruce Jacobson, Chris and Sharon Ziegler, Bill Sheibinger, George and Joyce Janice, Dr. Jonathan Tucker of the Monterrey Institute of International Studies, Rita Mitchell, Brian Merritt, Rev. Dr. Richard Emmons, Chad and Rebecca Allman, Mary Brooks, Gwen Payne, LTC Vic Salazar, USA, Audrey Van Der Horn, Bill and Sylvia Jacobson, Evelyn Greenwood, Rev. Dr. Ken Smith, and my church family at Princeton Presbyterian Church for their encouragement and assistance.

Finally, I extend much love and many thanks to my wonderful parents, Al and Cindy Calfano, for their unwavering emotional, spiritual, and financial support.

CONTENTS

	Page
ACKNOWLEDGMENTS	v
ABSTRACT	vii
I. <u>INTRODUCTION</u>	1
II. <u>SECTION ONE: THE TWENTY-FIRST CENTURY BATTLEFIELD</u> The United States Under Asymmetric Attack Terrorism As a Performing Art	3
III. <u>SECTION TWO: DISASTER SCENARIOS AND WEAPONS THAT CREATE THEM</u> The Silent Terrors of the Asymmetric Threat The Threat of Conflation	34
IV. <u>SECTION THREE: INTELLIGENCE AND A SAFER NATION</u> Bilateral Reform Intelligence and Intra-Government Cooperation	58
V. <u>SECTION FOUR: POLICY RECOMMENDATIONS</u> Medical Response and Coordination The True Source of Security	112
VI. <u>CONCLUSIONS</u>	139
NOTES	140
SELECTIVE BIBLIOGRAPHY	156
VITA	158

ABSTRACT

In the aftermath of the September 11, 2001 attacks came many predictions concerning the future. Speculation on the nature of future terrorist action, as well as the ways in which to protect U.S. interests, became a common feature of the incessant media coverage. Unfortunately, some saw the recent attacks as an opportunity to sell books and distort fact, rather than a chance to begin to educate the nation about the complex realities of asymmetric warfare in the twenty-first century.

This thesis endeavors to make a contribution to the reader's general appreciation of the threats and challenges posed by asymmetric warfare, especially in the area of bioterrorism. It also explores the nature of terrorism, and views terroristic actions as the likely delivery method for asymmetric attack.

It endeavors to bring balance to the views that posit imminent destruction via a Weapon of Mass Destruction, all the while giving credence to the need to make significant policy changes to prevent even more devastating attacks in the future. Most importantly, this thesis explores how better intelligence, as well as a number of local, state, national, and international solutions, can help the nation respond to the terror in the air.

**For New York City's Finest
And Bravest – True American
Heroes**

**TERROR IN THE AIR:
BIOLOGICAL WEAPONS, TERRORISM,
AND ASYMMETRIC THREATS TO U.S. NATIONAL SECURITY IN THE
TWENTY-FIRST CENTURY**

Introduction

The American people will have to acquire a taste for the unpleasant side of global leadership, including the ramifications that come with standing firm against the practitioners of terror. This thesis posits that the United States faces a daunting task in containing terror and defending its interests against asymmetric attack. However, policies can be implemented to deal effectively with these challenges, and they will be the subject matter for this thesis.

This thesis looks specifically at the asymmetric threat that biological weapons, and bioterrorism, present to U.S. national security in the coming years. Much has been made recently of the anthrax-tainted letters that have been sent to various media outlets and political leaders. Note, however, that such attacks, especially the threats of such attacks, are not new. What is new, and productive, is the immense attention bioterrorism is receiving from the general public, and all levels of government. It is the kind of enthusiastic undertaking that was impossible to imagine when work on this thesis began in October 2000.

However, much still needs to be done, not only in terms of bioterrorism, but also in regard to more conventional forms of asymmetric attack like terrorists placing C4 explosives in trucks and aircraft, and high tech challenges like Information Warfare. In short, the approach to protecting the United States needs to be deliberate

and comprehensive. From all indications, the White House and Congress are committed to making this kind of broad plan a reality. The challenge, however, will be to make sure that media reports do not drive public policy, and that broad engagement in fashioning, implementing, and adjusting policies to protect from future terrorist attack becomes a fixture of long term projection and planning.

This thesis is a general survey of the asymmetric threat landscape with a special focus on biological weapons and bioterrorism. It regards all asymmetric threats as important and worthy of policy attention, but uses biological weapons and bioterrorism as examples of asymmetric attack whenever possible. In addition, though it provides a general context for terrorism as the delivery vehicle of asymmetric attack, this thesis does not attempt to address the changing geopolitical landscape of the international campaign against terrorist entities. It is not a treatise on terrorism, and would regard terrorism as the single biggest threat to national security whether Osama bin Laden is culpable in the September 11, 2001 attacks or not. After all, the Oklahoma City bombing is not attributed to bin Laden.

Section One looks at the United States post September 11, lays out the history of U.S. security policies against terrorism, and plots a course for addressing asymmetric challenges. Section Two examines the specifics of various asymmetric attack scenarios, as well as specific policy proposals relating to how the United States can begin to mitigate the effects of such aggression. Sections Three and Four offer possible solutions to the asymmetric and terrorist threat by examining the improvements necessary in the United States Intelligence Community, and how they might effectuate a better public policy response to the asymmetric battlefield.

Section One: The Twenty-First Century Battlefield

The United States Under Asymmetric Attack

Asymmetric warfare is the greatest threat to U.S. national security. The policy, political, social, and military decisions of the coming months will influence profoundly the state of U.S. national security in the twenty-first century. This thesis posits that the terrorist attacks on New York City and Washington, DC were horrific, but they may be tame compared with what may come.

What the United States experienced in September 2001 was a foretaste of asymmetric warfare. The sobering thought is that the September 11, 2001 aggression, while not the material of a typical asymmetric attack, has the potential to be the first tier of a multi-tiered, multi-faceted asymmetric campaign that utilizes biological and/or chemical weapons, information warfare, mobile “suitcase” nuclear weapons, radiological weapons (sometimes referred to as “dirty nukes” because they release deadly radiation without an explosion), enhanced high explosive weapons, or all of these Chemical/Biological/Radiological/Nuclear/Explosive (CBRNE) Weapons of Mass Destruction (WMDs) on U.S. soil.

Until the morning of September 11, the only places one could go to get an understanding of the havoc created by an asymmetric attack were in Tom Clancy novels. Four hijacked commercial jets have forever altered the U.S. perception of

domestic security threats, and have brought the asymmetric realities of the new century into the national living room.

The Pentagon describes asymmetric warfare as the countering of an adversary's strengths by focusing on its weaknesses, and the United States certainly has its weaknesses.¹ Think of asymmetric warfare as an enemy intentionally trying not to match conventional, or symmetric, military strength with its adversary, in this case, the United States; but, rather, to focus on the points of the nation's greatest weaknesses – its centers of political, economic, and military gravity.

The United States certainly has points of weakness: its porous points of entry and exit, the virtually unrestricted travel of its citizens, and an overwhelming reliance on communication technologies make the United States, in many ways, the most vulnerable nation in the world to non-conventional, asymmetric attack. The Department of Defense's much anticipated 2001 Quadrennial Defense Review, released on September 30, 2001, assessed the threat of future asymmetric and terrorist action against the United States:

The attacks against the U.S. homeland in September 2001 demonstrate that terrorist groups possess both the motivations and capabilities to conduct devastating attacks on U.S. territory, citizens, and infrastructure. Often these groups have the support of state sponsors or enjoy sanctuary and protection of states, but some have the resources and capabilities to operate without state sponsorship. In addition, the rapid proliferation of CBRNE technology gives rise to the danger that future terrorist attacks might involve such weapons.²

Those entities that pose a threat to U.S. national security via asymmetric means possess both the capability and intent to do the nation harm, which is why they are regarded as national security threats.

However, as this thesis will document, the ability of these entities to perpetrate a mass casualty WMD attack using CBRNE technologies is not a certainty in 2001. It is more likely that terrorists will continue to pull off low-grade attacks, perhaps with the hint of escalating tactics that will create panic in the general public.³ In such an instance, panic is likely to become an effective weapon of mass disruption, not destruction, as the October 2001 rash of anthrax-tainted letters demonstrates.⁴

Since it is more difficult to pull off a successful WMD attack, terrorists might opt to go with what has always worked: a conventional bombing. Even the hijackings of September 11, though a chilling wake-up call for the nation, was not in itself a great technical undertaking; rather, it was modified version of the Japanese kamikaze. A variety of government studies concur.

A September 1999 General Accounting Office (GAO) report found that the threat of bioterrorism, a common term used to describe an intentional release of a pathogen into air and/or water supplies, was unlikely, especially in regard to the most deadly pathogens.⁵

A second GAO report in July 2000 criticized government agencies for exaggerating the possibility of a bioterrorism event in the United States.⁶ Recently the Gilmore Commission, a distinguished panel of statesman, terrorism experts, and scientists appointed by Congress and led by Virginia Governor James Gilmore, reaffirmed its contention that a WMD attack, especially one using biological weapons, is a low probability.⁷

Yet, as September 11, 2001 proved, assessing national security threats is more of an art than a science. Therefore, nothing can be taken for granted, or dismissed out of hand.

Bioterrorism receives special consideration in this thesis apart from the other WMDs since it is an emerging threat that has yet to be fully assessed. Unlike chemical weapons, which have found their way onto the battlefield, or nuclear weapons, which claimed the tactical spotlight during the Cold War, biological weapons, though dangerous and potentially more lethal than a nuclear bomb, have taken on almost mythological status.

The public might have no greater enemy than an over active imagination in terms of this threat. Yet the possibility exists that, since these weapons are in the hands of some unsavory entities, bioterrorism could find its way to U.S. territory sooner rather than later. Other forms of WMDs are also considered here, since they might play important roles in the terrorists' cookbook of schemes.

Note that entities wielding asymmetric technologies do not have to come in the form of international terrorist organizations. Yet, due to the overwhelming national war on terrorism, this thesis holds to the premise that, at least for the immediate future, the perpetrators of this new kind warfare are likely to at least attempt to use terroristic methods of delivering asymmetric attacks.

Once an attack has occurred, in whatever form, the burden of rescue, relief, and treatment rests squarely on the shoulders of the nation's emergency response infrastructure. These men and women, firefighters, police, Emergency Medicals Technicians (EMTs), and others, are called upon as the first line of defense. Yet their

jobs might be hampered by the lurking danger of other forms of asymmetric attack designed to fragment, and then disable, the government's ability to provide and lead crisis relief.

In fact, what occurred in New York and Washington, DC is likely the opening salvo in a sustained terrorist campaign against U.S. targets. The reason: terrorists thrive on the opportunity to use fear and chaos as weapons against their enemies. Their recent tastes of success might only embolden their spirits and motivation to launch more attacks, or at least threaten more attacks, that next time might target critical government infrastructure.

What could be more horrifying for U.S. citizens than to find that the same government that has promised swift retaliation and bold leadership in this time of crisis is itself the victim of a calibrated asymmetric attack? For instance, consider that, with a good portion of the emergency response infrastructure of New York City (and the surrounding communities from New Jersey and Connecticut) engrossed in a challenging recovery effort in lower Manhattan, other sections of the city, and the greater metropolitan area, are more vulnerable to both further terrorist attack, and other forms of domestic upheaval.

For instance, if terrorists want to place explosives near popular destinations on the Upper West Side of Manhattan, would the New York Police Department be in a position to detect their suspicious behavior if they are preoccupied with a bomb blast in the Lincoln Tunnel at rush hour? Are there enough New York City firefighters and ambulances left to put out more fires and treat more wounded?

What if, unrelated to any planned terrorist attack, the people of New York City decided to take advantage of the chaos created by a terrorist attack and start robbing stores and other centers of commerce; are enough police on the streets to keep the peace? The real answers might be too distressing to contemplate.

A terrorist attack doesn't have to have the visual impact of jets crashing into skyscrapers. The actual perpetration can be so insidious, so silent, that it is unnoticed completely. For instance, was anyone paying attention to the identities of "volunteers" who lent their efforts to the rescuer operations in lower Manhattan? The Environmental Protection Agency and National Guard say they were.⁸

Yet it is not outside the realm of possibility for someone to go undetected in all the bustle of any major city with a package of dry anthrax spores. If released properly into the air, these spores could infect thousands, including emergency response personnel, patients receiving treatment in local medical centers, as well as residents of adjoining municipalities. Such an attack would further diminish the emergency response infrastructure while, at the same time, placing on it an even greater burden for emergency services.

In the same way, national preoccupation with the tragedy of September 11 might lure many citizens into believing that the problem is confined to two major cities, leaving other areas, especially rural food manufacturing and distribution centers, medical treatment centers, and antibiotic storage facilities susceptible to sabotage. Suddenly, a disaster once confined to the "big city" has taken on national implications in terms of a spoiled food supply, infected hospital workers, unusable antibiotics, and a panicked public.

Another phase of a multi-tiered asymmetric terrorist attack is the disabling of the law enforcement and military sectors from carrying out their investigation and security responsibilities. Information warfare is a significant threat to the response infrastructure in that it can disrupt and/or disseminate false information both to and between civilian leaders and the military's command and control apparatus. How would it look if the world's most powerful military were unable to carry out its retaliatory mission against terrorist entities because its computers were taken off-line, or U.S. fighters hit the wrong targets because the coordinates for their sorties were figured with bogus data?

The threat of information warfare is well known in defense circles. The Pentagon discovered in March 1998 that unidentified hackers were hacking into secure defense computer systems on a regular basis.⁹ There is little that the Pentagon can do to stop the hacking and/or identify the hackers. Imagine the chaos if hackers were to disable U.S. satellites responsible for Internet commerce, cell phone transmission, ATM transactions, and the host of daily computer operations on which the nation has come to rely.

The current situation is rife with possibilities for terrorists with asymmetric aspirations, and, thus far, the emergency response community has been put under great strain. However, as these asymmetric scenarios show, the greatest attacks may still be in the works.

Of course, there are possible solutions to these problems, solutions that might get a fuller hearing now that the United States has had its wake-up call on national security challenges in the new century.

The United States must have better intelligence and a well-trained emergency response command chain to respond effectively to, and better anticipate, asymmetric attacks. This requires more money for more intelligence analysts, more secure computer networks, more antibiotics with comprehensive national distribution, and emergency workers versed in the procedures to treat the medical fallout from biological and chemical weapons.

Important also in defending the United States against an asymmetric attack is better cooperation between the government agencies responsible for national security. For example, reports continue to surface that the FBI and CIA continue to withhold information from the other. Bureaucratic territorial attitudes perhaps led to the intelligence failures of recent days, and any inter-agency friction must be kept to a minimum.

Better intelligence is the major key to better national security. Since the asymmetric means of attack focus not on the nation's strong conventional military capabilities, but, rather, on its civilian, information, and commercial vulnerabilities, more aircraft carriers and armored tank divisions are not the answer.

The best prevention is better national eyesight: the United States Intelligence Community (IC) must have enough intelligence analysts in place to be able to process the large amount of raw data transmitted by electronic intelligence, open source collection, and human intelligence sources. These analysts must then be afforded the access necessary to make the case for specific policy changes to Congress and the Administration.

Yet something else is in order – a new civic and political focus on the nature of asymmetric warfare. Historically, and with very few exceptions, the United States has never had to embark on a protracted defensive engagement that, when its resources and people were committed fully, it didn't win decisively, and rather quickly. This will not be the case with international terrorism and asymmetric warfare. The nation is too vulnerable to this kind of attack, and the perpetrators are too motivated for the solutions to be found in near-term retaliatory policies.

The American people will have to acquire a taste for the unpleasant side of global leadership, including the ramifications that come with standing firm against the practitioners of terror. This thesis posits that the United States faces a daunting task in containing terror and defending against asymmetric attack. However, policies can be implemented to deal effectively with these challenges, and they will be the subject matter for this thesis.

On September 12, 2001, Secretary of Defense Donald Rumsfeld declared the attacks in New York and Washington, DC as part of a new, twenty-first century battlefield.¹⁰ This thesis is focused on laying bare the specifics of this new battlefield, in regard especially to asymmetric threats, and, biological warfare in specific. To begin, an understanding of the psychological origins of asymmetric warfare must be established.

The Motivation for Asymmetric Attack

The ideological impetus for asymmetric attack is found in the writing of ancient Chinese philosopher Sun Tzu. In his seminal work, *The Art of War*, Sun Tzu wrote:

All warfare is based on deception. . . . Hold out baits to entice the enemy. . . . Pretend to be weak, that he may grow arrogant. If he is taking ease, give him no rest. If his forces are united, separate them. Attack him where he is unprepared, appear where you are not expected.¹¹

The United States did not find itself facing down the Sun Tzu doctrine overnight. The transformation began immediately after the end of the Cold War. With the Cold War over, the bi-polar international power vacuum that had provided an ironic sense of international stability for half a century was now gone. The United States' defensive and diplomatic communities were left with the unprecedented task of identifying and quantifying national security threats for a new century that was steaming ahead with continued international economic and political assimilation, not military polarization.¹²

This was a new political, economic, and military reality for the United States. The fifty-year Cold War with the Soviet Union, and an isolationist stance prior to World War II, conditioned policy makers to think in terms of limited conventional, bi-polar, and symmetrical approaches to national security policies.¹³ Though the threat of nuclear war was the backdrop for five decades of US-USSR tension, both sides were generally tepid in pursuing the logical outcome of mutually assured destruction.

Then, in the late 1980s, breakthrough nuclear reduction summits were held, treaties were signed, walls came down, and military aggression in the Middle East became the fulcrum for a united East-West military and diplomatic effort. The final implosion of the Former Soviet Union (FSU) in the early 1990s gave the United States the distinction of sole superpower status. It also inaugurated the opening scenes

of a continuing saga of how the United States planned to navigate through the evolving morass of covert threats to its national security.

The Sun Tzu quote mentioned above will aid in the understanding of asymmetric threats. Sun Tzu promulgated the virtues of a well-planned and executed offensive against an enemy. For him, the hallmark of offensive military excellence was epitomized in the general who precipitated victory without having to physically expend his resources. More than two millennia after his death, the Sun Tzu doctrine is now the mantra for entities that threaten U.S. interests: the most successful war makers are the ones who can subdue the enemy without firing a shot.¹⁴

Today, entities from around the world that harbor aggression against the United States for geo- and/or religio-political reasons, ideological motivations, and/or aggressive nationalistic tendencies are serious about inflicting harm against U.S. interests. Again, note that the conventional military superiority of the U.S. armed forces makes conventional, or symmetrical, confrontation unlikely. Thus, asymmetric tactics, designed to bypass U.S. conventional superiority, are attractive options.

To assess competently the state of U.S. preparedness for the specter of asymmetric attack, it is necessary for this thesis to document, as accurately as possible, the specifics of the asymmetric threat. Of central concern here are the nations and organizations that, according to U.S. intelligence and media sources, possess the means and motivation to unleash asymmetric aggression. These entities are assessed as threats to U.S. national security if they possess the capability and the intent to perpetrate harm against the United States.

It is possible that asymmetric tactics might be utilized in conventional warfare; there is nothing that prevents this occurrence. The Japanese contemplated biological weapons attacks against the United States in the waning months of World War II.¹⁵ More recently, Saddam Hussein was suspected of releasing chemical weapons in combat.¹⁶ However, in the absence of conventional military engagement, the options for perpetrating an asymmetric attack are limited to non-military options. This is especially true for those delivery methods that carry the element of surprise; in other words: terrorism.

The Typology of Terrorism

What Is Terrorism?

Dr. Cindy Combs of the University of North Carolina-Charlotte makes several observations concerning the dimensions of modern day terrorism. The first is a definition of terrorism itself:

... terrorism will be defined as a synthesis of war and theater, a dramatization of the most proscribed kind of violence – that which is perpetrated on innocent victims played before an audience in the hope of creating a mood of fear, for political purposes.¹⁷

From this definition, it is clear why terrorists would want to use the asymmetric means of attack: most of the victims of such attacks would be civilians due to the nature of the destruction created by biological and chemical weapons, information warfare, and portable nuclear weapons. (In this instance, both Combs and this thesis conceptualize “innocent” victims as being members of the civilian population, although it is possible under certain circumstances, like the USS Cole

bombing, to include members of armed services in the same category. Unless otherwise stated, “innocent” shall refer to civilians only.)

Recent developments send mixed signals to policymakers on this front. On the one hand, the bombings of the World Trade Center in 1993, the federal building in Oklahoma City in 1995, the USS Cole in 2000, and the World Trade Center and the Pentagon in 2001, demonstrate the inherent vulnerabilities of domestic and military targets to terrorism. On the other hand, research conducted by the State Department in 1997 shows that both the number of incidents of international terrorism, as well as the number of casualties incurred by those incidents, had dropped precipitously since the mid-1980s.¹⁸

However, it is doubtful that, given the events of recent days, any policymaker would apply a quantitative, rather than qualitative, approach to analyzing the effects of terrorism. This is especially important, for terrorism itself has evolved throughout the twentieth century into various forms.

Mass Terror: is sponsored and conducted by a state. It targets the general population either of the same state, or another state.

Dynastic Assassination: is an attack on a state’s leadership.

Random Terror: entails the perpetration of terrorist attack in order to harm people who happen to be in the area at the time of the attack. This was the form of terrorism used in the World Trade Center attack in September 2001.

Focused Random Terror: is the perpetrating of an attack where leadership and infrastructure centers are located. The Pentagon attack in 2001 can be described as Focused Random Terror.

Tactical Terror is directed specifically against the ruling apparatus of a state as a “broad revolutionary strategic plan.”¹⁹

Whereas in earlier times terrorists would target political leaders, the more recent acts of kidnapping and civilian execution signaled a shift from the dynastic assassination plots of an earlier era. The present day is witness to yet another shift in terrorist targeting. The State Department’s 1997 summary report on global terrorism patterns uncovered a growing trend: the overwhelming majority of terrorist attacks against U.S. interests were targeted at the business community and government institutions, like the 1998 African embassy bombings.²⁰

The destruction of the World Trade Center, and its subsequent effect on the U.S. economy, bears out this notion. By definition, attacks on business targets are attacks on civilian targets, making the prevention of such attacks a necessary item for policymakers and the national security policymakers to address.

For the government to be successful in its monitoring of terrorist developments, and prevention of terrorist attacks, it has to focus on two main lines of support for the terrorist community – the states that support terrorist entities both tactically and financially, and the prevailing ideological and religio-political impetuses that provide the emotional and intellectual nourishment for the terrorists themselves.

For states that either support and/or direct terrorist entities directly, or at least take a supporting role in providing the entities with refuge and resources, the terrorist action itself is viewed as an instrument of foreign policy. This is probably no more apparent than in the incessant terrorist acts perpetrated in relation to the Israeli-

Palestinian conflict. According to Combs, the purpose behind state-sponsored terrorism is for a state or states to weaken the political, military, and/or economic stability of other states.²¹

The sponsoring states may support the activities of indigenous terrorist cells, international terrorist networks like Osama bin Laden's al Qaida organization, or both. According to Combs, states like Syria, Iran, Libya, and Sudan have even formed private partnerships in sponsoring terrorist activities.²²

For states looking to use terrorism to weaken the United States in some manner, the more usual options are not at their disposal. For instance, the relative stability of the U.S. political system makes political assassination less of a threat to stability than it is in many Third World systems. In addition, the U.S. armed services are far less susceptible to the effects of covert undermining than are other military organizations, although, as this thesis will explore, the U.S.'s political, military, and economic functionalities are susceptible to asymmetric attack.

Terrorists, therefore, must look for other national vulnerabilities, finding them in the civilian population and commerce sectors. Mass death and interruption of commercial exchange, as was perpetrated in the 2001 World Trade Center attack, would serve to weaken the U.S.'s world position, and would be best accomplished through an asymmetric attack that utilizes a biological or chemical weapon, information warfare, portable nuclear devices, or all of these.

Questions of possible terrorist motivation surround the discussion of terrorism and asymmetric warfare. Combs points to a variety of ideological and religious impetuses. Most notable is perhaps the predominant theme of millenarianism that

espouses personal redemption through violent means. This belief system is common among terrorists with ostensible religious affiliations, and is manifest usually in suicidal actions on the part of terrorists. The terrorists believe that their violent acts will speed the coming of the millennium – the judgment and punishment of the evil the enemy embodies.²³

Another strand of motivation is found in religious fanaticism, especially in the principles of the Islamic Jihad that is set on waging a “holy” war in the name of Allah. The Shiite Muslims, who are the primary perpetrators of such religiously inspired terrorism, have a long history of sabotage, mass murder, and guerrilla warfare against Sunni Muslims, Jews, and Christians. The primary tenet of this terrorist cause is martyrdom, which serves as a compelling justification for one’s own death in the furtherance of the fanatical religious cause.²⁴ In the same way, some domestic terrorists have distorted Christian principles in order to provide a religious justification for their aggression.

Well known to Americans is the neofascist line of thinking that is championed by several U.S. groups like the Aryan Nation, the Order, the White Patriots Party, and the Covenant. These groups espouse disdain for the federal government. Timothy McVeigh was a member of a neofascist paramilitary group in Michigan that is suspected of intending to launch terrorist attacks against government institutions.²⁵

Issue orientation rounds out the list of major terrorist motivations. These issues range from abortion, to environmental and animal protection. Some radical opponents of abortion have been known to bomb abortion clinics and/or assassinate abortion doctors. Certain animal rights groups have been found guilty of burning

down animal testing centers; while some environmental groups have gone on record as suggesting that killing people would be a justifiable act if it meant saving trees.²⁶

Knowledge of the contours of the motivations for terrorism is a necessary lead-in to consideration of the performance dynamic of the terrorist acts.

Terrorism As a Performing Art

Recent days have demonstrated that the twenty-first century asymmetric threats, and the terrorist vehicles that deliver them, are no longer confined to esoteric policy discussion and overlooked congressional testimony. Instead, the threats of mass destruction, and the entities that perpetrate them, are really performers trying to shock their audience. This description may seem inappropriate until considering the full symbolic implications of the events of September 11, 2001.

The idea that terrorists are actors performing shocking acts designed to terrorize the world may seem like a trite description. However, the terrorist profile is changing.²⁷ Just note the new, seemingly “rock and roll” lifestyle of the terrorists suspected of hijacking the jets that crashed into New York and Washington. According to Rand Corporation advisor Brian Jenkins, the terrorists lived a life that included material pleasure, usually frequenting bars, eating in restaurants, and enjoying other local amenities, all the while cognizant of their date with destruction.²⁸

Actors don't spend time thinking about themselves as actors; rather, they practice for their shows, and, when they're not practicing, they usually go about their daily business, much like the new manifestation of terrorist. Consider now the specifics of the most effective terrorist performance on the U.S. mainland in history.

First, in order to set the stage, the terrorists extracted the highest form of visibility available – immediate and live television coverage. Much has been made of the fact that the kamikaze jet crashes into One and Two World Trade Center occurred just as the majority of the WTC's occupants were getting ready for the workday. However, if maximum building occupancy were the goal, the terrorists would have had more available bodies during the mid-morning hours, or about an hour and a half after the actual attack.

The possible reason for the attacks between 8:30 and 9AM was that the traffic helicopters reporting on the morning commute for the local New York media outlets were airborne and would be taking pictures of regular transportation issues until just after 9AM. The shocking professional footage of the hijacked jets ramming into the upper floors of the World Trade Center would have likely not been shot, especially from an aerial view, if the attack was aimed at taking out as large a civilian population in the towers as possible in the mid-morning hours.

Second, the symbolism in the timing of the attacks was profound. Just as the New York media was trying to make sense of the violent explosions that rocked the twin towers, personnel at the Pentagon began receiving reports of the unfolding catastrophe. As the U.S. defense establishment watched the New York drama in disbelief, the third suicide jet slammed into the venerable defense fortress. This was deliberate timing.

Certainly, it would have been possible for the terrorists to attack all three sites simultaneously, or even for the Pentagon to be the first target. Instead, a full thirty minutes went by while the Department of Defense began to consider the ramifications

of the New York attacks. Then, the headquarters of the most powerful military in the world was itself the victim of a successful terrorist penetration. The symbolism was piercing: even the mighty U.S. national defenses are no match for the rapier quick devastation of a well-planned terrorist campaign.

Third, the timing of the events impeded the effectiveness of, and, perhaps the nation's confidence in, the emergency response infrastructure. As police, fire, ambulance, and other unformed response personnel descended on lower Manhattan, and as they entered the compromised towers, the heroism of these men and women, and their dedication to their profession, became the fodder for the symbolism of tragedy. The implosion of the World Trade Center, and the certain deaths of hundreds of these emergency response workers, sent a clear signal to the nation: your civil recovery and response mechanisms are just as vulnerable to attack as your civilian population centers and defense institutions.

Fourth, the terrorists made great symbolic use of the icons of U.S. aviation. Long hailed as the safest form of travel, and taken for granted as an economic, social, and transportation necessity, the paralyzing fear experienced by many flyers in the aftermath shows the deep wounds inflicted on the national symbols of personal freedom of movement. Interesting also are the actual airlines the terrorists targeted. Rather than hijack planes from Delta or Continental, which has a major hub at Newark International Airport (the location of one the hijackings), United and American Airlines jets, both displaying logos symbolizing national freedom and strength, as well as larger model 757/767 aircraft, were the tools used in the attack.

Fifth, the venerable symbols of capitalism and national strength, the World Trade Center and The Pentagon respectively, were the targets of the attack. In ninety minutes, terrorists leveled landmarks and cast doubt on the economic and physical security of a nation that believed itself impervious to such disasters.

Symbolism is important to terrorists. Since their business depends upon creating terror, the greatest amount of shock value that can be incorporated in an attack the better. Yet the terror of the 11th of September 2001 may be only the beginning. Terrorists might have other targets in mind that could be even more shocking to the American psyche than what occurred in New York City and Washington, DC.

For instance, it is not impossible that major military communities, like Hampton Roads, Virginia, might be the next place for a terrorist strike. The objective for terrorists could be to strike at the families of service men and women deployed for military action, thereby distracting and demoralizing the military personnel half way around the world, and perhaps making the conventional military strength of the United States less formidable in the process.

The Terrorist Mind

What makes a terrorist and a terrorist operation tick? The answers are elusive, for even the best of U.S. intelligence has a hard time answering that question. However, there are specifics that are well known about the terrorist mind and the way it operates under specific conditions. Terrorism expert Edgar O' Balance offers this compendium on the characteristics of a "successful" terrorist.

Dedication: The terrorist must be a fedayeen, a “man of sacrifice.” He cannot take a part-time attitude toward his work. He must also have unwavering dedication to the leadership of the terrorist organization of which he is part.

Personal Bravery: As the attack on the World Trade Center and Pentagon demonstrate, bravery, as well as a willingness to sacrifice one’s life, is essential.

Without the Human Emotions of Pity or Remorse: The terrorist must be able to kill anyone, man woman, or child, with a moment’s notice, and without any remorse.

Fairly High Standard of Intelligence: A terrorist has to be able to collect and assess information, devise and perpetrate attacks, and evade capture. This requires a certain level of intelligence and ability.

Fairly High Degree of Sophistication: In order to mix with the more sophisticated quarters of society, the terrorist must be able to adapt and blend into such situations.

Reasonably Well Educated With a Fair Share of General Knowledge: O’Balance is adamant that a university degree is “almost mandatory” for the successful terrorist of the twenty-first century.²⁹

This list all but eradicates any notion of the terrorist as the lone nut working without a well-devised plan of action and financing. If, as it seems, the terrorist organizations responsible for the increasing attacks against the United States are deeply entrenched, well funded and organized, as well as a capable of exacting tremendous financial and human losses via asymmetric attack, an examination of U.S. security policy over the last few years is in order.

The Evolution of National Security Policy and Asymmetric Threats

The United States has been concerned about the threat of terrorism and asymmetric threats in one form or another since the 1970s. However, it wasn't until Vice President George H. W. Bush's Task Force on Terrorism made its recommendations in 1985 that a national program to combat terrorism received organized attention. In 1986, President Ronald Reagan issued National Security Decision Directive (NSDD) 207, which provided guidance for how law enforcement was to respond to a terrorist attack abroad.

The National Security Council (NSC), State Department, and Federal Bureau of Investigation all had roles to play in combating and respond to acts of terrorism overseas.³⁰ Little or no provision was made for procedures to follow in a domestic terrorist attack.

The focus on international acts of terror in NSDD 207 was not modified until two months after the 1995 bombing in Oklahoma City. President Bill Clinton ordered Presidential Decision Directive (PDD) 39 in May 1995, which reaffirmed the roles of the State Department and FBI under NSDD 207, but also included the designation of the Federal Emergency Management Agency (FEMA) as the lead agency responsible for responding to terrorist attack on domestic soil. In May 1998, Clinton issued PDD 62, which reaffirmed PDD 39, and established a National Coordinator for Security, Infrastructure Protection and Counterterrorism inside the NSC to coordinate the response of the various agencies involved in counterterrorism operations.³¹

Conservatives charged that Clinton did not make national security a priority during his tenure. Whether those charges are correct or not, on a busy Friday

afternoon in January 1999, Clinton demonstrated that he did possess knowledge of the emergence of terrorism and asymmetric threats when he sat down for an interview with reporters from *The New York Times*.

In a pronouncement that went largely unreported by a majority of the media, Clinton stated that it is “highly likely” that, within the next three years, terrorists will launch a biological weapons attack on American soil.³² *The New York Times* ran the story on January 22, 1999. Clinton never followed up on his initial statement to the paper. That job fell to his Secretary of Defense, William Cohen. In remarks made to former *Washington Post* defense correspondent George C. Wilson in 1999, Cohen elaborated on Clinton’s warning.

How do you defend against someone who has a biological agent? You have no way of knowing where it originated, who set it off, who to respond against. How do you deal with it? What about anthrax shots for the general public? How do you manage this with the first responders [local police, firemen, doctors, nurses] who can’t even identify what the biological agent was? It’s going to take us some time to organize, to train, to have supplies on hand to deal with it. All of that is very imposing.³³

As with Clinton’s interview, Cohen’s remarks were not well publicized. Perhaps as a result, few U.S. citizens viewed the threat of asymmetric attack against the United States as a likely scenario, if they considered the threat at all. Since Clinton and Cohen attested to the likelihood of such an attack, it might be assumed that the national security community has since developed an effective defense against asymmetric attack. The evidence suggests that a great deal of organization has occurred, but it is yet clear how effective these changes will be in the wake of an attack using a WMD.

President George W. Bush issued National Security Presidential Directive (NSPD) 1 on February 13, 2001 in order to modify the command structure established by PDD 62. The new structure includes Principles and Policy Coordinating Committees within the NSC that are responsible for the disparate elements brought to bear in combating terrorism: Counterterrorism and National Preparedness; Proliferation; Counterproliferation, Homeland Defense (Security); Intelligence and Counterintelligence.³⁴

These organizational initiatives aside, some insist that the Clinton and George W. Bush White Houses, as well as the Armed Services Committees in Congress, have been slow in providing for the development and implementation of security policies against asymmetric threats. Tennessee Senator Bill Frist criticized the disjointed approach of the federal government in attending to the threat of a bioterrorism to *The New York Times* on September 28, 2001:

In a report issued last week, the General Accounting Office said the government's bioterrorism planning was so disjointed that the agencies involved could not even agree on which biological agents posed the biggest threat. Officials at the Centers for Disease Control and Prevention, for instance, consider smallpox a major risk. But the Federal Bureau of Investigation does not even put smallpox on the list.

At the same time, there are holes in the federal bureaucracy, where two important health positions remain unfilled: commissioner of food and drugs and director of the National Institutes of Health. The Food and Drug Administration will play a crucial role in the development of vaccines or treatments for use in the event of a biological attack, but President Bush and Congress – in particular Senator Edward M. Kennedy, Democrat of Massachusetts – have been unable to agree on an acceptable nominee.³⁵

The September 11, 2001 attacks have changed the focus of many lawmakers who were content to increase spending on conventional security initiatives that fall in line with the traditional economic interests of their local constituents. As a result,

serious consideration of the domestic terrorist and asymmetric threats has been consigned to relatively small appropriations in the back pages of the annual budgets.³⁶ Recent actions from government officials in the wake of the anthrax letter incidents of October 2001 suggest that mindset is changing, however.³⁷

Some practical preparations were undertaken prior to the national wake-up call on September 11, 2001. By mid 2001, preparation for asymmetric attack had taken form, albeit in a less comprehensive manner than some would prefer. Author and *Newsweek* writer Laurie Garrett commented on Clinton's 1998 initiatives for beefing-up asymmetric defense, especially in the area of bioterrorism:

... Clinton requested congressional approval of a \$10 billion antiterrorism program, including \$86 million for improving public health surveillance, \$43 million for research on vaccines for anthrax, smallpox, and other potential bioweapons agents, and \$300 million for stockpiles of essential drugs and vaccines. The proposed expenditures doubled the previous year's bioterrorism budget.³⁸

It was expected that with Bush's appointment of Air Force General Richard Myers to Chairman of the Joint Chiefs of Staff in October 2001, the policy emphasis on preparedness against asymmetric threats would continue. This is especially true considering that the Air Force is viewed as the service branch most receptive to developing and implementing newer technologies and security procedures.³⁹ The DoD's preparation of the release the latest version of its Quadrennial Defense Review (QDR) is expected to provide greater insight into the DoD's commitment to securing against asymmetric threats.

The new QDR repositions DoD policy from a threat based to a capabilities based model. This change is based on the realization that threats may manifest in a

variety of forms, thereby impeding identification of all entities that pose a potential threat. Focusing on capabilities will allow the DoD to protect against similar capabilities wielded by disparate aggressors.

This shift to a capability-based model implies the need for a far-reaching transformation of U.S. defense; a transformation that the QDR insists must begin in earnest.

Section One of the 2001 QDR considers “America’s Security In The Twenty-First Century.” It posits three national goals: promote peace, sustain freedom, and encourage prosperity along the network of political and economic relationships the U.S. enjoys with its friends and allies. The QDR sees the military’s security role as providing the basis for stable international relationships. This role is even more important in the aftermath of September 2001, since the U.S. vulnerability to actors wielding asymmetric capabilities and methods of delivery, and is becoming more quantified.

Section One also assesses regional security developments. It looks at Asia as a gradually emerging source of significant military competition, the Middle East as a mixed economic and security challenge, and Russia as potential security partner, albeit one that continues to pursue policy objectives inimical to U.S. interests.

The new QDR establishes four defense policy goals: to assure allies and friends, dissuade future military competition, deter threats and coercion against U.S. interests, and, if deterrence fails, decisively defeat any adversary. Execution of these goals requires transformation of the military’s global posture. The QDR looks to the strengthening of joint operations for this transformation.

Specifically, the QDR calls for developing integrated combat organizations with rapid response forces, improved command and control over these joint operations, and the fostering of a joint professional atmosphere. It proposes a Standing Joint Task Force headquarters in each of the regional combatant commands to provide standards and procedures for joint operations.

The 2001 QDR places emphasis on increased information and decision superiority via timely, comprehensive, and relevant intelligence. Human Intelligence (HUMINT) receives a great deal of consideration in the overall intelligence strategy. The QDR admits to deficiencies in the collection and dissemination of HUMINT, and makes a general statement about the need for improvement. The review also calls for more collaborative intelligence, surveillance, and reconnaissance operations.

The QDR suggests that the intelligence products will become more effective if the tasking, processing, exploitation, and dissemination functions are integrated, and proposes investments in workforces with the analytical tools and databases to improve intelligence integration and planning.

The QDR also focuses on transforming priorities to address asymmetric capabilities that threaten U.S. bases of operation at home and abroad.

Specifically, the QDR proposes greater investment in DoD preparedness in assisting local authorities and lead federal agencies in responding to a CBRNE attack. It draws on the existing Weapons of Mass Destruction Civil Support Teams composed of Marine and National Guard personnel, and proposes enhancing training for Army Reserve components in this area.

Information Operations is also a transformation priority. The QDR recognizes the importance of superior information collection and dissemination, while concurrently denying effective information operations to adversaries. As with intelligence, the QDR suggests that current deficiencies can be remedied through an integrated approach to developing, acquiring, and programming future information operations.

Though much of the focus is on Homeland Security, the QDR suggests that the success of the nation's defense posture comes from maintaining and increasing the ability of U.S. forces to project power around the globe. Better force projection depends on new investments that address the growing threats posed by submarines, air defense systems, cruise missiles, mines, protecting strategic transport aircraft, and protecting U.S. force operations from chemical and/ biological attack.

The QDR views denying enemies access to sanctuary as an important transformation component. It suggests further investment in sustained surveillance, tracking, and rapid engagement in order to deny enemies safe haven. Space assets, which are valuable surveillance components, are identified as a possible target for asymmetric aggression against the United States. The QDR recommends modernization of these assets in order to provide both increased operability and asset protection.

Implementing these transformation priorities requires a rethinking of how DoD performs its tasks. To that end, the QDR suggests several innovations in DoD policy. First, it gives general support for a new round of base closings. Second, it calls for an upgrade of DoD accounting systems and practices. Third, the QDR

encourages greater risk taking on new technologies that are being developed rapidly in the private sector.

Another part of the retooling process is encouraging DoD talent to stay in their positions. The QDR proposes beefing up incentives to recruit and retain talented personnel, and encourages the services to find ways to persuade talent to make national defense a life long career. Business processes and infrastructure, identified as outdated, will be transformed to accommodate the quick flow of data and information. Such transformation requires a streamlining of overhead structure and consolidation of base infrastructure.

Along with these consolidations, the QDR advocates greater resources to improve facility structure, citing that a significant portion of the defense infrastructure has begun to age beyond acceptable levels. The QDR suggests ways to address risk management. It looks at four dimensions: force management, operational risks, future challenges, and institutional risks. To address all four, the QDR recommends a combination of realistic tempo standards, planning for a wider range of contingencies, better future risk assessment, greater experimentation, R&D, and better financial management as necessary first steps.

Finally, the QDR stresses the need for the DoD to balance the responsibilities of maintaining effective force structure today, and transforming for the projected needs of tomorrow.⁴⁰

Congress was also moving into action before September 11, 2001. Delaware Senator Joseph R. Biden Jr., chairman of the Senate Foreign Relations Committee, held hearings on September 5, 2001 to get briefed on the results of “Dark Winter,” a

“war game” conducted by the government that simulated the release of smallpox into the air supply of several U.S. cities via terrorists. Former Georgia Senator Sam Nunn was one of the coordinators of the exercise. According to Nunn’s testimony:

In the simulation, about 3,000 people initially were infected because the vaccinations most Americans received as children had worn off. Every 10 days to two weeks, the number of people infected would increase tenfold . . . While health care workers and doctors were immunized immediately, on day six of the game, the United States had run out of vaccine. ⁴¹

Nunn continued with his testimony by stating that the nation is as equally unprepared for another biological attack with an agent like anthrax. Biden took this information to the nation in the days following the September 11, 2001 attack, vowing to work to change policies to secure against such an asymmetric disaster. ⁴²

Before the September 11 attack, the Senate Intelligence Committee approved authorization for \$30 billion in fiscal year 2002 for the various national intelligence agencies. The authorization provided an increased of more than \$1 billion from the request made by the Clinton White House. (Note that the current budget submission was from the final months of the Clinton Administration.) The increase, according to Committee Chairman Sen. Bob Graham of Florida, was much overdue and represents “the first installment of a multi-year effort to correct serious deficiencies that developed over the past decade. ⁴³ Graham would soon learn of the prophetic nature of his statement.

In congressional testimony the day after the attacks, General Myers stated that the defensive and emergency response mechanisms to a variety of asymmetric attacks was necessary in order to guard against the repeat of a similar, or somewhat different, kind of attack against U.S. interests. ⁴⁴ The implications of a more

widespread asymmetric attack are clear since it is possible that terrorists could be planning a more devastating WMD attack in the future.

Advocating a sizeable increase in the government's counterterrorism operations, Biden suggested that the government must act now to channel the necessary resources into defending against asymmetric threats so as to address the threat that "comes to this country in the hold of a ship, the belly of a plane, or smuggles into a city in the middle of the night in a vial in a backpack."⁴⁵

Now that it appears that the United States has been sensitized to the new realities of asymmetric warfare and domestic terrorism, it is important to consider the specific kinds of disasters that could befall the nation in the future. Section Two examines the specifics of such disaster scenarios, as well as specific policy proposals relating to how the U.S. can attempt to mitigate the effects of such aggression.

Section Two: Disaster Scenarios and Weapons That Create Them

The previous section spoke to the evolving attitudes of policymakers in the area of defensive posture to guard against an asymmetric attack. However, any changes to the way in which the United States protects its interests will have to address the reality of the growing spectrum of technologies and offensive weapons at the disposal of terrorist entities.

Specifically, this section will examine the panoply of biological, chemical, informational, and radiological weapons that pose the threat of asymmetric attack, as well as examine areas in the national infrastructure that are susceptible to attack via information warfare. The section will conclude with a broad consideration of specific ways in which the United States can effectuate policy changes to confront the specter of attack.

The Silent Terrors of the Asymmetric Threat

Overview of the Biological Weapons Threat

Biological weapons, as defined for the purposes of this thesis, are cultivated germs, fungi, and viruses that are manufactured for intentional release into air and/or water supplies in order to infect, infirm, and/or kill people within a specific period of time.¹

Confirmed Biological Weapons in 2001

Note that the germs listed below are the three biological weapons that intelligence sources estimate pose the most current hazard to U.S. citizens. There are some 40 biological weapons known to be cultivatable. The well-known pathogens are:

Smallpox: The germ kills up to one-third of persons infected. There is no cure for smallpox, only treatment via preliminary vaccination, or administration of the vaccine within seven days of known exposure. The vaccine is not available commercially to the general public. Regular vaccinations of the general public were discontinued in the 1972. Smallpox is communicable; however, reports are inconclusive as its communicability.

A November-December 2001 study by the Centers for Disease Control and Prevention (CDC) claims that speculation of a smallpox victim infecting at least ten others is an over calculation of the threat. The CDC estimates that the actual infection rate might be between zero and two persons per victim²

Anthrax: The germ kills 80% of those infected with the pulmonary form of the disease within five days of the onset of symptoms, although recent treatments of patients with pulmonary anthrax suggest this fatality rate may not be as high. Antibiotics, like Ciprofloxacin and doxycycline, can treat anthrax, but only if administered before the onset of acute symptoms. Dr. John Bartlett of Johns Hopkins reports that most medical professionals cannot distinguish an anthrax infection from the common flu.³ Unlike smallpox, anthrax is not communicable.⁴ However, it is the most stable of all the pathogens available for weaponization. This is because anthrax

can exist as durable endospores that are more resistant to dilution via air, sunlight, and/or chemicals.⁵

Ebola: The germ is part of the viral hemorrhagic fevers family and kills 90% of those infected within five days of infection via massive organ disintegration. Antibiotics, such as ribavirin, can successfully treat Ebola, but, as with anthrax, only during the preliminary hours of infection.⁶

Lesser-Known Pathogens:

Brucellosis: Onset of symptoms in 5-60 days, making detection of the origin of infection nearly impossible. Responds to aggressive, and timely, treatment with doxycycline.⁷

Q fever: Onset of symptoms in 10-40 days, creating a similar detection problem as with Brucellosis. Responds to aggressive antibiotic treatment.⁸

Plague: Has been in existence for centuries, and has caused mass casualties, especially in Europe. The onset of symptoms occurs in 2-3 days. It can be treated with Ciprofloxacin.⁹

Entities Suspected of Possessing Biological Weapons in 2001:

Russia: U.S. intelligence shows that the FSU was preparing to unleash biological weapons against U.S. domestic targets during the Cold War. Ken Alibek, a former official in the Soviet government charged with oversight of their biological weapons operation, suspects that Russia retains the old FSU manufacturing capability.¹⁰

Iraq: Richard Butler, the former head of United Nations Special Commission on Iraq (UNSCOM), urges the UN to resume independent verification of the imposed

restriction on Iraqi biological weapons manufacturing. Independent UN assessment was discontinued in December 1998 after Hussein forced UN weapons inspectors to leave Iraq. No verifiable estimate of Hussein's capability in this area exists, but Butler is adamant that Hussein has had plenty of time to rebuild any biological weapons manufacturing assets destroyed in allied air strikes since the final 1998 inspections.¹¹

Osama bin Laden: U.S. Intelligence suspects that bin Laden has the money to finance the manufacturing of biological weapons, and is posting germ-cultivating instructions to members of his worldwide terrorist network, including members in the United States, via uncrackable Internet encryption technology.¹² Former CIA intelligence chief John Gannon speculates that bin Laden may be working to acquire a biological weapon, if he hasn't done so already.¹³

Domestic Attack Scenarios with Biological Weapons:

Contamination of the air supply: The germs listed above are distributed in the air. They can be stored in aerosol spray containers and released at any time and at any location, although many scientists are on record disputing claims that dissemination is easy and claim that the hurdles to effective use of a biological agent are significant.¹⁴ Depending upon wind conditions, the communicability of the germ, and population movements, a single aerosol spray container can infect thousands.¹⁵

Contamination of medical facilities: Along with a biological weapons attack, it is possible that centers responsible for treating the infected will become targets of biological weapons, or other forms of terrorist activity, themselves. Terrorists might

target metropolitan medical centers with a germ agent before releasing the germ in the general population, thereby crippling our emergency response infrastructure.

Confusion of the government response: Today, there is no clear chain of departmental command to deal with the military, medical, and criminal fallout of a biological weapons attack. Departmental confusion could contribute to the chaos of an attack by adding confusion to relief efforts, perhaps preventing the timely administration of medical aid.¹⁶

Overview of the Chemical Weapons Threat

Known Chemical Weapons in 2001

Unlike biological weapons, chemical weapons have already seen verified use in both combat and terrorist situations. James Wirtz, an Associate Professor of National Security Affairs at the Naval Postgraduate School, has compiled a primer on the chemical weapons threat.

Chemical weapons use toxic agents to incapacitate or kill people. The technology needed to make such weapons is widely spread throughout the world because it is used in basic pharmaceutical and industrial production. Chemical weapons can differ in lethality, mode of action (how they enter the body), speed of action (the period between exposure and observed effect), persistency (the amount of time an agent remains dangerous once released into the environment), and state (solid, liquid, or gas).¹⁷

Wirtz breaks the chemical weapons family down into four groups.¹⁸

Choking Agents: These chemical weapons, such as chlorine gas, are known as choking agents because they infiltrate, impair, and destroy the respiratory system of the victim.

Blood Agents: These weapons, such as hydrogen cyanide, disrupt the body's normal use of oxygen, thereby affecting blood circulation, and, as a result, creating immense damage to bodily tissues and organs.

Blistering Agents: These agents, such as mustard gas, are designed to burn exposed mucous membranes and skin. Upon initial contact, these chemicals cause little physical discomfort, which makes their detection even more difficult.

"G-Series" Nerve Agents: Discovered by German scientists in the 1930s, these agents, including Taubun, sarin, and soman, stultify the functioning of the central nervous system, which results in fatal failure of the body's respiratory system.

Entities Suspected of Having Chemical Weapons in 2001

Since chemical weapons have had longer and more prominent exposure in the international community via open warfare, there is less uncertainty over which nations possess chemical weapons, and which are disposed to using them in the future.¹⁹

According to Wirtz, 123 nations have signed the Chemical Weapons Convention and pledged not to develop or use chemical weapons. Absent from this international pledge are:

Iraq: Hussein is suspected of using chemical weapons on U.S. troops during the Gulf War, and U.S. Intelligence and international observers, including Butler, remain convinced that Iraq is the holder of large stockpiles of chemical weapons.

North Korea: *The Washington Times* reports that Iraq, in an effort to raise funds, has shared some of its chemical weapons manufacturing information with North Korea. Given North Korea's instability, and its uncooperative spirit in

complying with international agreements on other asymmetric technologies, such as nuclear weapons, this is a potentially threatening development to U.S. national security.

Iran: Though a signatory of the Chemical Weapons Convention, the United States suspects that Iran is maintaining a large chemical weapons arsenal. Given Iran's history with the United States, it is likely that Iran might pose a significant asymmetric threat to U.S. interests in the future, perhaps even acting in tandem with one of the non-compliant nations noted previously.²⁰

Osama bin Laden: According to the *London Sunday Telegraph*, members of bin Laden's terrorist organization, al' Qaeda, planned to release sarin gas into the European Parliament building in Strasbourg, Germany during the parliament's February 2001 meeting. German police were able to foil this plot, but, the evidence points to a bin Laden organization with the intent, and, perhaps, growing capability, to implement an attack using chemical weapons.²¹

Note also that signatory nations to the Chemical Weapons Convention may be violating the convention standards, thereby increasing the states and entities on this list.

Domestic Attack Scenarios with Chemical Weapons

These scenarios are much like those discussed in the biological weapons section. Note, however, that chemical weapons are more likely not to be diluted by natural forces like temperature and/or sunlight. As well, chemical weapons usually focus on the body's central nervous system, while biological weapons attack areas like the blood stream and mucous membranes.²²

Unlike with biological weapons, there has actually been a chemical weapons attack on a civilian population center by a terrorist group. On March 20, 1995, the Japanese terrorist group Aum Shinrikyo released several containers of sarin gas into the Tokyo subway system. Twelve people died and thousands were treated for exposure.²³ Experts claim that thousands would have died as a result, had it not been for the inability of the terrorists to manufacture sarin in a purer form.

The world might have had its first taste of a biological weapons attack by the same terrorist group before the Tokyo attack. According to Wirtz, members of Aum Shinrikyo visited sites in Africa where the deadly Ebola germ had recently been located. The group hoped to harness Ebola for an attack against civilians in the future. According to published reports, its efforts were unsuccessful.²⁴

The Aum Shinrikyo incident is cited widely as an example of the kind of hurdles facing terrorists trying to use biological weapons for large scale attacks. The group had one billion dollars in assets, state of the art production facilities, hundreds of scientists and technicians, and almost a dozen attempts to disseminate biological agents against targets in Japan. The fact that the group was unsuccessful led them to resort to the easier, and more predictable, use of chemical weapons.²⁵

Nuclear Proliferation in 2001

Nuclear weapons are undoubtedly the best known of all the asymmetric weapons, although their usage cannot always be described as asymmetric. During the Cold War, for example, both the United States and the FSU viewed the other's nuclear capabilities as part of the overall conventional strategic threat to national security.²⁶ However, asymmetric concerns arise in relation to nuclear weapons when

they become portable – not attached to a long-range missile launched from halfway around the world, but, rather, driven into a tunnel or major city in the United States.

How nuclear weapons are manufactured is still unknown to many. Wirtz explains that:

Nuclear explosions are caused by uncontrolled nuclear fusion or uncontrolled nuclear fission. Fission occurs when high-explosive ‘lenses’ squeeze (implode) a subcritical mass of fissile material (e.g., plutonium), forcing the mass to become supercritical. . . . Fusion occurs when a fission device is used to fuse nuclei of light elements with each other to form heavier elements.²⁷

Though the manufacturing principles behind nuclear weapons are known widely, the availability of the manufacturing materials is not great due to international monitoring of the diversion of nuclear materials from reactors. Still, the number of nations boasting nuclear capability continues to grow, with India and Pakistan joining the ranks of the United States, United Kingdom, Israel, Russia, France, and China.²⁸

What is even more troubling from the asymmetric security perspective is the possibility that bin Laden has tried to acquire a nuclear weapon of some form.²⁹ These weapons could be in the form of a more traditional nuclear bomb, or a “dirty nuke,” a radiological device that gives off tremendous radiation without an explosion.³⁰

Interestingly, the three nations suspected of possessing the capability and intent to manufacture and use chemical weapons, Iraq, North Korea, and Iran, are also suspected of subverting international treaties governing nuclear weapon manufacturing. North Korea is the most suspect in this regard; it was found in violation of the Non-Proliferation Treaty that prohibits “non-nuclear states” from

manufacturing nuclear weapons. In this instance, North Korea was found diverting “weapon-usable” material from one of its nuclear reactors in 1994.³¹

Nations with the capability to manufacture nuclear weapons pose potential security threats not only in the conventional military sense, but also under the asymmetric paradigm. Though the technologies are hard for many nations to procure, it is possible to produce nuclear weapons that can fit into small containers, even suitcases.

Up to one hundred of these “suitcase” nuclear weapons, known as atomic demolition munitions (ADMs) have been reported as missing from the former Soviet Union since 1997.³² ADMs are one-kiloton nuclear bombs. There has been no verification concerning the confiscation of these ADMs by Russian authorities. If ADMs are on the market to be sold to the highest bidder, it changes the complexion of the asymmetric threat facing the United States.

If international terrorist actors, like Osama bin Laden, or domestic entities, like Timothy McVeigh and far-right wing militia groups, are able to tap such technologies, the potential for a catastrophic asymmetric attack, or even the blackmailing effect of the threat of such an attack, would increase exponentially.

Information Warfare in 2001

Imagine that you are stopping to buy gas during an important road trip, only to find that the pump will not recognize your credit card. Perplexed, you walk over to an ATM to retrieve cash for the transaction, only to find that your checking account, usually robust in balance, has suddenly been reduced to zero. Frustrated, you pull out your cell phone to call both the bank and the credit card company, only to find that all

cell phone transmissions are impossible to connect. Angry, you pull back onto the road, only to find chaos: all the traffic lights have stopped working, and the police are unable to direct the busy intersections.

The scenario just described is one of the many inconveniences that might lead to a national emergency as a result of information warfare. All of the problems listed above, from the credit and debit cards not working, to unresponsive cell phones, to inoperative traffic lights could all be products of cyber sabotage.

Obviously, computers oftentimes do not need man's assistance in malfunctioning; however, man has the ability, and, in the case of certain entities, the intent, to induce malfunctions of the computer systems that the United States has come to rely on to maintain its quality of life. By tilting a *Galaxy 6* communication systems satellite just a few degrees off its programmed orbit, perpetrators of cyber sabotage could bring the entire national infrastructure to its knees.³³

The damages from cyber warfare can be more long-term than problems with cell phones. Corporate financial statements could be altered. Military and other government assets could be stolen and/or tampered with, thereby risking the overall effectiveness of certain command and control operations. Viruses infecting millions of computers, already a somewhat common occurrence, could become far more prevalent. In addition, corporate espionage would be harder to detect and monitor, leading to severe ramifications in the economic sector.

Mary Langston, former deputy chief information officer for the Department of Defense is warning that the United States should be prepared for an “ ‘electronic Pearl Harbor’ ” in which e-commerce and communication is disabled. The timing of

such an attack would be in tandem with the impairing of the more traditional financial and commercial interests that occurred during the September 2001 attack on the World Trade Center.³⁴

Corroborating Langston's testimony was retired Air Force Lt. General Al Edmonds who testified before Congress on June 21, 2001 that such an information warfare attack "would be absolutely paralyzing" to the national infrastructure.³⁵

Who are the perpetrators of cyber sabotage? There is much conjecture, and few hard facts, to answer such a question. Rather than assign specific identities, as the suspected perpetrators could range from nations like China and Iraq, to international terrorists like bin Laden, to the congenial neighbor's boy, it is of greater importance to examine four primary modes of cyber sabotage, and the likelihood that the four are employed in asymmetric attacks against the United States. Michael Erbschloe, a leading technological consultant in the area of cyber warfare, describes these four areas as follows:

Offensive Ruinous Information Warfare: This kind of warfare is a calibrated military campaign to impair totally the target's military, technology, information, communication, economic, and transportation infrastructures.³⁶

Sustained Terrorist Information Warfare: Erbschloe defines this as,

The ongoing deliberate efforts of an organized political group against the military, industrial, and civilian and government economic information infrastructures or activities of a nation, region, organization of states, population, or corporate entity.³⁷

Sustained Rogue Information Warfare: This is the ongoing campaign by a

“nonpolitical, criminal, or mercenary” group to disrupt the operations of critical national infrastructures.³⁸

Amateur Rogue Information Warfare: This form of cyber warfare comes from attempts by “untrained and nonaligned individuals or small groups” to disrupt the operations of critical national infrastructures.³⁹

The likelihood that these forms of cyber (information) warfare will be employed depends on the cost of and resources available to implement them. Erbschloe suggests that few entities possess both the capability and intent to wage the offensive ruinous cyber warfare mentioned previously. Instead, entities are likely to make use of the latter three forms of cyber warfare.⁴⁰

Already, the highest levels of the national security infrastructure are feeling the effects of cyber warfare. On July 24, 2001, the *Associated Press* reported that the Pentagon was forced to “shut down public access to its Web sites” for fear that its computer networks might not be protected from the “Code Red” computer virus that was making its way around computer networks at that time.⁴¹

Yet the Pentagon’s worries over cyber warfare go back to the early 1990s, when it was discovered that hackers from a unknown point of origin have been infiltrating DoD and NASA computer networks while the government was powerless to stop the occurrence. The ongoing infiltration, codenamed “Moonlight Maze” by the Pentagon, is an astounding commentary on the vulnerability of even the government’s most sophisticated computer networks, let alone the millions of business and personal computers in use every day.⁴²

The Threat of Conflation

Considered separately, these asymmetric threats cause tremendous security concerns. When utilized in any variety of combinations, their potential lethality is multiplied immeasurably. Consider, for instance, the possibility that, even if the government were to establish the sort of response infrastructure necessary to treat infected citizens from an outbreak of Ebola, its efforts stand a good chance of being sabotaged by a concurrent information warfare attack against vulnerable emergency response computer systems.

Concomitantly, it is possible that combinations of biological and chemical weapons might be used during a particular attack, perhaps confusing authorities as to the proper method of treatment and/or quarantine of infected individuals, as well as the proper method of sanitizing infected buildings, subways, and the like. (Note that the treatments of biological and chemical weapons infections differ from a medical perspective.)

Also important to consider is the potential for blackmail that might occur if entities acquire the technology to manufacture portable nuclear weapons. In this instance, the public hysteria that would be created by threats of nuclear bomb detonation would, in many cases, be more disruptive to national security than the bomb blast itself.

In all these scenarios, the ability of the federal and state governments to “provide for the common defense” is in jeopardy.⁴³ There are potential public policy solutions to the quagmire of asymmetric threats, and they will be explored in the following section.

The Infrastructure Targets

The purpose of an asymmetric attack has been described as an effort to destroy the critical infrastructures that provide the nation with the basic life-sustaining services on which it has come to rely.⁴⁴ Chapter Three of McNair Paper 64, published by National Defense University, identifies these critical infrastructures and the ways that they may be susceptible to asymmetric attack using one or more of the weapons described in the previous section.

Transportation Infrastructure: consists of the many roads, highways, airways, waterways, mass transit systems, delivery systems, and pipelines that transport natural gas, petroleum, and other materials. Under efficient operation, the transportation infrastructure provides safe, effective, and reliable movements of people, goods, and services. However, an asymmetrical attack, using a portable nuclear device or other weapon, or utilizing information warfare technologies to disrupt computer operations, would bring this infrastructure to a standstill.⁴⁵

Oil and Gas Production and Storage Infrastructure: This infrastructure allows for the safe and efficient production, processing, and storage of natural gas, crude and refined petroleum, and other petroleum products. The effective operation of this infrastructure is designed to ensure that these substances do not intrude into the public domain. However, in the event of an asymmetrical attack, be it a bomb or some other form of physical sabotage, and/or information warfare to disable necessary control and production systems, the fuel materials kept away from civilian food and water supply areas for obvious health reasons, might be introduced into these areas.⁴⁶

Water Supply Infrastructure: This includes the various sources of water, including reservoirs, aqueducts, pipelines, and holding facilities that enable the nation's population to consume safe drinking water. A biological and/or chemical attack would contaminate this infrastructure, and would likely create massive civilian unrest and revolt.⁴⁷

Electrical Power Infrastructure: The generation stations and transmission networks responsible for providing the public with reliable electricity might be disrupted through a series of information warfare attacks. The government has done simulation tests on the ability of power grids to withstand an information warfare attack, and found that the power grids were susceptible to sabotage.⁴⁸

Defense Infrastructure: This includes the military units and installations to affect an attack, as well as the command and control centers to coordinate it. During effective operation, the defense infrastructure should be able to carry out its operations with minimal disruption. The inability of the defense structure to do this could be effectuated by an asymmetric attack using any number of available weapons and technologies.⁴⁹

An Asymmetric Tag Team

As alluded to above, while one of these asymmetric weapons would be devastating to the nation's political, military, and economic functionality, the pairing of two or more of these forms of attack would be especially lethal. Note that as destructive as the September 11, 2001 attack was against the United States, the entities involved did not employ any of the asymmetric weapons discussed in this section. As such, the potential impact of an asymmetric attack cannot be overstated.

This thesis posits that the two most consequential forms of asymmetric attack are biological weapons and information warfare. The broad national dependence on computer systems, as well as the insidious nature of biological weapons, makes them more problematic than the more immediate consequences of a chemical and/or nuclear weapons attack. Consider now the suggested realities and problems the country would have in defending against, and responding to, an attack against the mainland United States using biological weapons.

The National Response

There are a number of response scenarios possible in respect to the asymmetric threats discussed in this thesis. Consider the possibilities in relation to the government's response to a biological weapons attack.

The Clinton administration's "A National Security Strategy for a New Century," identified the delivery of biological weapons as something "We continue to work vigilantly" to prevent.⁵⁰ Assuming that a biological weapons attack were to penetrate national defenses, what would be the American response? Is America's national security apparatus presently suited to handle the fallout of an attack? Consider the following.

Military: It would be difficult for the military to wage a counter offensive in response to a biological weapons attack since it may be weeks or months before any parties claim responsibility, assuming responsibility is claimed at all. In addition, ambiguity in detecting the precise location of the perpetrators further complicates the military's mission. Questions over the accuracy and propriety of American military action will invariably arise.

Should the Air Force use precision-guided munitions to target what intelligence sources believe to be the hideouts of the suspected perpetrators? If so, is the United States prepared to respond to declarations of war from regional powers like Russia and China if both feel such retaliation by American military forces threatens their national security? What if intelligence points to American citizens as possible suspects in an attack? Are the U.S. armed forces truly prepared to turn their weapons against the American population, e.g., shooting down civilian airliners that stray off course?

Law Enforcement: Recall that the incubation period for the four “category A” biological germ agents listed earlier could last between one day and seven weeks. Assuming that an outbreak can be detected within five days of germ exposure, a generous estimate considering the possibility of a much longer incubation period, what kind of preserved crime scene will law enforcement agents have to investigate?

Should an attack like the one the Japanese terrorist group Aum Shinrikyo perpetrated in Tokyo subways in 1995 occur with aerosol-sprayed anthrax in New York City’s Pennsylvania Station, it could be weeks before any member of the law enforcement community suspects a crime has been committed.⁵¹ Needless to say, attempting to piece together evidence of a terrorist attack would be a daunting challenge for law enforcement agencies.

Exacerbating law enforcement’s frustrations in the event of an attack is the need to control the movement of those exposed to the released agents, particularly in the case of communicable agents. Undoubtedly, persons suspected of infection would have to be quarantined. Yet such action raises questions of civil liberty infringement

and would face certain court challenges from the American Civil Liberties Union.⁵² In addition, it is not at all certain that the government's response to an attack would be well coordinated between the responding agencies, making a quarantine action even less effective.

In the event of an attack on U.S. interests, Title 10 of the United States Code gives the President the authority "to mobilize the Department of Defense to respond."⁵³ The last time a President sent military forces into a domestic crisis was 1992, when President Bush authorized Army and Marine forces to help quell the Los Angeles riots that followed the Rodney King verdict.⁵⁴

Yet the combined effort of the Los Angeles Police, National Guard, and regular military personnel only added to the hysteria of the situation, since there was not a clear chain of command, or organized effort, between the agencies.⁵⁵ In the event of a large-scale biological attack today (anthrax-laced letters do not qualify in this regard), it is not clear what government agency would assume lead responsibility for relief and enforcement efforts.

The newly formed White House Office of Homeland Security, and its Director, Tom Ridge, is making progress on the coordination front. Coordination with the 46 responding federal agencies, as well as regular conference calls with state and local health and law enforcement officials, are promising steps in better federal coordination.

Medical Response: The Centers for Disease Control and Prevention estimate that the national stockpile of smallpox vaccine is between 7.5 and 15.4 million doses.⁵⁶ Scientists and doctors believe this figure would not be adequate should a

large scale biological attack occur. Recall that successful treatment of anthrax, plague, and hemorrhagic fevers depend solely on the timely administration of antibiotics.⁵⁷ The availability of antibiotics will probably not be a challenge; rather, the true test is whether hospitals responding to the victims of a biological weapons attack would have timely access to such medical resources.

As with military and civilian law enforcement, the medical community faces a variety of daunting challenges. The lack of wider awareness of the biological weapons threat has been a growing concern of some in the medical profession. In the last two years, a study conducted by Dr. John Bartlett has been a catalyst for uneasiness.

On February 13, 1999, Bartlett, head of the Division of Infectious Diseases at Johns Hopkins University School of Medicine, conducted an experiment in which he observed his nurses, doctors, and other medical personnel continuously misdiagnose classic cases of inhalational anthrax.⁵⁸

Convinced that the staff of Johns Hopkins University hospital was oblivious to the symptoms of biological germ contamination, Bartlett decided to see how fast the government would respond to a doctor suspecting that a biological weapons attack had occurred. Bartlett contacted the Maryland Department of Health about a possible biological weapons outbreak. The department returned his call three days later.⁵⁹

Evidence suggests that the anthrax letter scares of October 2001 have galvanized health professionals and responding agencies in ways lectures and seminars could not.

Yet even if hospital personnel were able to accurately identify symptoms of biological contamination, Bartlett is concerned about the ability of the nation's

national health care system to provide adequate and timely treatment. On the day of Bartlett's experiment, Johns Hopkins was experiencing a routine influx in the number of flu patients admitted for care. The flu sufferers had put Johns Hopkins on "blue alert," meaning that all emergency room staff and resources were being fully utilized.⁶⁰

Had there actually been a biological weapons attack, Bartlett is convinced that Johns Hopkins, a premiere medical facility in the state of Maryland, could not accommodate the crisis.⁶¹ The ability of other facilities to handle an influx of patients suffering from a biological weapons attack is yet unknown, since few communities have done an assessment of their capability in responding to such a situation.

Michael Osterholm, a leading epidemiologist from the University of Minnesota, and Bartlett concur that a change in approach to the biological weapons threat is necessary if the United States is to be able to respond effectively to an attack. The same holds true for the other forms of asymmetric threats: policy changes, utilizing existing infrastructure and implementing new procedures, is the way toward securing the nation from the devastation of future terrorist aggression. There are specific policy changes that the government can implement to guard against an attack using any of the five WMDs discussed.

For the nuclear and radiological threats, heightened security, international pressure on nations and entities suspected of shipping uranium, and increased security and checkpoint procedures at U.S. points of entry are valuable policies. For biological and chemical weapons, international pressure on entities known or suspected of creating these weapons to desist from their manufacturing and/or submit to U.N.

inspection, improved government health care response capability (explored in Section Four), and tighter domestic security are all helpful. For information warfare, upgrading computer hardware, creating back-up networks, and hiring more technology savvy staff to protect vital software files are all important changes.

However, there is one set of policy changes that transcends the rest.

The Path Toward More Effective Protection

A recent presentation made by former State Department Ambassador-at-Large for Counterterrorism, L. Paul Bremer, suggests that there exist fixes that can be implemented in the short term to bring about enhanced national security. In a lecture delivered to the Heritage Foundation on July 31, 2000, Bremer outlined necessary steps to combat domestic terrorism.

In his view, the best source for providing a competent national security policy against a terrorist scenario is superior intelligence gathering, processing, interpretation, dissemination, and adjudication of gathered data. In Bremer's view, problems arise because, in many instances, bureaucratic and procedural obstacles impede the channeling of pertinent information into the appropriate hands.

Bremer recommends fixing this information blockage through establishing inter-agency assimilation procedures whereby information sharing can be easily accommodated. Such changes would require greater budgetary resources, as well as a clear set of objectives and consistent leadership for the intelligence community.

Information from the Defense Advanced Research Projects Agency, released January 7, 2001, concurs with Bremer: good intelligence is the best resource not only

to portend the potentiality of an attack, but also to detect the perpetrators of terrorist aggression.⁶²

In the final analysis, it is the nature of the threat that must guide the tenor of the preparation. In Federalist Paper 41, James Madison argued, "The means of security can only be regulated by the means and danger of attack."⁶³ This section has documented that certain entities have at their disposal the capability and intent to threaten many lives. Therefore, from all outward indications, even assuming that a devastating WMD attack is not in the immediate future, policy changes to empower the timely and effective government planning are now due.

At stake in the year 2001 is more than just the initial disruptions incurred after a terrorist attack. Today, a nation's national security is no longer defined simply in terms of how secure its shores are from conventional military or terrorist aggression. Recent decades have shown that a nation's long-term economic health has become inextricably linked to the ability of that nation to facilitate a secure and stable economic system. The attacks of September 11, 2001 have certainly had an impact on the economic side especially; future attacks might erode the other areas.

As well, the political health of a nation is dependent upon the surety of its ability to exercise sovereignty in its established sphere of influence. Losing such a governing prerogative via a destabilizing terrorist catastrophe could place a nation's military and economic communities in positions of inappropriate power and responsibility, resulting perhaps in government overthrows, and followed by anarchy or tyranny.

Like concentric circles mutually sustaining the integrity of each other, a nation's economic and political organs are the direct beneficiaries of an adroitly calibrated defense apparatus. Madison's sentiments, especially in light of September 11, 2001, are more incisive today than ever.

This thesis posits that Bremer's statement about good intelligence being the best defense against asymmetric attack is profound. It will turn now to a fuller consideration of the U.S. Intelligence Community (IC) in Section Three.

Section Three: Intelligence And A Safer Nation

Almost immediately after the attacks on September 11, 2001, politicians, policymakers, and analysts identified problems in the U.S. IC as the primary reason for the attacks going undetected. Since intelligence is the only way to gain some appreciation for the general picture of a terrorist operation, it is imperative to study the nature of intelligence, the role it plays in national security, and the new changes that must occur to make intelligence the kind of asset on which the defense and law enforcements communities can count.

This thesis argues that, by considering the national defense readiness against asymmetric attacks from a proactive posture, policymakers would be given the ability to use existing resources to address asymmetric threats, and at less human and financial cost. In other words, instead of focusing on how to clean up the disaster once it occurs, which is the only reaction possible after an attack like the one in New York City, existing government resources should be focused in specific ways to try and keep an asymmetric attack from happening in the first place. In other words, more proactive responses should be undertaken; the resources for this are found in the IC.

This thesis views the capability of U.S. intelligence agencies to intercept information regarding plots by foreign and/or domestic entities to perpetrate asymmetric attacks as the best defensive and offensive assets in the national security

arsenal. Yet the intelligence process must become far more capable to pinpointing with greater clarity the threats that exist.

For instance, in June 2001, the United States Armed Forces in the Persian Gulf, went on heightened alert because U.S. intelligence intercepted messages between operatives in Osama bin Laden's terrorist organization that detailed plans for attack against American interests in the region.¹ While the military began to hunker down, the citizens on the U.S. mainland hardly noticed the reports coming from the Middle East.

Though recent reports suggest that U.S. intelligence picked up on some of the movements of the hijackers involved in the September 2001 attacks, intelligence was unable to predict the disaster. Thus, while a small war in terrorism was won in regard to the security of the military overseas, a major battle was lost in the form of thousands of dead civilians.

However, there is still no better way to protect against an asymmetric attack than good intelligence reported in a timely fashion. This information, drawn from a variety of sources, and analyzed by people trained in the specifics of geopolitical, ideological, and regional issues, may play the pivotal role in how prepared the United States will be in its response to terrorism, and, in specific, future asymmetric threats.² Indeed, the timely and accurate report from intelligence agencies, delivered to the right policy makers in enough time, can make the difference between a nation that is poised to defend itself against specific threats, and even prepared to launch preemptive action to prevent attack, and a nation that is caught off guard completely, suffering great human, financial, and strategic losses as a result.

Sun-Tzu recognized that the most effective way to prepare against the machinations of the enemy was to obtain precious insight brought about by foreknowledge. He identified foreknowledge as “the reason the enlightened prince and the wise general conquer the enemy whenever they move.”³ Thus, quality intelligence seems to be the time-honored method of establishing a sound security policy.

With regard to the United States Intelligence Community, it is important to discuss both the history of the IC, as well as the major agencies and policymakers that run it, for only a rather comprehensive study of the community as a whole will bring the necessary breadth of understanding about the complexity of intelligence issues in 2001.

The History of U.S. Intelligence

U.S. intelligence operations can be traced back to Benjamin Franklin, who, while negotiating with France for economic and military aid, established a cadre of agents in London to monitor the activities of the British.⁴

Nineteenth century America saw no deviation from the use of intelligence: James Madison employed intelligence operations in order to frustrate the British in the War of 1812.⁵ The Civil War found both the North and the South using intelligence to further their campaigns, though the latter made much greater use of its intelligence operation.⁶ By the closing decades of the century, the two established military departments erected permanent intelligence units: the navy began its intelligence collection in 1882, designed specifically to focus on the shipbuilding

methods employed by other nations. The army followed with its intelligence division in 1885.⁷

The breakthrough for U.S. intelligence came with the introduction of cryptanalysis (code breaking) during World War I. Yet while the advent of cryptanalysis was an important technological step, policy makers were not yet willing to employ this capability in a peacetime context. During the Hoover administration, code interception and breaking became prohibited.⁸

This policy was reversed during the years immediately preceding America's entry into World War II, which saw significant development in American cryptanalysis. According to journalist Pat Holt, despite the development of American intelligence capabilities, the government was not adroit at distributing the information to the necessary decisions makers in the required amount of time. This communicatory difficulty, in Holt's estimation, contributed to the success of the Japanese at Pearl Harbor.⁹

As German espionage and the greater use of message encryption became prevalent in the 1930s, political pressure mounted for more resources to develop a quality U.S. intelligence operation. During World War II, various agencies attempted to work in tandem to produce a competent intelligence product. The different requirements for successful overt and covert operations necessitated the establishment of separate agencies. The Office of Strategic Services (OSS) was created to handle the covert side of the intelligence community, and was the precursor to the CIA.¹⁰

Bureaucratic jealousies between the agencies prevented full cooperation, a reality not different from the present. At the close of the war, with the growing need

to develop a precise set of strictures for U.S. intelligence operations, President Truman and Congress enacted the National Security Act of 1947.¹¹ The growing role of the United States as the international equalizer to Communist expansionism created a perceived need for a permanent intelligence apparatus. A sustained U.S. diplomatic and military presence was becoming more important to the world community, and good intelligence, proven indispensable in the war against Germany and Japan, was vital. Although covert action was originally discontinued because Truman saw little need for it immediately after World War II, covert operations were soon reinstated.

The National Security Act of 1947

The National Security Act of 1947 laid the groundwork for the contemporary infrastructure of the intelligence community. The act established the Central Intelligence Agency (CIA), the National Military Establishment (renamed the Department of Defense, DoD), the Joint Chiefs of Staff, and the United States Air Force.¹² The newly created agencies and departments were given charge over the collection, analysis, and production of both tactical and strategic intelligence. (The former refers primarily to military intelligence, the latter to other forms, including counterintelligence and covert operations.)

The U.S. Intelligence Community in 2001-2002 is in fact almost the same intelligence structure that was established in 1947. Created originally to monitor the actions of the former Soviet Union (FSU), the intelligence community of today is still based on the construct of post-World War II threat assessment. Even the post-Cold War military doctrine of preparedness to fight and win two major regional

contingencies (MRCs) continues to frame security challenges in conventional, or symmetric, terms. U.S. intelligence is invariably influenced by the type of threat assessment the greater defense community adopts, thereby making it difficult to examine potential threats not considered germane to the general national security posture.

Interestingly, the intelligence community began to assess the specifics of the asymmetric threat in the mid 1990s, despite the fact that the prevailing view of national security threats remained codified in the symmetrical, or conventional, defense policy lexicon.¹³ Recall that a “threat” to national security is defined as one entity having the capability and the intent to perpetrate harm against U.S. interests, be they foreign or domestic.

The issue before the intelligence community today deals specifically with how it collects data on suspected asymmetric warfare perpetrators even as the defense community at large has yet to prove willing to put more emphasis on combating the asymmetric threat. The 2001 QDR’s threat assessment shift to a capabilities-based strategy is a departure from previous threat-based assessment, and should enable the IC to produce better intelligence products.

Despite predictions, the 1990s was not the decade that ushered in the stability of a New World Order. In fact, even though the 1990s saw a decline in defense spending worldwide (precipitated by the disintegration of the Soviet Union and the subsequent reduction in U.S. defense spending), the spending reduction, in the estimation of Vice Admiral and Defense Intelligence Agency Director Thomas Wilson, has motivated entities contemplating aggression against the United States to

consider cheaper, less administratively burdening, asymmetric options in exercising their aggression.¹⁴

Wilson views the growing economic interdependence of the world community as a catalyst for aggression against the United States. In his estimation, the propagation of American values, culture, and institutional norms to Eastern (especially Muslim) cultures, has ignited efforts by some in Muslim societies to undo the influence of the United States. Economic protectionism is becoming a technological impossibility. Hence, U.S. commercial, military, and transportation centers become the prime targets.¹⁵

Furthermore, Wilson views the relative strength of U.S. values, economic principles, technological development, and educational institutions as creating a resolve on the part of U.S. adversaries to employ asymmetric tactics to frustrate the continued U.S. dominance of these spheres. In the new century, the United States faces threats presented by domestic terrorism, missile proliferation, WMD proliferation, and Cover, Concealment, Camouflage, Denial, and Deception (C3D2) – an activity designed to impair U.S. intelligence efforts to monitor, and frustrate, the mobilization and attack preparation activities of terrorist entities.¹⁶

While the United States is no stranger to terrorism, especially terrorism based on ethnically, regionally, and/or religiously imbedded motives, the paradigm by which the world community operates has changed dramatically; the United States is no longer playing a tug of war with an equal power. During the Cold War, regional conflagrations, though existent, were subordinated by the overarching bi-polar dynamic of the superpower standoff.¹⁷ Many of the same entities that are now

identified as having the capability and intent to perpetrate harm against the United States were client states of the FSU. Today, these former clients are left unconstrained by the absence of the FSU.

The test for the United States Intelligence Community rests in how effective it will be at shifting from its seminal focus on the activities of one superpower to a sustained concentration on the activities of a variety of threatening entities, both of the national and inter-national variety. The success of U.S. intelligence in this endeavor depends directly on how well and how quickly the community's infrastructure, established in great part by an act of Congress fifty-four years ago, can adapt.

In the following chapter, this thesis will consider specific changes that need to be undertaken by U.S. intelligence in order to function effectively in the asymmetric threat environment. Before broaching that discussion, this chapter will delineate the basic structure of the intelligence community. The intelligence community is divided into three general categories: the Director of Central Intelligence and his supporting organizations, the Department of Defense and its intelligence agencies, and intelligence agencies that fall under the jurisdiction of other departments.

Central Intelligence Agency and the Director of Central Intelligence

Probably best known of all the intelligence agencies is the Central Intelligence Agency (CIA). Officially, the CIA was created to coordinate and supervise the collection, analysis, and dissemination of intelligence to policymakers. The Director of Central Intelligence (DCI) runs the CIA. (The DCI is also the statutory head of the

intelligence community (IC), reporting directly to the President on intelligence operations.

The Intelligence Authorization Act for 1993 vested in the DCI the authority to establish collection requirements and priorities.¹⁸ Since it is the coordinating agency responsible for the intelligence products put forth by the IC, the CIA maintains several interdisciplinary centers that address areas of security concern. Some of these centers oversee activities like nonproliferation, counterterrorism, and counterintelligence. All three are crucial in addressing asymmetric threats.

The agency's areas of specialty are covert intelligence and counterintelligence. Since it is responsible for the operation of all non-military intelligence operations overseas, the CIA maintains a presence in the military commands. Its position as the preeminent intelligence agency requires it to establish collaborative relationships with the rest of the IC. These relationships enable the CIA to coordinate the analytical effort of the community, which in turn enables the community to achieve effective coverage of key topics of interest to both intelligence agencies and policymakers.¹⁹

Community Management Staff

The Community Management Staff exists to assist the DCI in the management of the IC. Part of the responsibility of management entails selecting those entities that will serve as collection targets; the management staff works with the DCI in this regard.²⁰

National Intelligence Council

The National Intelligence Council is another administrative structure that the DCI has at his disposal. Specifically, the council members are each responsible for specific operational functions within the IC. The council is also concerned with the state of community cooperation, especially in regard to how the agencies collaborate on the creation of the National Intelligence Estimates.²¹

Department of Defense

As mentioned previously, the Navy and Army established their own intelligence divisions in the late nineteenth century. With the addition of the Marines and the Air Force, the DoD has added two more intelligence divisions; it also has under its jurisdiction the following agencies.

Defense Intelligence Agency

The Defense Intelligence Agency (DIA) was established in 1961 to function as the senior coordinating component for military (tactical) intelligence. Important areas of emphasis for the DIA include targeting and battle damage assessment, weapons proliferation, and collection on foreign military organizations. Though an agency within the DoD, the DIA staff includes both military and civilian personnel, with most members working at the Defense Intelligence Analysis Center at Bolling Air Force Base in Washington, DC.²²

National Security Agency

The National Security Agency (NSA) was established in 1952 in order to coordinate foreign signals intelligence. (Signals intelligence will be explored further

in the next chapter. It deals mainly with the interception of electronic emissions, which may be in the form of voice, code, radio transmissions, and/or radar signals.) The NSA is the largest of the thirteen intelligence agencies, employing approximately 30,000 military and civilian personnel, and operating with an annual budget of approximately \$4 billion. It is located at Fort Meade, Maryland.²³

National Imagery and Mapping Agency

NIMA came into existence in 1996 as part of an effort to merge the previously separate disciplines of imagery and mapping. The information provided by the agency allows intelligence users to receive necessary awareness of their operational space in a given mission. To that end, NIMA works to provide users with timely access to all available imagery intelligence, with the intent of fostering a greater level of integration of intelligence products in the future.²⁴

National Reconnaissance Office

The NRO is charged with the research, development, acquisition, and operation of the technologies necessary to operate the space-borne monitoring of areas of collection interests, including the monitoring of military exercises, assessment of natural disasters and other environmental concerns, and warning and indication of enemy attack via conventional and/or nuclear assets. The NRO was established in 1960, but the government did not acknowledge its existence publicly until 1992.²⁵ CIA and DoD personnel staff the NRO.²⁶

Department Intelligence Elements (Non-DoD)

In order to carry out their administrative functions, the Departments of State, Energy, Treasury, and Justice (through the FBI) all have intelligence divisions.²⁷ The

work performed by these divisions is tailored to the specific functions of the departments. For instance, since the FBI is the primary agency charged with the operation of counterintelligence, the FBI's intelligence division is geared almost exclusively to counterintelligence operations.²⁸

Intelligence Disciplines

This section examines three general types of intelligence data: Technical Intelligence (TECHINT), including Open Source Intelligence (OSINT), Human Intelligence (HUMINT), and Counterintelligence (CI), and discusses the collection and processing phases.

Technical Intelligence is a conglomerate heading that includes forms of intelligence data whose collection is dependent upon some form of technical device, be it a communications network, photographic lens, and/or satellite image.²⁹ Some forms of TECHINT date back to the Civil War, when Photographic Intelligence (PHOTOINT) was used to detect troop movements via vantage points from hot air balloons.³⁰

Other forms of TECHINT are rather new, as is the case with fiber optic transmission technologies that allow spies to send information undetected through sophisticated encryption devices.³¹ Still other forms of intelligence have been used for decades, but technology has made their usage more efficient in recent years. This is true especially in regard to satellite imagery that can now be transmitted to intelligence analysts in "real time," as opposed to the three-week lag period that once impaired a satellite's utility.³²

Less sophisticated technically is the collection discipline of Open-Source Intelligence. Unlikely material for spy novels, OSINT entails the monitoring of openly accessible information sources on a particular subject. Such open sources include newspapers, personal conversations, radio and television programs, and, especially within the last decade, Internet resources. Though OSINT is not well recognized by the general public as a vital form of intelligence collection, 75 to 90 percent of all intelligence is collected using OSINT sources.³³ Technological advancements continue to impel improvements in collection methods. Long gone are the days when spies had to use heavy photographic equipment in hot air balloons to get information on troop movements.

Human Intelligence is the collection of intelligence data from human sources, although some technical devices, i.e. wiretaps, may be employed in the process.³⁴ A majority of HUMINT is collected via OSINT, which is overt. This form of intelligence might be derived from bartenders and barbers – people who are likely to share information about events and gossip. HUMINT is also a product of clandestine operations. This kind of intelligence has been getting a great deal of attention from policymakers because of its usefulness in penetrating terrorist cells.

The DIA supervises the Defense HUMINT Service (DHS), which is comprised of the attaché services of the Army, Navy, and Air Force, and is responsible for the collection of clandestine intelligence in selected areas and situations.³⁵ All such collection is done in foreign environments; federal law prohibits the collection of intelligence against American citizens living in the United States.³⁶

The collection of HUMINT is performed through intelligence officers, referred to usually as agents. Agents may be American citizens under the direct employment of the CIA (in which case they are career employees), or they may be foreign citizens who report to CIA case officers stationed overseas. These case officers are responsible for remunerating the agents for their work, as well as assessing the value and credibility of the intelligence the agent has furnished.

These foreign agents are, for all intents and purposes, spies for the United States, and put themselves at great risk to collect HUMINT data. Recruiting these agents is often difficult, and depends on the ability of the case officer handling the HUMINT collection in a given area to recognize, recruit, and retain the kind of agents who will prove capable and loyal.³⁷

HUMINT is also the intelligence discipline that executes the greatest amount of covert action. (Covert action refers to secret actions a state undertakes to carry out some aspect of a security policy.)³⁸ The 1970s was an especially difficult period for HUMINT, as the Church and Pike Committees (named after members of Congress) questioned the propriety of the CIA's involvement in the assassination plots against Cuban leader Fidel Castro, and Chilean President Salvador Allende.³⁹

President Carter, hoping to establish closer oversight of the IC, issued Executive Order 12036. The order created two new NSC committees; one would monitor the activities of covert intelligence, the other would observe the IC in general. Another corollary of the order was the National Intelligence Tasking Center, which helped set collection priorities. The oversight by Carter and his DCI, Stansfield Turner, marked a new era of close scrutiny of the IC. The scrutiny may have

weakened the community's ability to collect enough intelligence to predict seminal events like the attack on the American embassy in Iran in 1979.⁴⁰

Counterintelligence refers to efforts to keep entities from collecting intelligence against a nation's interests and institutions.⁴¹ CI is also a form of intelligence monitoring that provides information on the intentions and activities of entities seeking to obtain information about the United States. This is vital work in the wake of September 2001 terrorist attacks, and the threat of continued terrorist activity within the United States.

The FBI is responsible for overseeing CI operations in the United States; the CIA performs the same function for U.S. institutions overseas; however, as was seen with the investigation of the terrorist bombing of the USS Cole in October of 2000, and the World Trade Center and Pentagon attacks of September 2001, the international scope of intelligence and terrorist action requires a blurring of the jurisdictional line somewhat.

CI has made the news recently with the arrest of former FBI agent Robert Hannsen. Hannsen was actually working a CI assignment at the FBI while furnishing intelligence to Russian authorities. Both the CIA and FBI have begun to collaborate with greater regularity in the aftermath of both the Hannsen and Aldrich Ames (a former CIA agent) spy cases in order to preserve the effectiveness of CI.⁴²

With the three major intelligence disciplines delineated, this thesis now turns to the processes by which these forms of intelligence, once collected, are processed (or analyzed), and then disseminated to the proper officials.

Collection and Processing

The collection of intelligence is performed through one or more of the three disciplines. In most cases, even with HUMINT and CI, some form of technology is used to facilitate the collection process. Innovations in technology have meant clearer, faster, and more reliable intelligence, which has enabled the United States to realize increasingly effective intelligence operations. Yet while collection technology continues to improve, it has not kept pace with the rapier-quick innovations in the private sector.

This is not to suggest that the technology used to collect intelligence is obsolete; however, because of the increased vulnerability of national cyber infrastructure to sabotage, the IC needs to appreciate fully the hardware, software, and attack methods that might be used in cyber space.

James Adams, a member of the NSA Advisory Board, laments that government directives do not drive current technological developments as they did during the Cold War. Instead, the interests of private industry are the catalyst for continued advancement. This ostracizes decision makers in Washington from much of the breadth of knowledge necessary to make sound judgment on procuring new technologies that will allow intelligence services the capability to provide timely and accurate analysis of technological threats to national security, especially in the form of cyber warfare.⁴³

During the Cold War, the United States was funding approximately 70 percent of the development costs for new technology.⁴⁴ That kind of investment enabled the government to remain engaged in the changing technological landscape: anticipating

challenges presented by the new technologies, and, at the same time, benefiting from a more intimate knowledge of those technologies, and how to counter them if necessary.

However, with the collapse of the FSU, and the end of the exigent funding initiatives that went with it, government investment in technological development has declined drastically. Another barrier to greater government collaboration in technological advancement is its slow procurement schedule. Put simply, private interests move much faster than government planning.⁴⁵ Thus, the profit motive that drives current technological advances does so with little collaboration with the government.

Concomitantly, the burst of personal computer ownership among U.S. citizens, as well as ever-increasing business sector reliance on computer networks, creates an easy target for cyber sabotage. Intelligence collection on an entity's intent to use cyber warfare to damage U.S. military and commercial interests requires IC collection priorities that emphasize ascertaining the dimensions of the actual threat posed, warning signs of an attack, speculation of the identity of the perpetrators, and contingency plans available to prevent, or mitigate, the attack. These ends can only be achieved if the government is more involved in the process of technological development and procurement.

Remedying the government's minimal level of input in technological development does not necessarily mean a return to previous levels of government funding of technological initiatives. Rather, a concerted effort at better communication on the part of private developers and the government will do much to

keep the government abreast of the newest technological initiatives, while allowing private sector technologies the latitude to develop at a free market pace.⁴⁶

Collection problems also exist with HUMINT and CI. With regard to the former, Arthur Hulnick, former Chairman of the DCI's Management Advisory Group, comments that finding, recruiting, and retaining qualified and loyal HUMINT personnel has always been challenging. The post-Cold War budget cuts for intelligence operations, which have led to personnel layoffs, have only exacerbated the difficulty, especially when considering that former agents might seek revenge against the agency for their termination.⁴⁷

This revenge would likely manifest in the form of the former agent selling information about U.S. intelligence procedures to foreign intelligence organizations, thus compromising the continued capability of the clandestine U.S. intelligence infrastructure. Hulnick further comments that morale among current CIA employees is low as a result of the budget cuts.⁴⁸

CI has been in the news recently because of the discovery of moles in both the ranks of the FBI and CIA. Holt comments that the CIA was slow in moving to remove its agent Aldrich Ames, head of the CIA's Soviet CI division, from the field after beginning to suspect Ames' involvement in the disappearance of CIA agents within the KGB in the mid 1980s.⁴⁹ The loss of the clandestine HUMINT presence within the KGB was an impediment to intelligence collection. Despite Ames' lavish spending sprees, as well as CIA suspicion that Ames received payment from the Russians, the CIA did not restrict Ames' access to sensitive agency documents, even allowing Ames to remove those documents from agency headquarters in Virginia.⁵⁰

On February 18, 2001, the FBI arrested Richard Hanssen, its agent in charge of counterintelligence for Russian interests in New York City. The bureau believes that Hanssen furnished his Russian handlers with information concerning the identity of U.S. spies in Russia, as well as sophisticated information software technology used by U.S. intelligence agencies.

The FBI now suspects that Russia has since given this software technology to suspected terrorist Osama bin Laden, possibly allowing him to monitor efforts to track his activities.⁵¹ Hanssen's actions probably impair intelligence collection efforts in at least two ways: first, those U.S. agents working in Russia have now had their identities compromised, and are likely dead, or at least unable to continue with their collection tasks. Second, bin Laden's ability to anticipate intelligence collection against his positions will enable him to obfuscate his activities even more successfully than in the past.

Remedying the current problems with HUMINT and CI collection, as well as preventing new ones, requires more than larger budget allocations to boost morale, or better investigational procedures in the wake of suspicious activity by an agent, though both initiatives would improve intelligence collection. Hulnick cites the option of giving the DCI more budgetary and administrative control over the operations of the member agencies of the IC.

Currently, the DoD controls roughly 90 percent of the overall intelligence budget, thus minimizing the DCI's influence.⁵² Transferring greater budgetary control to the DCI might encourage greater collaboration between the intelligence agencies.

Better collaboration is necessary, especially considering the pervasive nature of asymmetric threats.

The DCI, the IC at large, and the Congress, which appropriates funding for the intelligence agencies, will want to consider other challenges facing U.S. intelligence operations, particularly as they relate to the processing and dissemination of collected data.

The sophisticated technologies employed in intelligence collection enable the agencies to collect substantial amounts of raw data, and then to analyze that data in preparation for dissemination to the proper officials for decision-making purposes. Note that however capable these technologies are, the raw data they collect is useless unless it is put through the processing phase and then passed along to the proper authorities. Hulnick considers the inability of the intelligence agencies to process and disseminate the prodigious amount of data generated by current technologies to be a daunting challenge for U.S. intelligence.⁵³

Part of the reason for the lack of available resources for intelligence processing is that, given the limited resources available for the intelligence operations, and given the billions of dollars in cost to procure, operate, and maintain the TECHINT systems, not enough is left to fund the processing activities.⁵⁴ The necessary personnel are not available to make proper sense of the data once it is collected. This results in a greater lag time between the collection of data and its employment in furnishing the government with information on a variety of subjects, including national security threats.

Another aspect of the processing dilemma refers back to the lack of cooperation between the agencies as it is related to collection. The lack of cooperation also affects processing, making it hard for employees from one agency to gain access to data held by another, even if that data would prove crucial in the processing of important collected material.⁵⁵

As with collection, funding for more personnel to analyze the collected intelligence data would be useful, but it would only be half the answer. A shared agenda and vision between agencies is the other half of the equation. Yet neither seems easy to effectuate. It is more attractive for members of Congress to appropriate money for conventional technology procurement, since that means government contracts with manufacturing firms in congressional districts, than it is to hire more unidentified personnel to work in an undisclosed location performing classified research for the federal government.

At the same time, the various agencies charged with specific operational tasks, though unified by their general responsibility for U.S. intelligence, view each other as competitors for budget appropriations, prestige, and authority.⁵⁶ Until a more intrinsic sense of cooperation is established between the agencies of the IC, it is unlikely that significant improvement on these matters will occur.

This issue parlays into a discussion of the relationship between the intelligence community and the political institutions that have charge over it: the Executive and Legislative branches of the federal government. Consideration of these branches leads to consideration of the judiciary and the media, and all four will be assessed in terms of their relation to intelligence activities.

Intelligence and Oversight

The Executive

The Constitution vests the president with the power of administration over all activities of the United States government. With such a large governing apparatus to supervise, the president has at his disposal personnel who are charged with the daily administration of the various departments, agencies, and bureaus. The intelligence community is no different. The IC is headed by the DCI, with senior intelligence officials comprising the Community Management Staff and the National Intelligence Council to help the DCI establish budgetary and collection priorities.⁵⁷

During the Cold War, the president drew upon the expertise of a cadre of advisors possessing experience in foreign policy, technology, and related issues. President Eisenhower established the President's Foreign Intelligence Advisory Board (PFIAB) via Executive Order 10656 in 1956. Over its lifespan, the PFIAB provided the president with assistance on topics ranging from U-2 reconnaissance flights, to procedural issues.⁵⁸ The Intelligence Oversight Council (IOC), established in 1976, served as a processing center for reports between the president and the inspectors general of the intelligence agencies.⁵⁹

The relationship between the president and the IC has varied depending upon the president's priorities for the community, with some taking greater steps to direct the functioning of the community. Presidents Ford and Carter issued executive orders that required the IC to report a larger portion of its activities to both Congress and private institutions.⁶⁰ Yet the most comprehensive approach to the functioning of U.S. intelligence was Executive Order 12333, signed by Ronald Reagan on

December 4, 1981. E.O. 12333 delineated the organization, composition, and duties of the IC, relaxed the regulation of the Ford and Carter administrations, encouraged competition between the various intelligence providers (thereby creating an array of input for the policymaker), and called for a balance between the technical and human means of collection.⁶¹

Besides an administrative component to the dynamic between the president and the IC, there is also a different set of operational norms to consider. Presidents are politicians, with large networks of supporters and contacts, and a great amount of exposure before the general public.

The president, despite his array of advisors and staff members who provide unseen technical and political support, has to function in the public eye; his policies are scrutinized by the media, and his job performance is reviewed directly by the electorate every four years. In contrast, the career service officers in the intelligence community do not work under the same conditions of public scrutiny, and for obvious reasons.

This dichotomy, while unavoidable, presents the ingredients for conflict between members of the intelligence community who see their jobs as vital to the preservation of national security, and presidents who, though vested with the constitutional authority to administer national defense policies, are not always inclined politically to take advice from career government officers.⁶² The ability of these civil servants of different perspectives to work together is based largely on the kind of relationship the president has with his DCI, and, concurrently, the kind of relationship the DCI has with the other major players in the national security

structure, especially the Secretaries of Defense and State, and the National Security Advisor.⁶³

To aid in the oversight of the IC, the president has at his disposal the power and advice of the NSC. Simply put, the president uses the NSC to control the IC.⁶⁴ The extent of the control depends a great deal on the leadership style of the particular president. It also depends on the specific operations the IC must carry out, and how effective it is at accomplishing such tasks. Covert action presents the greatest challenges to Presidential oversight, since covert action is linked with the doctrine of plausible deniability, which states implicitly that there is no direct oversight by the president.⁶⁵

Oversight by the president and his senior staff also entails establishing effective communication between the personnel responsible for furnishing the processed intelligence products, and those policymakers responsible for using those products in making governing decisions. Glaring examples from history, including the Japanese attack on Pearl Harbor in 1941, point to the need for well-established relationships between intelligence providers (the analysts in the intelligence agencies) and users (those who consume intelligence information to help make public policies).

Hulnick makes the point that most of the difficulty in communication between providers and users occurs over intelligence that is strategic, not tactical, in nature. (Note that tactical intelligence is mostly the domain of the military services, since it has to do with information of a strictly military nature, i.e., war and contingency plans. The collection, processing, and dissemination of tactical intelligence is limited

mostly to the DoD, and thus does not face the same obstacles found in the inter-agency collection and sharing of strategic intelligence.)⁶⁶

The major communicatory difficulty found between providers and users regards the provider's misunderstanding of what the user needs. In other words, intelligence providers have not always been able to present intelligence users with the right pieces of processed data at the right times, or in an understandable format.⁶⁷ Sometimes, this problem is the result of providers focusing on their publishing deadlines (and the career prestige accorded to those analysts who publish seminal papers on intelligence topics), rather than on the specific needs of the users. Other times, problems arise because the users expect providers to present their products in a manner that corroborates the policy position of the user, even though decisions on public policies are never the responsibility of the providers.⁶⁸

Another issue that creates a less effective relationship between providers and users is the kind of intelligence product each group prefers. Providers oftentimes favor presenting the product in long and forward-looking formats, culminating in substantial documents like the National Intelligence Estimate (NIE).⁶⁹

Users, however, prefer concise summaries of intelligence analysis that provide intelligence on contemporary matters and that are formatted in regularly published documents like the *President's Daily Brief* (a highly classified document available only to the President, the Secretaries of Defense and State, the NSA, and the Joint Chiefs of Staff), and the *National Intelligence Daily* (a less classified document distributed to other intelligence users).⁷⁰

The differing proclivities have a lot to do with the perspectives of the two groups. The providers feel that their best analysis is found in the lengthy presentations that forecast future events and issues facing national security organizations; the users have a more short-term orientation, and are tepid about projecting policies out farther than six months.⁷¹ Thus, neither group is satisfied in its relationship with the other. Intelligence that is provided for consumption is oftentimes too late in arriving, and not relevant to the needs of the decision makers. At the same time, providers' assurances that their analyses can predict future events with a great degree of accuracy are often contradicted by actual events.

In the end, the decisions made by policy makers suffer because of the problems with the dissemination process. The solution to better relations between the two groups needs to be a priority for the president and his senior officials. It should also be a priority for the congressmen who are responsible for funding the intelligence budgets.

The Congress

When the IC was first established in the 1940s, it fell under the jurisdiction of the House and Senate Armed Services Committees. Yet, while Congress had the oversight authority, it was content in the 1940s and 50s to allow the DCI to perform most of his duties without overt supervision.⁷² This de facto policy changed after the Bay of Pigs, Cuban Missile Crisis, and the failed attempt to oust Allende; Congress became more wary and vocal in opposition to the Executive's historically unfettered domain over U.S. intelligence.⁷³

The Watergate scandal was the final straw; Congress launched two high profile committee investigations of the U.S. Intelligence Community in the mid-1970s to examine allegations of illegal covert operations conducted by the CIA.

The Senate's Church Committee found many of the allegations to be unsubstantiated, but did make recommendations in regard to a permanent committee that would establish oversight over U.S. intelligence operations. The Pike Committee in the House reached the same conclusion as the Senate in regard to the establishment of a permanent oversight committee on intelligence, but added that Congress needed to exact greater fiscal control over the intelligence agencies.⁷⁴

Both the House and Senate Intelligence Committees have come to influence the actions of the IC by holding hearings on a variety of subjects, including the propriety of certain intelligence activities, and by placing constraints on the authorization and appropriation of funding for the intelligence agencies.

Oversight of the IC is more difficult than oversight of other government functions in that the community is shrouded in various degrees of secrecy. The possibility exists that, with close congressional oversight, and the requisite transfer of classified information to a larger number of individuals, intelligence operations may be compromised. However, according to Holt, there have been few instances where members of Congress have compromised the ability of intelligence agencies to perform their tasks effectively.⁷⁵

Since the IC depends upon a great degree of secrecy in its operations, the temptation on the part of the committees is sometimes to allow the intelligence agencies to function without close oversight. At the same time, congressional

overseers run the risk of succumbing to co-optation.⁷⁶ The Intelligence Committees cannot fall into either habit, for they are the conduit of information for the rest of the Congress, and must remain engaged in order to encourage the needed reform in the IC that the president cannot perform alone.

Bilateral Reform

As was noted above, much of the difficulty surrounding the dissemination of the analyzed intelligence product from providers to users manifests in the different vantage point each group has in relation to its purpose. The reason that this aspect of the intelligence production process is located under the sections dealing with the president and Congress (as opposed to being listed with the collection and processing stages) is that it is in the ineffective dissemination of the intelligence product that asymmetric threats might be able to bypass the efforts of intelligence agencies and policy makers.

Ironically, it may be the case that a successful asymmetric attack might occur against U.S. interests and/or assets because government employees are unwilling to adapt their procedures to meet new challenges. The president and Congress are both responsible for and capable of working in tandem to reform the current shortcomings in intelligence reporting and usage.

Hulnick believes that greater interaction is the key to more effective usage of intelligence by policymakers. Specifically, he advocates that the intelligence providers establish good working relationships with the decision makers they are servicing. Hulnick posits that better relationships will lead to an enhanced understanding of the types of intelligence items, and the specific presentation formats,

that users prefer to have at their disposal. These enhanced relationships work both ways, and enable intelligence providers to gain access to policymakers that will enable them to advocate certain intelligence items that might go overlooked on a regular basis.⁷⁷

Holt adds that the intelligence providers need to also recognize that they are not the only capable analyzers of intelligence data; certain users may also have important analytical contributions. For instance, the Foreign Service officers and career diplomats who have spent decades specializing in certain regions of the globe and/or on certain subjects germane to national security and international relations are capable analytical resources, and should be viewed as such.⁷⁸ In other words, collaboration between providers and users should not only occur in regard to the content and presentation of intelligence, but also in regard to its analysis.

Some have also criticized the intelligence agencies for not hiring the best analysts in the first place. Former Navy admiral David Jeremiah, who was commissioned to report on the quality of IC analysts, comments that often the community does not hire the best candidates.⁷⁹ Hulnick claims that a main reason for the hiring problems is that the agencies are not taking full advantage of the growing number of potential employees being produced by U.S. universities with burgeoning intelligence education programs. These points aside, Hulnick insists that the quality of U.S. intelligence has never been in question, but that could change.⁸⁰

Realizing these reforms will not happen because providers and users initiate the process; reforms will happen because the administrative, legislative, and financial organs of the federal government mandate and monitor their implementation. The

overhaul of the DoD Budget and Pentagon procurement priorities is a useful opportunity for introducing reforms of intelligence dissemination, the standards used for new hiring, and the level of funding for the community at large.

Judging by the role the intelligence data played in alerting U.S. installations in the Middle East about possible terrorist attacks, it is apparent that the best method of defense against terrorism is an awareness of when perpetrating entities are likely to strike. Unfortunately, that intelligence did not make it all the way back to where it was needed the most: the U.S. mainland. The success of the September 11, 2001 attacks were not caused by incompetent intelligence workers, but by the issues discussed previously in regard to budgetary problems and Bremer's point about a lack of inter-agency cooperation.

Better intelligence means better relationships between its providers and users. Both the president and the Congress must ensure that this relationship improves. The president, despite his constitutional authority, is not in a position to implement sweeping changes in the bureaucratic system, since civil servants are not always inclined to follow directives established by senior administration officials as closely as is desired.

Since most civil servants, including members of the IC, are career civil service workers, their terms of employment are not affected directly by the direction of the political winds in Washington. The difficulty with this arrangement is that civil servants are not employed at the whim of the administration, and therefore do not usually face the same kinds of disciplinary penalties for not responding to administration directives with timely exactitude.

Therefore, getting the members of the IC to respond to Hulnick's proposal for more interaction between providers and users might not be well accomplished by a presidential directive. Congress, through its authorization and appropriation processes holds the most sway over the civil servants of the IC, since agency funding depends on congressional approval.

However, the president does have a role to play in the reform process – setting goals for administrative departments to meet, appointing department secretaries and agency directors with experience in implementing change into bureaucratic environs, and maintaining good relations with members of Congress in order to reinforce the authority of both governing branches.

The Judiciary

Though it does not possess the legislative functions of the Congress, or the administrative power of the president, the judiciary, especially at the federal level, is becoming a pivotal institution as it relates to the operations of the IC. As technology and collection methods improve, and the presence of asymmetric threats, with their unprecedented challenges to domestic security, continue to develop, the IC is presented with the challenge of balancing effective collection with legal propriety. It is the judiciary that must provide the guidelines for how the IC is to function within constitutional boundaries.

It is illegal for the United States government to collect intelligence against its citizens.⁸¹ It is also illegal for citizens of the United States to take action to subvert the functioning of the government: such action is treason. Recall that asymmetric

threats do not have to be executed by Third World figures like Osama bin Laden; they can be the work of U.S. citizens like Timothy McVeigh.

Thus, U.S. intelligence has an understandable desire to monitor the activities of groups and individuals suspected of harboring the capability and intent to threaten national security and domestic tranquility via asymmetric attack. However, the strictures governing such monitoring are fodder for contentious debate between intelligence and law enforcement agencies, and civil liberties advocates.

On April 23, 2001, the American Civil Liberties Union (ACLU) posted an "Action Alert" to its membership that encouraged them to petition against the use of new intelligence gathering technologies like the FBI's online wiretapping system, Carnivore.⁸² The Carnivore system gives the FBI the ability to monitor the e-mails and other communications of millions of Internet users. This is a departure from laws that constrain monitored content in traditional wiretaps, where, according to the ACLU, the government must winnow out its interception of information not germane to the specific wiretap case.⁸³

The ACLU claims that the FBI's ability to search through millions of private communications, when it has the jurisdiction to search only for specific communications, is an abuse of power and a clear violation of the Fourth Amendment's "right to privacy" guarantee. (Note that the wording of the Fourth Amendment does not include the actual term, "right to privacy.") The civil liberties organization asserts further that technology like Carnivore is unnecessary, since Internet service providers can already monitor the communications of their customers

and furnish authorities with the information for which they have a court order to procure.⁸⁴

David Sobel, General Counsel of the Electronic Privacy Information Center (EPIC), shares similar concerns about the ability of the government to use new technologies to examine private communications. Sobel's group and other civil liberties organizations oppose the nascent development of international cyber crime treaties that, according to the civil liberty organizations, would give unprecedented powers to police authorities and abrogate due process protections.⁸⁵

These criticisms will likely gain little traction in the wake of Attorney General John Ashcroft's plea for expanded wiretapping capabilities in order to monitor the activities of suspected terrorist cells operating within the United States. However, the arguments continue to manifest against expanding the FBI's powers.

Dave Kopel, Director of the Independence Institute, points out that while the FBI and other law enforcement agencies have the authority to search through a single person's regular "snail" mail prior to receiving a search warrant, the practice of reviewing e-mail through the Carnivore system would mean that authorities would be able to search through everyone's mail pursuant to conducting an investigation. Kopel asserts that promises from authorities not to abuse the system are unreliable, but he is not as quick to call on the judiciary to restrict the actions of law enforcement; he feels the private development of technology (as referred to earlier in the chapter) will be able to outpace government monitoring capabilities, and allow for virtually inviolable encryption of e-mail in the near future.⁸⁶

Should the judiciary decide to restrict the usage of technologies like Carnivore, it would undoubtedly be a victory for civil liberties organizations. How much of a defeat such a ruling would be to the collection of U.S. intelligence, especially as it relates to asymmetric threats, is not known, since the actual success rate of Carnivore is classified.

However, a restriction on law enforcement's ability to collect intelligence through the tapping of Internet correspondence would mean an impairment of collection capability; the magnitude of the loss would depend on the degree of the restrictions. Any restriction would provide terrorist organizations with the opportunity to continue, and even enhance, their growing use of the Internet as a means to disseminate information between their members.

If intelligence and law enforcement agencies become restricted in the procedural use of Carnivore and other surveillance technologies, it might mean that terrorist plots, which would have otherwise been detected, might go unnoticed. Citing the impairment of intelligence collection and law enforcement, Adams advocates the same surveillance methods the ACLU rejects:

. . . the intelligence agencies must improve their sources and methods. They will have to develop new means of infiltrating private and government-sponsored groups that wage war in cyber space . . . Congress should pass new legislation that will allow the tracking of intrusions through the Internet. Further legislation is needed to allow law-enforcement agents to infiltrate computer networks when tracking a cyber-criminal, just as they can tap telephone lines. If a national security priority can be shown, such taps could be allowed by law.⁸⁷

Proponents of both sides in the discussion favor using legislation to further their perspectives. A clear standard by the judiciary is needed in this instance.

Though its rulings have yet to pertain to devices like Carnivore, the judiciary has given some indication of its proclivity in regard to the employment of intelligence collection technologies on domestic sites.

The New York Times reported on 11 June 2001 that the United States Supreme Court ruled 5-4 to restrict the usage of a thermal imaging device to detect heat patterns in homes unless a warrant is issued.⁸⁸ If the courts view the legality of employing Internet collection devices in the same way, the IC would be restricted from tracking the actions of a myriad of suspected terrorists who might be plotting an asymmetric attack. The future restrictive rulings of the judiciary might force another entity to perform the collection tasks that the IC cannot without court permission.

The Media

Holt comments that the relationship between the IC and the media is characteristically tense: the media wants to know what the IC is doing, and the IC wants to use the media to further its purposes.⁸⁹ She is quick to point out that, while their relationship is tense, both the IC and the media are performing the same task: collecting information. The similarities between the entities encourage both to use the resources of the other.

In the last decade, OSINT, especially in the form of broadcast cable news networks like CNN and MSNBC, has become the primary information source for policymakers, especially in terms of transmission. It is now commonplace for intelligence analysts and policymakers alike to learn of an event from media organizations first. However, intelligence agencies sometimes have designs on using

media networks and individual journalists for other purposes than the general procurement of breaking news data.

The agencies have solicited the assistance of news organizations, and individual journalists, in order to procure information, or send messages to leaders and/or contacts in foreign countries. For example, ABC reporter John Scali acted as a conduit between the U.S. and the KGB during the Cuban Missile Crisis. In recent years, Bob Woodward has admitted being briefed by the CIA on specific questions to ask foreign leaders during his visits to their countries.⁹⁰

In other instances, the media can be a source of frustration for policymakers and intelligence agencies. "Leak" is the term used to refer to the publication of classified information. Media outlets are sometimes able to create leaks through their own reporting work. The reporter, piecing together bits of information collected from various authorities, usually creates the leak. Usually, no single individual provided the reporter with enough information for the leak; the reporter ascertained what was occurring from the contact he had with officials. In other cases, the leak is a purposeful act performed by a person in position of authority. The reasons for leaks vary, with the most common purpose having to do with one bureaucratic agency undermining the position and/or activities of another.⁹¹

The dynamic relationship between the government and the media impels consideration of the ways in which both entities will come to depend on each other in the new century, and in the aftermath of the terrorist attacks on New York and Washington, DC. This consideration is relevant especially in regard to how the IC

will continue to collect information in the wake of possible court decisions barring the use of Carnivore and thermal imaging.

It is possible that intelligence agencies could come to rely on media organizations to provide information on the activities of suspected terrorists. If intelligence gathering from Internet monitoring is restricted, agencies might be compelled to call upon their relationship with media outlets to provide data that will fill in the gaps. While the media would not be likely to try to monitor Internet correspondence, it could make use of its strongest asset: the willingness of terrorist leaders to employ the media for their own public relations agenda.

This use of the media is prevalent especially among leaders of states known, or suspected, of sponsoring terrorist organizations. Coverage of the life and times of suspected terrorist sponsors like Saddam Hussein and the Ayatollah Khomeini have become centerpieces for U.S. news magazine programs.

The possibility exists that U.S. intelligence agencies would encourage journalists covering such leaders to attempt to gain information about terrorist operations, both in and out of the United States, that intelligence agencies might be prohibited from obtaining for one reason or another. Journalists, realizing the value of the information they would be procuring, might be inclined to cooperate, provided they were allowed to use portions of the collected data in their reports. From this arrangement, a quid pro quo might develop by which media outlets, enticed by the prestige the exclusivity of their coverage provides, might become willing to withhold information from public view in order to continue the lucrative access to leaders and environments that come with cooperation with the government.

As Holt points out, the propriety of such an arrangement is in doubt. The press, at least in the conception of the Founding Fathers, was intended to remain free from coercion by government interests. It was to be an independent adjudicator of events, a conduit of information for public consumption and enlightenment.⁹²

Of course, the media already has access to figures like Hussein without doing collection work for the IC. For this reason, it is possible that the media could refuse to perform collection favors for the intelligence agencies should agencies be restricted in their collection capabilities. However, Holt intimates that the media community might be inclined to go along with the IC to a certain extent because of the allure of access to government operations.⁹³

The allure of intimate cooperation with intelligence agencies, and the informative benefits such cooperation provides, might prove to be too tempting for the media in the long term. Unfortunately, the closer the relationship between the two parties, the less likely it is that the public interest will be the foremost concern of the journalists involved:

At this point, the media and the IC seem to be two separate entities with similar functions. How separate the two remain might depend on whether the judiciary permits the IC to pursue its collection tasks without prohibition on certain procedures.

While this section considerable time to exploring the issues challenging the successful operation of the IC, its main point is not that the IC is incapable of functioning properly. On the contrary, if such were the case, there would be no need for this thesis, since the shortcomings of U.S. intelligence would be apparent to all. The fact that this consideration of U.S. intelligence is short, compared to the length it

might be if there were a multitude of glaring intelligence failures, is an indication of the IC's fulfillment of its tasks.⁹⁴

The considerations presented below are some of the areas where academics, diplomats, and former members of the IC feel the community's operations can be improved. This chapter is intended to be a general assessment of the IC's relationship with the branches of the federal government, and the public at large. It is intended to expound further on the general introduction of the IC in the preceding chapter, and provide a point of reference for recommendations on how to address asymmetric threats effectively.

While the IC concerns itself with the collection and processing of data covering a wide variety of topics germane to national security, this chapter is concerned primarily with the manner in which intelligence can be collected and used to help deter and prevent terrorist activities that utilize asymmetric tactics.

Intelligence, Asymmetric Threats, and Intra-Government Cooperation

In any attack using asymmetric means, local authorities will be the first to encounter the fallout from the crisis. This is especially the case with attacks using chemical and/or biological weapons (information warfare is likely to strike larger areas at one time). For municipalities to respond effectively, budgets will have to be reexamined, and spending priorities rearranged, in order to accommodate the personnel and equipment necessary to treat thousands of infected citizens.

The going rate for some of the most basic types of equipment used in these circumstances ranges from \$200 for a regular decontamination kit, to \$3,000 for a high-tech, gas-proof anticontamination suit.⁹⁵ Given the large emergency

management divisions in many towns and cities across the United States, it is clear that local officials will have to make choices between the maintenance of older acquisition items, such as police cars, and the procurement of newer technologies, like the gas-proof suits. Karen Ann Coburn, a writer for *Government* magazine, states that for years, local governments did not consider preparatory action against terrorist attack as a serious issue.

However, the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City changed the minds of many local governing officials.⁹⁶ Yet, even with greater preparation at the local level, municipalities simply do not have the requisite resources to mount a thorough response plan. This is where the quality of the relationship between local, state, and federal officials is important.

Historically, local officials have been suspicious of the commitment of state and federal agencies to prevent, or at least mitigate, a terrorist attack. According to Kathleen Henning, emergency management coordinator for Montgomery County, Maryland, the suspicion started when federal agencies established disaster response policies that required evidence of mass death at the municipal level before sending aid to the site of the attack. That policy did not leave local emergency response teams feeling confident that, in the event of an attack, federal assistance would arrive in a timely manner.⁹⁷

Federal agencies, the FBI and DoD especially, continue to have a reputation for uncooperativeness with local authorities. Henning claims that local requests for information (derived from intelligence data) from the DoD and/or FBI results usually in the agencies claiming that the information cannot be shared.⁹⁸ In recent years, the

Federal Emergency Management Agency (FEMA) has earned a reputation for improving its relations with local governments, especially by encouraging the stockpiling of vaccination supplies to counter chemical and biological agents.⁹⁹

Part of this change in FEMA's conduct is due to the 1996 Defense Against Weapons of Mass Destruction Act, better known as the Nunn-Lugar Act in recognition of its two main sponsors. Nunn-Lugar directed the DoD and FEMA to provide \$160 million to train the nation's 120 largest communities how to respond to attacks where incendiary, biological, chemical, and/or nuclear materials were introduced.¹⁰⁰ Another resource for local government is Presidential Directive 39, which provides a specific blueprint for intergovernmental coordination in the wake of a terrorist attack.¹⁰¹

While these improvements will certainly help in providing the necessary relief in the aftermath of an asymmetric attack, note that they are strictly response oriented. If the IC has information that suspects an attack might occur, it should consider how it might communicate that warning to the appropriate local authorities without compromising its own ability to maintain quality collection. This thesis suspects that bureaucratic competition may have more to do with the FBI and DoD withholding data, than any concern over protecting classified material.

Strictly speaking, the function of both the FBI and the DoD is to provide the nation with the best perception of current events available, including educated foresight on the entities suspected of hatching terrorist plots against national interests. Intelligence data is not the exclusive property of the isolated IC in that it is paid for by the tax dollars of the U.S. citizenry. Therefore, any deliberate withholding of vital

information that might be used to forewarn local authorities of a terrorist attack, and perhaps prevent the attack from happening in the first place, is inexcusable.

This thesis recognizes that intelligence collection, especially in the HUMINT realm, must be protected from breaches of “cover” (the identity protection afforded agents in the field); however, if local officials can be counted on to maintain protection of the intelligence data (keeping it away from local media outlets that might be less than discriminate in reporting classified data), there should be little reason why the federal intelligence agencies do not establish more open sharing policies with local and state authorities.

Government silence is not limited to its relationship with local governments, however. Private entities are just as likely to receive little advanced warning from the government regarding incipient asymmetric attack, especially in the area of information warfare. Adams writes,

Despite the warning signs, the United States still does not prioritize threats to the private sector or sufficiently emphasize cooperation between citizens and government in defense. In many cases, Washington remains legally constrained from passing on information about potential threats to the private sector.

For example, intelligence officials now believe that certain hardware and software imported from Russia, China, Israel, India, and France are infected with devices that can read data or destroy systems. The names of the suspected companies and producers are not available to the private sector, however, and because that information and the intelligence that supports it are so highly classified, the suspicions are impossible to verify.¹⁰²

Thus, the high levels of classification of intelligence data present vexing challenges to both the local governments and the private industries that are looking to protect their assets. In the absence of quick reform of the IC in this regard, other reform policies might be of some assistance.

Since the majority of the IC is housed and financed under the edifice of the DoD, Adams suggests that the DoD take the lead in organizing a response to the asymmetric security challenges, especially in the area of cyber defense. A more pronounced effort by the DoD in Homeland Security would alleviate the problem of the IC having to share its information with outside agencies at the state and local level. Under such a plan, the DoD, and the rest of the IC, could continue to collect, analyze, and disseminate intelligence data according to current practice; the agencies would simply add the responsibility of domestic defense to their job descriptions.¹⁰³

Yet the establishment of Homeland Security might not be easy for some to accept. The U.S. military establishment has spent decades building its policy objectives around force projection, not domestic defense. A change in this dynamic would certainly require a pronounced alteration in current defense priorities; DoD policymakers will likely not welcome these changes. At the same time, the public might have mixed feelings about an overt military presence in their daily activities.¹⁰⁴

In summary, the IC, if it has information pointing to an impending asymmetric attack, must be able to share that information with officials who will need the information the most: those on the local governing level. It is hard to know if the classification of intelligence data is really as necessary in all cases.

However, if high classification is necessary, perhaps it is time to transfer primary responsibilities for prevention and defense against attack to the federal agencies that have the most accurate information on the threat. The legal implications are obvious, especially in regard to the preservations of civil liberties by a defense department whose service personnel are subject to martial law.

The policy problems created by asymmetric threats are obvious, but they pale in comparison with the consequences of not taking constructive action to make the necessary defensive provisions.

Intelligence, Asymmetric Threats, and Foreign Policy

This portion of the chapter will examine the IC and foreign policy in relation to the three major areas of asymmetric threats – biological and chemical weapons, and information warfare.

Biological Weapons

As a signatory to the 1972 Biological Weapons Convention, the United States is in a position that precludes it from manufacturing such material. The effect has been noticeable. According to Peter Pringle, a writer for *The London Sunday Times*, the U.S. biological weapons stockpile included 400 different agents, 17 of which were toxic enough to be employed on the battlefield.¹⁰⁵ Following ratification of the 1972 agreement, U.S. biological weapons production was scaled back to virtually inoperable status. The same cannot be said for the FSU, which, according to estimates, continued to produce billions of metric tons of anthrax and other biological agents every year.¹⁰⁶

Frank Gaffney Jr., Director of The Center for Security Policy in Washington, DC, suggests that the entire premise of the 1972 agreement was flawed, since the agreement made no provision for verification of the destruction of then-current stockpiles, or credible monitoring of restrictions against production of new stockpiles.¹⁰⁷ As with many “goodwill” agreements, those nations valuing rectitude in

their dealing with the world community follow the letter of the agreement; unfortunately, all nations do not value rectitude as highly.

Chemical Weapons

Gaffney views the 1993 Chemical Weapons Convention in the same light as the biological convention, claiming that it is unenforceable because of the lack of verification of compliance, and the relative ease with which the agents may be manufactured.¹⁰⁸ Another aspect of the problem is the fact that the materials used to manufacture chemical weapons are part of a large set of “dual use” technologies also responsible for the manufacturing of fertilizers, pesticides, and pharmaceuticals. Private firms conducting international business may not realize that the technologies and equipment they are selling Third World entities for supposedly commercial purposes might actually be used for making chemical weapons.¹⁰⁹

The major problem with both weapons conventions results from the gap of verification of compliance. Given that many of the entities suspected of manufacturing biological and chemical weapons are from the Third World, and given the predominance of Third World influence in international organizations like the United Nations, the United States is in a position of having to advocate policy changes in the approach to biological and chemical weapons proliferation that will resonate well in the global community.

Global Solutions to Biological and Chemical Weapons Proliferation

Consideration of the global environment in relation to the establishment of provisions against asymmetric threats is extremely relevant. Gaffney is quick to point out, however, that, while his four solutions are improvements over the hard-to-verify

biological and chemical weapons agreements, they do not constitute an inviolable aegis for either world, or U.S. security.

First, according to Gaffney, multilateral agreements between the nations possessing the most sophisticated manufacturing technologies would help both in curbing the proliferation of those technologies into more irresponsible hands, and in providing a checks-and-balance system to encourage technologically advanced nations to act responsibly.

Second, the provisions for prohibition on the use of chemical weapons in warfare (a provision of the 1925 Geneva Convention), if enforced strictly, would be a good deterrent, especially if prospective perpetrators knew they would face certain retaliation as proscribed by international agreement.

Third, the destruction of the actual manufacturing facilities suspected of making the biological and chemical weapons agents should be utilized, provided policymakers have accurate intelligence that is reasonably sure that the right target will be hit.

Fourth, a strong deterrence by conventional military force is always a way by which manufacturers of biological and chemical weapons may be dissuaded. According to Iraqi officials, this was indeed the case with Saddam Hussein's decision not to unleash chemical and/or biological weapons during the Gulf War.¹¹⁰

As the precepts of the global paradigm begin to take form in the institutional language of the U.S. marketplace, and educational institutions continue to inculcate the doctrine of a one world globalism the institutions created to encourage international interdependence will continue to tolerate less and less the aberrant

behaviors of nations that are not willing to comply with the general protocols and standards adopted by the global (or at least partially global) community.

The United Nations has long advocated, especially through its Brandt Commission, global nuclear disarmament. While the United States is not in a position to surrender its nuclear assets in the near future, the constant drum beat by global proponents for disarmament have made it all but impossible for U.S. policymakers to consider realistically the use of nuclear weaponry in response to a biological and/or chemical weapons attack.

Thus, if the United States is to mount a successful deterrence effort, it will have to do so using other means than Gaffney suggested in his fourth point. The dissemination of some U.S. intelligence products for consumption by world organizations like the UN, as well as coordination of efforts among members of the international intelligence community, are constructive and effective ways to reduce the possibility of a biological and/or chemical weapons attack.

Ely Karmon, a research analyst on terrorism, commented on the state of international intelligence cooperation at the Conference on “Intelligence in the 21st Century” in Priverno, Italy, 2001:

International cooperation has improved, mainly on the bilateral level. Even the Israeli security services have been cooperating . . . The Arab league countries have arrived at an agreement to coordinate their intelligence and security activities against the radical Islamist movements . . . Even Russia, and for the first time China, have united their efforts to fight Islamic radicals in Central Asia . . . Russia has upgraded and enhanced its intelligence cooperation with the United States, Great Britain, Turkey, and Israel . . . A new European body, Europol, is also a step in the improvement of cooperation at the regional level.¹¹¹

How cooperative some of these entities will remain with each other has yet to be seen. For instance, it is not clear what kind of sustained relationship China and Russia will have in relation to intelligence cooperation both with each other and with the Western intelligence community. Recall that both states are suspected of manufacturing and distributing biological and chemical weapons materials to rogue entities like North Korea and Iran. China and Russia may be collaborating on intelligence efforts to secure interests that are not in harmony with the needs of the Western powers.

The same cannot be said, at least publicly, about the relationship between the United States and Europe. In an op-ed column in the June 11, 2001 edition of *The Washington Times*, National Security Advisor Condoleezza Rice commented on the state of the U.S.-European security relationship.

Europe and the United States are partners today. We will continue to be partners tomorrow and the day after – strong partners. Not because of destiny, but by choice. Not because of inertia of our common history, but because of our common interests, and, indeed, our common values.¹¹²

Whether or not all the major world powers cooperate fully in regard to sharing intelligence data, the infrastructure is in place to create a somewhat reliable network of collection and dissemination. The world will soon know whether the immense intelligence sharing operation resulting from the terrorist attacks against the United States will bear fruit. *The London Times* reported on September 15, 2001, that all 18 NATO nations, as well as other U.S. allies in Asia are working closely on disseminating intelligence on the activities of terrorists throughout the alliance.¹¹³

If globalization is the trend that will eventually mean the vitiation of sharp nation-state distinctions in the world community, then national intelligence organizations must be prepared to accommodate such change, and they might be more willing to do so given the events of September 2001.

A corollary of shared intelligence is that, by gathering information on the activities of suspected perpetrators of terror, the various national intelligence communities would then be able to make a collective assessment of the threat to global security, disseminate that information to world bodies like the United Nations, which could then use that information to respond either as a decision-making institution (if the global power structure has progressed to that point), or broadcast the findings of international intelligence to the world media, thereby bringing unwelcome elucidation on the otherwise surreptitious terrorist activities, and states that sponsor them.

Admittedly, there are flaws in such a theory. Whether any international organization would have the ability to thwart a terrorist plot in all circumstances is doubtful. However, it is possible that cooperation between national intelligence agencies would deter terrorists from perpetrating attacks on unsuspecting targets. It is also a more practical alternative to a national reliance on nuclear deterrence. This is true especially in regard to asymmetric attacks, since terrorists would find it more difficult to establish safe havens of operations in countries that are encouraged to desist from supporting terrorist entities.

Interestingly, international cooperation on intelligence data collection already takes place, much to the consternation of critics who claim that spy systems like

ECHELON (a network of electronic spy stations in the United States, Canada, England, New Zealand, and Australia run by the NSA), which are capable of intercepting virtually all electronic communications worldwide, violate the First, Fourth, and Fifth Amendments of the Constitution, and are not consistent with Western democratic values.¹¹⁴ ECHELON has raised concerns on the part of European Union (EU) nations that believe that the United States might use concerns about terrorist plots to justify signal interception in Europe, and other parts of the globe.

Thus, there is potential good and bad that could result from a global effort at intelligence collection. This thesis holds that despite the constitutional and diplomatic issues, international collaboration in intelligence collection is a requisite for effective defense against asymmetric threats, especially cyber warfare.

Information Warfare

The significant level of dependence Western societies, and the United States in particular, place on computer technology presents terrorist entities with a perfect asymmetric target. Perhaps the most lethal of the asymmetric threats considered in this thesis is information warfare, which entails the sabotage of computer networks and other hardware and software components that support the functioning of U.S. civilian and military infrastructures. It has the ability to disrupt the basic life-sustaining services that provide the basis for quality of life in the United States.

Specific details regarding the nature of the cyber warfare threat were discussed in Chapter Two. The purpose of this section is to consider cyber warfare

from a global perspective in conjunction with the recommendations made for international intelligence collaboration discussed previously.

In his testimony before the Senate Select Committee on Intelligence on February 2, 2000, Vice Admiral Wilson stated:

The information operations threat continues to spread worldwide . . . opponents . . . will seek to develop only computer network attack options . . . Today, we are more likely to face information operations carried out by terrorists, insurgents, cults, criminals, hackers, and insider individuals spurred by a range of motivations.¹¹⁵

In order to mitigate the threat of cyber warfare, Karmon suggests that the intelligence agencies need to do more to collect data from geographic regions where terrorist entities are suspected of hiding their infrastructure from the rest of the world.

It is important that intelligence services also cover the so called gray zones and do not permit the formation of 'blind spots' in the overall intelligence picture, such as Afghanistan and Somalia. Such 'holes' in intelligence would permit terrorists groups to find safe haven in such places, and from there to develop and proliferate to the outside world.¹¹⁶

Preventing the "blind spots," as Karmon calls them, requires the coordination of efforts of the U.S. intelligence agencies, and their compatriots in locations that afford better surveillance of the terrorist activities, which is all the more urgent given recent days. Therefore, foreign and diplomatic relationships with states that may have ranked lower on the U.S. foreign policy agenda in the past (African states especially) will have to be cultivated.

The United States can draw on examples from its closest allies to observe ways in which intelligence operations can counter terrorism and asymmetric threats

effectively. Germany is an important example of how a concerted collection effort of OSINT, SIGINT, and HUMINT can prove to be a useful anti-terrorism tool. The success of the German intelligence system is based largely on a sophisticated computer program that processes information collected on suspected terrorists.

The processed information, obtained via the OSINT methods of media collection, the SIGINT method of communication interception, and/or through HUMINT collection is then disseminated to all law enforcement personnel in the country. The law enforcement officers carry printouts of the information with them during their investigations, be they related ostensibly to terrorist attacks or not. The heightened concentration on the identity and activities of terrorist entities makes the development of terrorist acts harder to realize, and, according to Combs, has had success in preventing new terrorist attacks.¹¹⁷

Yet it is unclear whether a similar program could even be implemented in the United States. With a population and geographic area several times larger than Germany, as well as a law enforcement establishment already stretched thin with other security and investigational tasks, such a concerted effort against terrorist and asymmetrical threats would be a logistical and fiscal impossibility. Another issue with the German model is that it abrogates the statutory distinctions between intelligence collection, law enforcement, and due process. The legal system in the United States would be far less willing to sidestep civil liberty safeguards for fear of abuse by authorities.

However, a less controversial path to the same goal might be the creation of a terrorism intelligence-monitoring center, which would be staffed and overseen by

components of existing IC agencies. The newly created White House Office of Homeland Security could be the beginning point of this new type of monitoring effort. The specific focus on terrorism and asymmetric attack by a separate agency would enable other collection targets to receive necessary attention from intelligence analysts and policymakers.

International cooperation is the key to frustrating the efforts of terrorist entities. This is especially the case in the realm of cyber warfare, where perpetrators need not be anywhere near their intended targets. INTERPOL, the international police organization, seems to be the best candidate for coordination of the international intelligence collection effort on terrorism. INTERPOL members would have at their disposal collection products from intelligence organizations that bring a wide variety of strengths in TECHINT and/or HUMINT, as well as geographical advantages that other national agencies might not have at their disposal.¹¹⁸

Summary

This section has examined the intelligence community in some detail. It has also explored some of the issues facing U.S. and international intelligence agencies as they work to attempt to provide timely and accurate data on the activities of possible perpetrators of asymmetric attack. It did so because of the supreme importance of a good intelligence product in securing national security against terrorism and asymmetric threats.

While the challenges presented here are daunting, and the recommendations for improvement only partial solutions, there are initiatives that can be undertaken that will help mitigate the overall danger posed by asymmetric security threats.

This thesis argues that a quantified assessment of the actual dimensions of the entities possessing the capability and the intent to perpetrate an asymmetric attack, clear and specific operational procedures between the three levels of government and their respective law enforcement and security agencies, and greater inter-national cooperation, both on a diplomatic and an intelligence collection level, are all necessary improvements in the current mode of national and international security operations. The fourth section considers specific policy proposals in light of the information on the nature of the asymmetric threat, and the role of good intelligence.

Section Four: Public Policy Recommendations

The events of September 2001 underscore the need for a comprehensive response to the issue of Homeland Security. President Bush has made the initial moves to implement such a response to the nation's security vulnerabilities by appointing Pennsylvania Governor Tom Ridge to head a new White House office directed toward coordination of the 40-60 federal agencies and departments that will play a role in securing the continental United States, Alaska, Hawaii, and U.S. territories and embassies – the homeland – from attack, especially with biological weapons.¹

This section considers specific policies that Ridge must consider if he and the Bush Administration are to be successful in staving off another round of terror attacks against U.S. interests. It considers policies that will address all asymmetric contingencies, but it concentrates on bioterrorism in specific.

The recommendations that follow do not deal with the international aspects of a national security campaign against terrorism, although, as was discussed at the closing of the previous section, there are areas (like intelligence) where international and inter-agency cooperation is vitally important.

These recommendations also do not assume that all future attacks can be prevented, or that there are not future attacks in the works as of this writing (late October 2001); however, they do proceed with the idea that prevention is always

better than response. New York City mayor Rudolph W. Giuliani stated it well when he commented that to assume that future attacks will not occur if we refrain from addressing the terrorist entities through interdiction of and planning response to their attacks is simply misguided.²

As with the previous sections, these recommendations focus on the various forms of asymmetric attack, with particular consideration to biological weapons.

Law Enforcement and Executive Branch Responses

Give Homeland Security Director Budgetary Control

Creating a new White House office to combat terrorism will only be effective if he has the ability to abolish the parochial interests and turf battles that have heretofore existed between the various law enforcement, intelligence, defense, economic, and emergency response organizations that play a part in countering terrorism.³

Ridge must have the ability to hire and fire personnel, as well as re-direct funding to specific areas of the security infrastructure that will be required to handle the first response duties, if another terrorist attack occurs. He must also be able to meet with the President and the National Security Council staff on a regular basis to ensure that there is seamless cooperation between the various heads of government.⁴

Establish Joint FBI and CIA Task Forces

Former Ambassador-At-Large for counter-terrorism, Paul Bremer, has made it clear that part of the problem in anticipating a terrorist attack is that the FBI and CIA are not in the habit of sharing information with agents from the other organization. This must change.

Part of the problem, according to Bremer, is the fact that the agencies are charged with carrying out two different kinds of functions: the FBI is primarily a law enforcement organization, with a smaller division devoted to counter-terrorism, and the CIA is an intelligence agency. Even the manner by which the two agencies approach their anti-terrorism duties is fundamentally different. When encountering a suspected terrorist, the FBI's first reaction is to incarcerate; on the other hand, the CIA is likely to want to turn the captured operative into a mole for CIA HUMINT service. Thus, there is inherent tension between the two agencies in terms of how they function.⁵

The reason cooperation is so important is that, by law, the CIA is prohibited from conducting intelligence collection within the domestic United States. So long as this is the law, there will need to be a heightened level of cooperation between the two agencies, which would be best accomplished by a joint agency task force that focuses on making sure that information from the national field offices of the FBI and the international offices of the CIA, is collected, processed, and disseminated to the necessary personnel. A task force would also have the potential to palliate the sharp functional differences between the agencies in terms of an approach to Homeland Security.

Expand Wiretapping Capability

The Patriot Act, signed into law by President Bush on October 26, 2001, allows the FBI to conduct wiretapping not just on individual land lines, as is now the practice, but on all communications equipment (especially digital) suspected of use by a terrorist organization.⁶ The changes have already been implemented in states like

New York, whose legislature passed new legislation allowing for expanded wiretapping capability against suspected terrorists.⁷ These changes need to be reevaluated continuously for their efficacy.

Abolish Laws That Restrict CIA Collection Against Domestic Entities

On the theory that two heads are better than one, it is necessary to involve the CIA in the collection of intelligence on the actions of entities suspected of hatching terrorist offensives against the United States. Since evidence continues to suggest both the continued presence of terrorist “cell groups” throughout the nation, as well as the FBI’s difficulty with investigating all of them competently, the introduction of the CIA into the process could only have a beneficial effect.

The alternative would be to increase sharply the financing and personnel devoted to FBI counter-terrorism efforts. However, time is of the essence. Any significant upgrades in the capabilities of the FBI infrastructure could take years to implement.⁸ The CIA, for all its alleged shortcomings, is still the specialist group in terms of HUMINT collection. Since many experts agree that better HUMINT is paramount to better national preparation against terrorism, the CIA needs to be brought into the domestic counter-terrorism picture.

As was mentioned in the previous section, greater intelligence collection in the United States raises implications for the preservation of civil liberties. Such concerns need to be addressed, but terrorism policy experts, like Virginia Governor James Gilmore, believe that constitutional liberties can be preserved in spite of increased domestic intelligence surveillance.⁹

Limit FBI Responsibility on Other Domestic Investigations

Though it is the lead domestic law enforcement and investigating agency into the U.S. terror attacks, the FBI continues to have a full plate in terms of other law enforcement responsibilities. Important as these other responsibilities are, they pale in comparison to an effective counter-terrorism program. Therefore, giving other state and federal agencies the jurisdiction over certain federal law enforcement issues would alleviate the strain placed on the FBI, and allow it to devote its fullest measure of resources to combating terrorism.

Examples of shifts in responsibility would be to encourage state police organizations to coordinate their resources on kidnapping cases, and transferring full responsibility to overseeing the enforcement of drug laws to the bureau of Alcohol Tobacco and Firearms (ATF) and the Food and Drug Administration (FDA).

Increase Infrastructure Security

In the days immediately following the attacks on New York and Washington, DC, the Coast Guard took unprecedented steps to ensure that ships were not carrying explosive devices or other weapons by stopping and boarding vessels before allowing them to dock at ports. Germ warfare units from the National Guard were sent to nine select locations around the United States.¹⁰ The American Water Works Association (AWWA) ordered the highest state of alert for security around the nation's water supplies.

In addition, Environmental Protection Agency Administrator Christie Whitman directed the EPA to initiate readiness to implement countermeasures against any outbreak of a biological and/or chemical weapon.¹¹ The Centers for Disease

Control in Atlanta, Georgia has alerted hospitals and health care facilities around the nation to be on the alert for any signs of bio or chemical terrorism.¹²

At the same time, the Department of Health and Human Services (HHS) has activated the National Pharmaceutical Stockpile to prepare for any eventualities.¹³ The FBI grounded crop-dusters for fear that terrorists were contemplating their use for delivering biological and/or chemical weapons.¹⁴ Security at airports, stadiums, and all other major open-air events has been increased to levels heretofore unknown in the continental United States.

All these are good and important steps, however, with a nation this large and this vulnerable, more needs to be done in these areas to improve communication between the various entities, as well as provide the personnel necessary to extend the web of protection already in place. For instance, while nine National Guard germ warfare units are better than none, the insidious nature of the biological weapons discussed previously suggests that more units would be a welcomed presence.

In May 2001 testimony before Congress on the issue of the FBI's efforts in countering terrorism, Attorney General John Ashcroft requested \$107.96 million to combat terrorism in its various forms, including cyber, nuclear, and chemical and biological.¹⁵ This level of funding is likely to increase exponentially after the attack on September 11, and should be placed toward buttressing and expanding the security activities discussed previously.

However, spending more money, though a natural reaction for politicians who want to appear as though they are addressing policy issues with all deliberate speed, may actually be unproductive in terms of providing clear leadership and effective

countermeasures. This is why Secretary Ridge must have the ability to direct budgetary resources in specific directions, and not allow the funding to be lost in departmental turf wars.

“Go to the Guard”

In January 2001, the U.S. Commission on National Security in the 21st Century, chaired by former senators Gary Hart and Warren Rudman reported on ways in which to secure the highest levels of national defense against asymmetric threats, including all forms of WMDs. The problem of a lack of national preparedness has much to do with the fact that there is little in regard to a organizational infrastructure that could coordinate the activities and training of the first responders to an attack – police, fire, rescue, and, in the event of a bioterrorism event, the medical community.

The commission recommended changing the basic responsibility of the National Guard from supporting overseas military activities to being the organization responsible for establishing the infrastructure to allow the other response agencies (FEMA, EPA, HHS), to perform their functions effectively.¹⁶

Uninterrupted security, logistics, and communication infrastructures are the keys to an effective response to an asymmetric attack. Little has been made of the possibility of civil unrest in the wake of a bioterrorism assault. However, as was discovered in the “Dark Winter” simulation of a smallpox outbreak, the line between national unity and anarchy is a thin one.¹⁷ (“Dark Winter” was a simulation of a smallpox outbreak in Oklahoma City. It was designed to show the impact of such an outbreak on local first responding agencies.)

Thus, there need to be an agency whose job it is to coordinate and secure the base of operations so that the other forms of government response are not overwhelmed, or overrun.

The strategic proximity of the National Guard in all 50 states makes it a likely choice for assuming the primary coordination and implementation responsibilities in the event of a WMD attack. Title 32 of the U.S. Code, which gives control of the National Guard units to the individual states, and PDD 32, discussed in Section One, would have to be reworked in order to assist the National Guard with its growing federal role.

This is not to suggest the National Guard be used as a federal police force. This proposal envisions the National Guard in a response, not law enforcement, capacity. It does not recommend the stationing of National Guard troops in permanent security positions at airports, bus terminals, and other locations.

Establish An Anti-Terror DoD Command

It is possible that the conversion of the National Guard into a force capable of the type of leadership necessary to establish effective homeland security measures might take too long. If such is the case, emergency response and homeland security protocols that are conceptualized and approved by Ridge and President Bush could be implemented by one of two U.S. military commands. The 2001 Quadrennial Defense Review, which will guide DoD spending priorities beginning with the FY 2003 budget, is already positioning homeland security as the top DoD priority.¹⁸

Either the U.S. Joint Forces Command in Norfolk, Virginia, which already has responsibility for 80 percent of U.S. military forces, or the North American

Aerospace Defense Command, which is based in Colorado Springs, Colorado, could oversee implementation of homeland security measures.¹⁹

A stronger case can be made for the assumption of security responsibility by the Joint Forces Command, since it already has existing responsibilities in assisting federal responding agencies in the event of a WMD incident.²⁰ However, given the different kinds of responsibilities required in defending the United States, it is possible for both commands to have a significant role in implementing homeland security.

Of course, as Gilmore pointed out in congressional testimony on September 21, 2001, introducing the regular military into lead roles in homeland security is contrary both to U.S. Code and the intention of the Founding Fathers.²¹ These issues will have to be considered, but, regardless of whether the National Guard or defense commands are used to implement response programs, there must be a clear and accepted chain of command and cooperation between the federal, state, and local responders.

Even if the National Guard is used to oversee the WMD response efforts, the vast resources of DoD will be a great asset in such a response and will need to be well coordinated and prepared. Thus, a command devoted to preparing DoD assets for use in Homeland Security missions is still a necessary initiative.

Use Better Intelligence to Assess the Bioweapon Threat

Some of the sources cited previously take for granted that asymmetric warfare, and the specter of bioterrorism in specific, is the greatest new threat to national security. In the weeks following September 11, 2001 attacks, many media

outlets began running stories detailing in almost apocalyptic language the draconian threats posed by biological and chemical weapons, and the likelihood that millions of citizens would die from infection.²² This thesis views terrorism, asymmetric attack, and bioterrorism seriously, but with an objective eye.

As stated in Section One, this thesis is concerned with ways to assess the threat of bioterrorism in as rational a way as possible. Such objectivity is beneficial especially for policymakers who will have to make the tough decisions concerning policies to combat bioterrorism. Section Two established the position of several experts on the nature of the bioterrorism threat. Section Three introduced the intelligence community and its role in fashioning accurate information on all national security threats. This portion of Section Four looks at how OSINT can bring balance to the bioterrorist data employed by analysts like Osterholm and Henderson.

The question here is whether intelligence collection and analysis can further define the actual threat posed by asymmetric aggression, thereby providing a frame of reference from which policymakers can work. It is possible that intelligence data could actually dispel some of the contentions made by proponents of greater defense spending to guard against an asymmetric WMD attack.

Drs. Jonathan Tucker and Amy Sands, directors of the Chemical and Biological Weapons Nonproliferation Project at the Monterey Institute for International Studies, dismiss the idea that many terrorist organizations have the capability to manufacture biological and chemical weapons. (The use of chemical weapons by Aum Shinrikyo in a Tokyo subway on March 20, 1995 that killed 12 and injured four thousand civilians actually substantiates the Tucker/Sands assessment,

since the group lacked the technical knowledge to manufacture and disseminate more lethal biological weapons.)

Tucker and Sands base their position on more than the notion that terrorists lack the engineering ability to manufacture such weapons: they believe that many terrorist organizations would find the utilization of asymmetric devices counterproductive to their aims.²³

Tucker and Sands cite the slow incubation period of some biological weapons as a reason why terrorist groups, which thrive on the immediate turmoil an unexpected catastrophe creates, would be unwilling to use such weapons. They introduce an interesting perspective for consideration.

Whereas bioterrorism experts like Osterholm assumed that the insidious nature of biological weapons made them the perfect weapon for terrorists, and Combs' definition of terrorism emphasized the targeting of the civilian population, the Tucker/Sands assessment takes the opposite view, claiming that the delay in recognition of the terrorist act by the victimized entity would prove to be too frustrating to the terrorists in the long term. This is why, according to Tucker and Sands, terrorists are more likely to continue using conventional explosive devices in their attacks.²⁴

The Tucker/Sands perspective bears out in relation to recent developments pertaining to water contamination in metropolitan areas. According to *The New York Times*, the contamination of bottled water in New York City in the fall of 2000 was the result of lax monitoring by the municipal sources that provided the bottled water, not any kind of foul play as some suspected.²⁵

The same can be said for recent outbreaks of St. Louis encephalitis in New York City and northern New Jersey. On September 19, 1999, *The New York Times* cited the contention of some health policy experts that it was the lax surveillance of the metropolitan mosquito population, precipitated by a reduction in the city's Health Department pest-control unit, which caused the deaths of at least three people that year.²⁶ Some speculated that the water and mosquito contaminations were the product of biological attack, but that has proven highly unlikely.

The challenge presented to intelligence agencies deals specifically with their ability to extrapolate future occurrences from historical data. Tucker and Sands give them a head start. According to their research, between 1900 and May 1999, there were 263 reported incidents of biological and/or chemical weapons attacks worldwide. (The 263 cases cited are the actual events that the Monterey Institute has been able to record and find enough data about to be able to conduct cross-case comparisons. The actual number of attacks may be significantly higher.) Of those 263 cases:

... 26 percent were hoaxes or pranks, eight percent involved an apparent conspiracy that did not proceed far, four percent involved the attempted acquisition of dangerous materials, 10 percent involved the actual possession of dangerous materials, 21 percent concerned a threatened attack that did not materialize, and only 27 percent (71 incidents) included the actual use of a chemical or biological agent. Of the actual attacks, 83 percent (59) occurred outside the United States. . . In very few cases did the perpetrators seek to inflict mass casualties – defined as 1,000 or more deaths – and in none did they occur.²⁷

Peter Mazur, Research Professor at the Department of Biochemistry and Molecular Biology at the University of Tennessee at Knoxville went on record in the days following the 11 September attack to dispel the notion, promulgated by

Osterholm, that the manufacturing and delivery of biological weapons, especially via aerosol technology, is relatively easy:

... to be infectious via a pulmonary route, organisms like anthrax spores would have to be dispersed as aerosolized liquid droplets or dried particles of a very restricted size range. If too large, they will not enter the lungs. If too small, they will not remain in the lungs. Thus, to be an effective weapon of mass destruction, terrorists must not only manufacture and smuggle in 200 pounds of anthrax, they must have devices to disperse it as properly sized droplets or particles. The latter is no simple matter.²⁸

As a response to the media misrepresentations of the biological weapons threat, other scientists, like Dr. Barbara Rosenberg, director of the Federation of American Scientist's chemical and biological weapons program, and Dr. Milton Leitenberg, a microbiologist and senior fellow at the Center for International and Security Studies at the University of Maryland at College Park, offered their views that a mass casualty biological weapons attack (with 1,000 or more deaths) was not very likely at the moment due to the immense technical hurdles involved in acquiring, cultivating, and disseminating the agents.²⁹

Another challenge facing the IC deals with the alleged tendency of policymakers to exaggerate and/or misrepresent the available intelligence on a particular issue in order to justify certain policies. Journalists Kevin Whitelaw, Warren Strobel, and Brian Duffy contend that the U.S. bombing of a pharmaceutical plant in Sudan on August 20, 1998, though described by the Clinton Administration as a retaliatory measure against alleged terrorist Osama bin Laden's alleged involvement in the bombing of U.S. embassies in Africa earlier that month, was based on incomplete and inconclusive intelligence that proved neither bin Laden's involvement in the bombing, nor the complicity of the destroyed plant.³⁰ Instead, the

writers allege that the impetus for the bombing was nurtured by the staunch anti-Sudan policies in the State Department and National Security Council.³¹

Peter Pringle, a writer for *The London Sunday Times*, raises concerns that asymmetric defense policy may be the new vanguard program advocated by the defense establishment at the end of the Cold War nuclear era. He cites comments made by former Secretary of Defense William Cohen during a news conference in 1998, in which Cohen used a standard bag of sugar to demonstrate that the same amount of anthrax has the ability to kill half the population of Washington, DC, as an example of policymakers stoking the embers of public concern, even though these officials have little in the way of empirical and historical evidence to substantiate their positions.³² Pringle makes a similar case to that of Tucker and Sands, citing the frequency of hoaxes and false alarms in regard to suspected biological and chemical outbreaks.

For Pringle, Tucker and Sands, and others, there is concern that policymakers in the national security community may be overstating their assessments of the nature of the asymmetric threat in order to find ways to maintain and increase levels of defense spending during the yearly authorization/appropriation sessions with Congress. Certainly the 2001 version of the QDR moves in the direction of increased spending by the DoD in the area of Homeland Security, especially in regard to WMD attacks.³³

Contributing to these concerns is the growing possibility that the perspective of some policymakers may be influenced by information sources other than U.S. intelligence. Stephen Hall, science editor for *The New York Times Sunday Magazine*,

contends that the media fascination with the sensational aspects of the asymmetric threat may be leading policymakers who read media products on the subject to take certain positions on defense and prevention policies without paying enough attention to what intelligence agencies have to say on the matter.

Hall's point is simple: the profusion of movies, books, and media reports on biological and chemical weapon outbreaks, information warfare, and nuclear holocaust may be profitable for writers and producers of such media, but the storylines may not comport with reality.³⁴ No one is suggesting that these asymmetric challenges, especially biological weapons, should not be addressed, especially in the aftermath of the September 2001 attack and October 2001 rash of anthrax-tainted letters. However, balance provided by good intelligence is the key to effective policy decisions.

Unfortunately, intelligence agencies have to compete with open sources of information that purport to fill in information gaps with compelling conjecture. This is an interesting twist to the prominent use of OSINT by intelligence agencies, and requires that the agencies ask themselves certain questions regarding the process by which they collect, analyze, and disseminate their products. One such question regards the level of trust agencies accord the information they are collecting from open sources.

The agencies should also consider if they are creating an intelligence product more to compete for the policymaker's attention by overstating, or understating, a problem, rather than simply reporting what they know on a given subject.

In summary, the IC must guard against an overstatement of the actual severity of the security threats posed by asymmetric tactics. Commentators insisting that the actual possibility of an asymmetric attack against U.S. interests is small, based on the historical dearth of successful attacks, have cogent points to contribute.

However, these commentators would be the first to admit that history does not always portend the future as accurately as one might like. The fact remains that various entities around the world with the intent to harm U.S. interests may be developing their capabilities rapidly. In the words of NBC News correspondent Linda Fasulo:

Saddam Hussein possesses tons of chemical stocks despite the efforts of the U.N. Special Commission, or UNSCOM, which has found and destroyed 127,000 gallons of chemical agents. But inspectors cannot account for 600 tons of 'precursor' chemical that could be used to manufacture a 200-ton batch of VX, a nerve gas . . . UNSCOM knows even less about Iraq's biological weapons program, whose existence Baghdad did not acknowledge until August 1995. Iraq has since admitted producing 19,000 liters of botulinus, 8,400 liters of anthrax, and 2,000 liters of aflatoxin³⁵

In addition, according to Dr. Amy Smithson of the Stimson Center in Washington, DC, the CIA's Office of Technology Assessment has gone on record on several occasions to warn about the availability of information on the technical procedures for successful dissemination of a biological weapon.³⁶

U.S. intelligence needs to establish a clearer picture, a better guidepost, for policymakers in identifying the current field of threats, and, specifically, how much of the assessment of asymmetric threats is based on quantifiable data, and how much is predicated on speculation. Both sides in the debate have necessary points, but either extreme, a lax standard for asymmetric attack contingency policies, or an

overstatement of the perceptible nature of the threats, is not productive for the nation's security posture.

Given the existence of large stockpiles of biological weapons in the hands of entities hostile to U.S. interests, the fluidity of travel worldwide, the potential virulence of several biological weapons, the availability of dual use technologies for manufacturing these weapons in the United States, as well as the intent of terrorists to inflict harm on the civilian population, this thesis views biological weapons as a growing threat to U.S. national security. It does not, however, view the biological threat as likely to occur in the near term because of the technical hurdles mentioned previously.

Instead, bioterrorism, consisting of smaller scale attacks with biological toxins, and involving innovative delivery methods, like the U.S. Mail, will continue to constitute an immediate threat. The motivation for these attacks can range greatly depending upon the perpetrator(s). However, government preparation is necessary nonetheless.

Good intelligence in sizing up this fluid threat is crucial. OSINT can play a major role in this regard. Good intelligence can lead to good preparation for a bioterrorist attack, in regard especially to how the critical first responders – doctors, nurses, and EMTs respond in the critical first hours of a suspected bioterrorist attack. This section assumes preparedness is a necessity, and turns now to how to bring about greater national readiness.

Medical Response and Coordination

Reinvigorate the Public Health System

In the event of a biological weapon attack, rapid diagnosis and assessment of the infected population are crucial. Since some biological weapons like anthrax and smallpox mimic symptoms of the cold or flu in their early stages, the prevention of misdiagnosis is the first step in mitigating the effect of such an attack.

Only effective and rapid communication between healthcare workers at the frontline of an attack and experts on diagnosis of these pathogens can address the issue of misdiagnosis. Ideally, as the issue receives greater attention, mass-training exercises in diagnosing infection from bioterrorism will be the optimum way of addressing the current health care deficiencies.

Shortages in medical facility availability and emergency response personnel will take longer to correct. However, a well-coordinated system of communication and support from federal agencies in the event of a biological weapons outbreak can be addressed effectively in the near term.³⁷ Those making the early decisions in the medical community must have the ability to pick up the phone and consult with bioterrorism experts at any time. Measures are being undertaken as of this writing.

The CDC's National Center for Infectious Diseases is tweaking its Bioterrorism Preparedness and Response Program that is used to establish surveillance and communication between state and local health care communities and the CDC.³⁸

The CDC is also activating working relationships with public health laboratories that would be used to determine if a biological and/or chemical attack has occurred. This Laboratory Response Network (LRN) would work in collaboration with the Association of Public Health Laboratories, and the CDC's Rapid Response

and Advanced Technology Laboratory in order to provide a rapid analytical and epidemiological response to a possible outbreak.³⁹

Since it is a certainty that local health care providers will be overwhelmed by an attack, HHS has established the National Disaster Medical System. This system, comprised of 44 Disaster Medical Response Teams, stand ready to be deployed to the areas where outbreak has occurred. In addition, four National Medical Response Teams, which carry their own supplies of pharmaceuticals, can be deployed to areas where they can help in detection, treatment, and decontamination processes.⁴⁰ These HHS resources do not include the resources available from the EPA, FEMA, and DoD.

All these are productive steps that must be expedited in order to ensure the maximum level of health care and governmental response to an attack. Note, however, that it will take large quantities of both money and resolve to see the necessary improvements effectuated. For while the nation may be prepared for a minor to medium-sized biological weapons attack, it is doubtful that the existing infrastructure could handle even multiple minor biological attacks, let alone a variety of major epidemics occurring in succession.

Like intelligence, public health needs to be strengthened and given the resources to combat the major health crises of the twenty-first century. Recent years have seen a move toward privatization of health care, and a significant reduction in the resources devoted to public health. These developments must be reversed. The federal, state, and local governments must have control over the kinds of decisions

made by the health care community if they are to mount a successful response program to fallout from WMD attacks.⁴¹

Increase Pharmaceutical Stockpiles

The National Pharmaceutical Stockpile (NPS) is run by the CDC and includes vaccines, antidotes, and antibiotics that can be delivered rapidly to areas where a biological and/or chemical weapons attack has been detected. The NPS consists of materials divided into eight “12-hour Push Packages” that are located at specific areas throughout the nation and can be distributed to the areas in need within 12 hours.⁴² In 2001, the HHS finalized agreements with private vendors of additional pharmaceutical stockpiles known as Vendor Managed Inventory (VMI), and will be adding an additional four push packages in 2002.⁴³

Most potential germs that could be employed in a biological attack respond to the tetracycline family of antibiotics.⁴⁴ However, smallpox requires a vaccine that is low in supply. Last estimates place the stock of the vaccine between seven and fifteen million doses. As of September 29, 2001, the CDC had awarded contracts to two firms to produce an additional 40 million doses of smallpox vaccine, but these will not be available until mid-2004.⁴⁵ However, in congressional testimony on October 17, 2001, HHS Secretary Thompson announced that the CDC has expedited the smallpox vaccine program. The government will take delivery of to 300 million doses of the vaccine sometime in 2002.⁴⁶

Note also that, in the case of smallpox, there are likely not enough medicines available to treat a significant outbreak. Pharmaceutical manufacturers, however, are confident in their ability to provide enough antibiotics to treat other germ outbreaks,

like anthrax.⁴⁷ On September 26, 2001, BioPort Corporation of Lansing, Michigan admitted it's in discussion with the CDC, HHS, and FDA to begin mass-producing a national stockpile of anthrax vaccine.⁴⁸

Whether the government will have access to enough medical supplies or not (depending upon the germ used), the need to address these shortfalls in the stocking of these life-saving materials must be of the highest priority. The government must award multiple contracts and monetary incentives to the pharmaceutical companies responsible for the production of these medical resources. These contracts should be like the large conventional defense contracts awarded during the 1980s in order to ensure treatment coverage of the population.

Expand Funding for Bioterrorism Research

Federal funding for research into bioterrorism and ways in which to combat its germs increased 116 percent between 2000 and 2002. The federal budget put \$92.7 million toward research for new treatments of infection from biological weapons in its proposed FY 2002 budget, which was formulated before September 11, 2001.⁴⁹ The number should be increased in order to accelerate research of new treatments that might be more effective than standard pharmaceuticals.

In addition, the \$265.2 million per year biological and chemical weapons detection industry, which manufactures and sells equipment that can detect the presence of biological and/or chemical weapons in the air, should be given high priority by both government and private entities alike in the coming months.⁵⁰

Fortify Critical Infrastructure

Much focus has centered on the possibilities of an exotic future attack against the United States using a WMD. The previous portion of this section focused on threats of infrastructure using a chemical or biological weapon. However, given the difficulty in carrying out such an attack, terrorist entities might seek to continue using the proven methods of terror – conventional bombings and infrastructure disruption using computer hacking.⁵¹

Joint military and civilian test studies, like 1999's Zenith Star, found that the nation's power grids, utilities, and emergency response systems were susceptible to information warfare sabotage.⁵² These systems could be overwhelmed by bogus information fed into them by terrorists, or shut down completely by skilled hackers.

In addition, the nation's 103 nuclear power plants are not well prepared for terrorist strikes. The Nuclear Regulatory Commission admitted on September 26, 2001 that its plants are vulnerable to terrorist attack, especially from bombs and airliners crashing into the reactors.⁵³

The problems are not limited to the local and state governments. The federal government is having its own difficulties with keeping its many computer networks safe from terrorism, and even operational in the absence of a confirmed information warfare attack. For three days in 2000, the NSA computer network was out of operation, with old network mainframes the culprit. The agency claims that it is working on the problem by spending billions on upgrading its aged computer systems.⁵⁴

The solution in case of the power grids, emergency response and national surveillance computer systems is similar. More money needs to be allocated in order to keep pace with the technological changes that are occurring at a breakneck pace in the private sector.

These funds must be directed toward research and development of new technologies to protect military, government, and civilian computer and infrastructure networks from sabotage, and not the usual parochial department interests so prevalent in government. Money must also be allocated to provide for the establishment of back-up power grids and computer systems that can be brought on-line immediately, should a terrorist attack aimed at critical infrastructure targets occur.⁵⁵

Enact Civil Defense Training

The insidious nature of asymmetric warfare, and the immense freedoms under which U.S. citizens live, present daunting challenges for law enforcement, defense, public health, and intelligence agencies to handle. No matter how good any number of these professionals might be, there are too many targets, and too many people, to both protect and guard against. Thus, the American people must be utilized for what they are: the greatest untapped intelligence and prevention network available. Ashcroft said it well when he called public vigilance a “national neighborhood watch.”⁵⁶

If people were given basic training in how to be observant in their neighborhoods, places of work, houses of worship, and halls of recreation the possibility that perpetrators of asymmetric attack could continue their activities undetected would be diminished. Such training could be given under the auspices of

local law enforcement, and augmented by state and/or federal agencies with experts on how to spot and report specific suspicious activities.

This new kind of twenty-first century militia is called for under the principle of stewardship – each person has a responsibility to protect and care for the possessions he, his family, and his nation have been bestowed. Expecting help from the citizenry will establish a connection of personal ownership in the act of defense for the American people. This personal ownership in securing a strong defense for the homeland will likely serve to keep the public engaged in what is promised to be a protracted campaign.

Establish Clear and Consistent Communication

After announcing on October 4, 2001 that a man in Florida had tested positive for pulmonary (inhalational) anthrax poisoning, HHS Secretary Thompson took great pains to assure the nation that the case was an isolated incident, not related to a bioterrorist attack, and that the government was monitoring developments on the health front closely.⁵⁷

Unfortunately, Thompson's initial comments were wrong, and government officials have had some difficulty communicating accurate and consistent information to the public. Yet reassuring communication early on in a potential crisis situation might mean the difference between a population that begins to riot over fear of infection, and a nation that is able to receive information, instructions, and/or treatment in an orderly and effective fashion. It must be the number one policy of the crisis managers to make honest communication about a bioterror attack the first action in the response plan.

Hire Old Soviet Scientists and Put Them to Work

The greatest threat in terms of bioterrorism might not be from bin Laden, but from unemployed former Soviet scientists employed in biological weapons manufacturing facilities during the Cold War. If desperate, these scientists might be willing to sell their expertise to the highest bidder, possibly even terrorist networks.

Authors Judith Miller and William Broad state that Clinton encouraged U.S. and Russian scientists to work together on common medical issues, like gene sequencing, in order to add extra hands to the work, and keep track of what the Russian scientists were doing with their time.⁵⁸ If, as National Security Advisor Rice suggests, the United States and Russia are about to fundamentally alter their relationship and become closer, this might be the best opportunity yet to increase security and accountability on the part of Russian biotechnology.

Keep the National Focus on the True Source of Security

Consideration of the various policy changes and defense postures necessary to defend the United States from the specter of asymmetric attack cannot be complete, or even truly considered, without acknowledgement of the God that sustains and protects nations from the scourge of war and defeat. Patriotism is a unifying feeling for any nation, but it cannot be substituted for worship of and reliance on Almighty God.

Some might find this notion riddled with presupposition, and they would be correct in their conclusion. This thesis posits the presupposition that man cannot protect himself from the trials of pain and suffering, and he cannot prolong the inevitable reality that death will occur. The unfortunate events of September 11, 2001

prove this reality. Only through God's mercy, and a person's faith in Jesus Christ as Lord and Savior can there be found the kind of security for which every person, especially after 11 September 2001, longs.

The reliance on the Providence of God is not a new line of thought to the United States. Consider the words of Patrick Henry in 1775 as the colonies prepared to sacrifice for freedom. The words have as much to say in 2001, as they did in 1775:

Sir, we are not weak, if we make proper use of the means which the God of nature hath placed in our power. Three millions of people, armed in the Holy cause of Liberty, and in such a country as that which we possess, are invincible by any force which our enemy can send against us. Besides sir, we shall not fight our battle alone. There is a just God who presides over the destinies of nations; and who will raise up friends to fight our battle for us. The battle, sir, is not to the strong alone; it is to the vigilant, the active, the brave. .
59

Now consider the words of Presbyterian minister, educator, and signer of the Declaration of Independence, John Witherspoon:

It is in the man of piety and inward principle, that we may expect to find the uncorrupted patriot, the useful citizen, and the invincible soldier. God grant that in America true religion and civil liberty may be inseparable and that the unjust attempts to destroy the one, may in the issue tend to support the establishment of both.⁶⁰

Dutch Reformed theologian, educator, and statesman Abraham Kuyper considered recognition of Christ's Lordship over the earth as central to personal, and national strength and greatness. His admiration of the United States mirrored that of de Tocqueville; he was convinced that Christianity must be the central force that guides any society. He wrote in 1880: "There is not a square inch in the whole domain of our human experience over which Christ, who is Sovereign over all, does not cry, 'Mine!'"⁶¹

The United States has no hope for a sound national security against asymmetric threats, if it does not recognize the source of all security – Jesus Christ. This war against terrorism leaves no room for equivocation. It is a contrast between good and evil, and those on the side of good can only remain righteous if they recognize Christ’s Lordship in their endeavors.

Conclusions

As this thesis has demonstrated, asymmetric threats are part of the new reality of American life. It is virtually certain that they will disrupt the flow of daily life in the future, since the nation's vulnerabilities are too tempting for terrorists to ignore. Horrifying as the recent attacks were, however, they were also helpful. The United States has been given notice that it must be more serious about domestic security.

With that said, the nation must be careful not to over exaggerate some threats because of their exotic nature, especially in the area of biological and/or chemical weapons. There will be a growing threat of bioterrorism, as the anthrax letters demonstrate, but the government's resolve to improve its ability to address this threat is heartening. This kind of quick policy response must also be used to address other potentially destructive forms of asymmetric warfare, whether there is a media frenzy surrounding them or not.

Asymmetric threats will take some time to get used to, especially for a nation raised on the idea of war as relatively short, and fought by conventional means on someone else's property. The United States has the ability to overcome this new challenge, but it will not be successful unless it has fortitude, foresight, and, most importantly, faith in the Almighty.

NOTES

Section One

1. James Adams, "Virtual Defense," *Foreign Affairs*, May- June 2001, 105.
2. U.S. Department of Defense, "Quadrennial Defense Review," 30 September 2001, <http://www.defenselink.mil>.
3. Bruce Hoffman and Jennifer Morrison Taw, *A Strategic Framework for Countering Terrorism and Insurgency* (Santa Monica: Rand, 1992), 136-140.
4. Jonathan Tucker, interview with NBC News, WNBC-TV, New York, NY, 2 October 2001.
5. *The New York Times* (New York, NY), 3 October 2001.
6. Ibid.
7. Gilmore Commission Second Annual Report to Congress, "Second Annual Report List of Key Recommendations," online transcript, Rand Website: 15 December 2000, <http://www.rand.org/nsrd/terrpanel/recommendations.html>.
8. *The Washington Times* (Washington, DC), 22 September 2001.
9. Adams.
10. Secretary of Defense Donald H. Rumsfeld, "DoD News Briefing," *DefenseLink: U.S. Department of Defense News Transcript* 12 September 2001, 14 September 2001, http://www.defenselink.mil/news/Sep2001/t09122001_t0912sd.html.
11. James Clavell, ed., *The Art of War*, by Sun Tzu (New York: Bantam Doubleday Dell Publishing Group, Inc., 1983), 11.
12. Henry Kissinger, *Diplomacy* (New York City: Touchstone, 1994), Chapter Thirty One.
13. Amos A. Jordan, William J. Taylor, Jr., and Michael J. Mazarr *American National Security*, 5th ed., (Baltimore: The Johns Hopkins University Press, 1999).
14. Clavell, 11.
15. Jonathan Tucker, ed., *Toxic Terror: Assessing Terrorist Use of Biological and Chemical Weapons* (Cambridge: MIT Press, 2000), 3.
16. Lee Waters, "Chemical Weapons in the Iran/Iraq War," *Military*

Review, Vol. 70, No. 10 (October 1990), 57-63.

17. Cindy C. Combs, *Terrorism in the Twenty-First Century*, 2nd ed., (Upper Saddle River: Prentice Hall, 2000), 8.

18. *Ibid.*, 222.

19. *Ibid.*, 12.

20. *Ibid.*, 223.

21. *Ibid.*, 22.

22. *Ibid.*, 77.

23. *Ibid.*, 41.

24. *Ibid.*, 42.

25. *Ibid.*

26. *Ibid.*, 43.

27. Brian Jenkins, interview with Tony Snow, Fox News, WNYW-TV, New York, NY, 15 September 2001.

28. *Ibid.*

29. Edgar O' Ballance, *The Language of Violence: The Blood Politics of Terrorism* (San Rafael: Presidio Press, 1979), 300-301.

30. The United States House of Representatives Subcommittee on Economic Development, Public Buildings, & Emergency Management, "Combating Terrorism: Options to Improve the Federal Response," online transcript, 24 April 2001, 17 September 2001, <http://www.house.gov/transportation/pbed/04-24-01/01-24/01memo.html>.

31. *Ibid.*

32. *The New York Times* (New York, NY), 22 January 1999.

33. George C. Wilson, *This War Really Matters: The Inside Fight for Defense Dollars* (Washington: CQ Press, 2000), 177.

33. House Subcommittee on Combating Terrorism.

34. *The New York Times* (New York, NY), 30 September 2001.
35. Department of Defense Budget, Fiscal Year 2001, class hand-out, "U.S. National Defense Policy," Dr. Richard Kilroy, October 2000.
36. Donald H. Rumsfeld, letter, *The New York Times* 27 September 2001, <http://www.nytimes.com/2001/09/27/opinion/27RUMS.html?ex=1002612722&ei=1&en=84881793fb0244d>.
37. *Foreign Affairs*, January-February 2001.
39. Class Notes, "U.S. National Defense Policy," Dr. Richard C. Kilroy, October 2000.
40. "Quadrennial Defense Review"
41. Delaware Senator Joseph Biden, interview with Peter Jennings, ABC News, WPVI-TV, Philadelphia, PA, 13 September 2001.
42. *The Washington Post* (Washington, DC), 7 September 2001.
43. Ibid.
44. *The Washington Times* (Washington, DC), 13 September 2001.
45. *The Washington Post* (Washington, DC) 7 September 2001.

Section Two

1. Annual Report to Congress on Combating Terrorism: Including Defense Against Weapons of Mass Destruction/Domestic Preparedness and Critical Infrastructure Protection, May 18, 2000.
2. Steve Milloy, "Smallpox Attack Exaggerated," Fox News, 5 October 2001, www.foxnews.com.
3. Michael T. Osterholm and John Schwartz, *Living Terrors: What America Needs to Know to Survive the Coming Bioterrorist Catastrophe* (New York: Delacorte Press, 2000), 15.
4. Ibid.
5. Gerard J. Tortora, Berdell R. Funke, and Christine L. Case, *Microbiology: An Introduction*, 6th ed., (New York: Addison Wesley Longman, 1998), 98.

6. Osterholm, 14.
7. Medscape, "Citywide Pharmaceutical Preparation for Bioterrorism," Medscape Internet Site, 2001, 17 September 2001, <http://www.medscape.com/ASHP/AJHP/2001/v58.n03/ajhp5803.03.../ajhp5803.03.terr-08.htm>.
8. Ibid.
9. Ibid.
10. Ken Alibek, *Biohazard: The Chilling True Story of the Largest Covert Biological Weapons Program in the World – Told From Inside By the Man Who Ran It* (New York: St. Martin's Press, 2000), 395.
11. Richard Butler, *The Greatest Threat: Iraq, Weapons of Mass Destruction, and the Crisis of Global Security* (New York, PublicAffairs, 2000), 169.
12. Donald Kagan and Frederick W. Kagan, *While America Sleeps: Self-Delusion, Military Weakness, and the Threat to Peace Today* (New York: St. Martin's Press, 2000), 395.
13. *The Washington Post* (Washington, DC.), 25 May 2000.
14. Steve Fetter, "Ballistic Missiles and Weapons of Mass Destruction: What is the Threat? What Should Be Done?" *International Security* 16, no. 1 (1991), 5-42.
15. Osterholm, 10-22.
16. Judith Miller, Stephen Engelberg, and William Broad, *Germes: Biological Weapons and America's Secret War* (New York: Simon and Schuster, 2001), 270-77.
17. Peter R. Lavoy, Scott D. Sagan, and James Wirtz, eds., *Planning The Unthinkable: How New Powers Will Use Nuclear, Biological, and Chemical Weapons* (New York: Cornell University Press, 2000), Introduction.
18. Ibid.
19. Ibid.
20. Cindy C. Combs, *Terrorism in the Twenty-First Century*, 2nd ed., (Upper Saddle River. Prentice Hall, 2000), 77.
21. *London Sunday Telegraph* (London, England), 16 September 2001.

22. Lavoy, Introduction.
23. *Toxic Terror: Assessing the Terrorist Use of Chemical and Biological Weapons*, ed. Jonathan B. Tucker (Cambridge: MIT Press, 2000), 37-60, 170-217.
24. Ibid.
25. Ibid.
26. Lavoy, Introduction.
27. Ibid.
28. Ibid.
29. *The Washington Times* (Washington, DC), 15 September 2001.
30. *The New York Times* (New York, NY), 4 October 2001.
31. "U.S. Concerned About Reports of Plutonium In North Korea," CNN, 19 November 1998, www.cnn.com.
31. Scott Parish and John Lepingwell, "Are Suitcase Nukes On the Loose? The Story Behind the Controversy," *CNS Reports* (1997), 7 September 2001, <http://cns.miis.edu/pubs/reports/lebedst.htm>.
32. Combs, 9-16.
33. James Adams, "Virtual Defense," *Foreign Affairs*, May-June 2001, 105.
34. *The Washington Post* (Washington, DC), 6 September 2001.
35. *The Washington Times* (Washington, DC), 22 June 2001.
36. Michael Erbschloe, *Information Warfare: How To Survive Cyber Attacks* (New York: McGraw Hill, 2001),
37. Ibid.
38. Ibid.
39. Ibid.
40. Ibid.

41. *Associated Press Wire*, 24 July 2001, www.ap.org.
42. Adams.
43. Ibid.
44. LTC Vic Salazar, USA, personal interview, 6 September 2001.
45. National Defense University, *McNair Paper 62, The Revenge of the Melians: Asymmetric Threats and the Next QDR*, (Washington, DC, National Defense University, 2000), Chapter Three.
46. Ibid.
47. Ibid.
48. Ibid.
49. Ibid.
50. "A National Security Strategy for a New Century," The White House, Office of the Press Secretary, Washington, DC, 1999, iii.
51. Osterholm, 161.
52. Ibid.
53. "U.S. Code Title 10," Cornell University Law School Legal Information Institute, 20 September 2001, <http://www4.law.cornell.edu/uscode/10/-3k>.
54. Osterholm, 158.
55. Ibid, 159.
56. *Associated Press Wire*, 5 February 2001, <http://www.ap.org>.
57. Osterholm, 15.
58. John G. Bartlett, "Applying Lessons Learned from Anthrax Case History to Other Scenarios," *Emerging Infectious Diseases*, vol. 5, no.4 (July-August 1999).
59. Ibid.
60. Ibid.

61. Ibid.

62. Paul R. Bremer, "New Terrorist Threats and How To Counter Them" (paper presented at the Heritage Foundation Lecture, Washington, DC, 12 July 2000), <http://heritage.org/library/lecture/hl678.html>; Defense Advanced Research Projects Agency, Joint Forces Staff College e-mail information, 7 January 2001.

63. Alexander Hamilton, James Madison, and John Jay, *The Federalist Papers*, ed. Clinton Rossiter (New York: Penguin Putnam, 1999), 225.

Section Three

1. "The News With Brian Williams," MSNBC, 25 June 2001.

2. Pat M. Holt, *Secret Intelligence and Public Policy: A Dilemma of Democracy* (Washington, DC: CQ Press, 1995), 21.

3. Ibid.

4. Ibid., 22.

5. Ibid.

6. Ibid.

7. Ibid., 23.

8. Ibid., 24.

9. Ibid., 27.

10. Ibid., 28.

11. Ibid.

12. Amos A. Jordan, William J. Taylor, Jr., Michael J. Mazarr, *American National Security*, 5th ed., (Baltimore: The Johns Hopkins University Press, 1999), 87.

13. Statement Before the Senate Select Committee on Intelligence given by Vice Admiral Thomas R. Wilson Director, Defense Intelligence Agency, "Military Threats and Security Challenges Through 2015," United States Senate Select Committee on Intelligence, online transcript, 2 February 2000, <http://intelligence.senate.gov/0002hrg/000202/wilson.htm>.

14. Ibid.

15. Ibid.
820. 16. Henry Kissinger, *Diplomacy* (New York: Simon and Schuster, 1994),
17. Holt, 44.
18. "United States Intelligence Community," organization description, *Office of the Directorate of Central Intelligence*, 25 June 2001, <http://www.odci.gov/ic.html>.
19. Holt, 44.
20. Arthur S. Hulnick, *Fixing The Spy Machine: Preparing American Intelligence For the Twenty-First Century* (Westport, Praeger Publishers, 1999), 50.
21. <http://www.odci.gov/ic.html>.
22. Holt, 48.
23. <http://www.odci.gov/ic.html>.
24. Holt, 49.
25. Ibid.
26. Ibid.
27. Hulnick, 51.
28. "Intelligence Agencies – Collection," description of intelligence disciplines, *MILNET*, 20 June 2001, <http://www.milnet.com/milnet/collecti.htm>.
29. Hulnick, 10.
30. Ibid., 23.
31. Ibid., 28.
32. Holt, 57.
33. Ibid., 68.
34. Ibid.
35. Hulnick, 16.

36. Holt, 69.
37. Hulnick, 16.
38. Henry Kissinger, *Years of Renewal: The Concluding Volume of His Memoirs* (New York: Simon and Schuster, 1999), 316.
39. Holt, 45.
40. Ibid., 4.
41. Hulnick, 15.
42. James Adams, "Virtual Defense," *Foreign Affairs*, May-June 2001: 104.
43. Ibid.
44. Ibid.
45. Ibid.
46. Hulnick, 135.
47. Ibid.
48. Holt, 114.
49. Ibid., 115.
50. *The Washington Times* (Washington, DC), 14 June 2001.
51. Hulnick, 148.
52. Ibid., 24
53. Ibid., 25.
54. Ibid.
55. Ibid., 147.
56. Holt, 43.
57. Ibid., 202.
58. Ibid., 204.

59. **Ibid.**
60. **Ibid., 45.**
61. **Ibid., 190.**
62. **Ibid., 191.**
63. **Ibid., 201.**
64. **Ibid.**
65. **Hulnick, 57.**
66. **Ibid., 54.**
67. **Ibid., 51.**
68. **Ibid., 55.**
69. **Ibid., 45.**
70. **Ibid., 56.**
71. **Holt, 210.**
72. **Ibid., 217.**
73. **Ibid., 222.**
74. **Ibid., 230.**
75. **Ibid., 232.**
76. **Hulnick, 58.**
77. **Holt., 104**
78. **Hulnick, 59.**
79. **Ibid., 60.**
80. **Ibid.**
81. ***The Los Angeles Times (Los Angeles, CA), 20 June 2001.***

82. "The News With Brian Williams," MSNBC, 22 June 2001.
83. Jordan, 146.
84. Ibid.
85. "Urge Congress to Stop the FBI's Use of Privacy-Invading Software," website article, *American Civil Liberties Union Freedom Network* 23 April 2001, <http://www.aclu.org/action/carnivore107.html>.
86. Ibid.
87. Ibid.
88. "Cyber-Rights Groups Join Forces to Oppose Anti-Privacy Cybercrime Treaty," website article, *American Civil Liberties Union Freedom Network* 23 April 2001, <http://www.aclu.org.news/200/n121300.html>.
89. *National Review* (Washington, DC), 23 August 2000.
90. Adams, 110.
91. *The New York Times* (New York, NY), 11 June 2001.
92. Holt, 171.
93. Ibid.
94. Ibid., 180.
95. Ibid., 179.
96. Ibid., 186.
97. Hulnick, 3.
98. Fox News Live Coverage, 15 September 2001
99. Karen Ann Coburn, "Local Government's Responses to Biological and Chemical Terrorism," *At Issue: Biological And Chemical Weapons* (San Diego: Greenhaven Press, 2001), 84.
100. Ibid.
101. Ibid., 85.

102. Ibid.
103. Richard K. Betts, "Biological Weapons Are a Serious Threat," *At Issue: Biological And Chemical Weapons* (San Diego: Greenhaven Press, 2001), 18.
104. Coburn, 86.
105. James Adams, "Virtual Defense," *Foreign Affairs*, May-June 2001, 105.
106. Ibid., 108.
107. Pringle, 24.
108. Ibid., 26.
109. Frank J. Gaffney, Jr., "The Chemical Weapons Convention Is Unenforceable," *At Issue: Biological And Chemical Weapons* (San Diego: Greenhaven Press, 2001), 81.
110. Ibid., 76.
111. Ibid., 77.
112. Ibid., 82.
113. Ely Karmon, "The Role of Intelligence Communities In The Fight Against New Forms of International Terrorism," Conference in Italy on "Intelligence in the Twenty-First Century," Priverno, 14-16 February 2001.
114. *The Washington Times* (Washington, DC), 11 June 2001.
115. *The London Times* (London, England), 15 September 2001.
116. "ECHELON: America's Secret Global Surveillance Network," ed. Patrick S. Poole, 1999, 23 July 2001, <http://home.hiwaay.net/~pspoole/echelon.html>.
117. "Statement Before the Senate Select Committee on Intelligence given by Vice Admiral Thomas R. Wilson Director, Defense Intelligence Agency: Military Threats and Security Challenges Through 2015," United States Select Committee on Intelligence, transcript, 2 February 2000, <http://intelligence.senate.gov/0002hr/000202/wilson.htm>.
118. Karmon, 2.

Section Four

1. *The New York Times* (New York, NY), 21 September 2001.
2. Mayor Rudolph W. Giuliani, interview with Tim Russert, CNBC, New York City, 22 September 2001.
3. Dr. Michael S. Ascher, California Department of Health Services, *Rand Conference On Bioterrorism: Coordination Among Government Agencies* (Rand, 2000).
4. Brian Jenkins, interview with Tony Snow, Fox News Channel, Washington, DC, 15 September 2001.
5. Gilmore Commission Second Annual Report to Congress, "Second Annual Report List of Key Recommendations," online transcript, Rand Website: 15 December 2000, <http://www.rand.org/nsrd/terrpanel/recommendations.html>.
6. CNN Live Coverage of Attorney General John Ashcroft's Congressional Testimony, CNN, Washington, DC, 24 September 2001.
7. *The New York Times* (New York, NY), 18 September 2001.
8. *The Washington Post* (Washington, DC), 26 September 2001.
9. Virginia Governor James S. Gilmore III, interview with C-SPAN, Alexandria, Virginia, 17 September 2001.
10. *The New York Times* (New York, NY), 18 September 2001.
11. *The Washington Times* (Washington, DC), 22 September 2001.
12. "Likelihood Terrorists Can Acquire and Use Chemical or Biological Weapons," ed. Dr. Amy E. Smithson, September 2001, The Henry L. Stimson Center Chemical and Biological Weapons Nonproliferation Project, online journal, Washington, DC, 28 September 2001, <http://www.stimson.org/cwc.htm>.
13. *Ibid.*
14. *The Washington Post* (Washington, DC), 28 September 2001.
15. United States Attorney General John Ashcroft, Statement Before The United States Senate Committee On Appropriations Subcommittee On Commerce, Justice, and State, The Judiciary and Related Agencies, online transcript, 26 April 2001, <http://www.senate.gov/~appropriations/commerce/testimony/ascrft42601.htm>.

16. Keith J. Costa, "Hart-Rudman Calls for Homeland Defense: The Commission Predicts A Direct Attack On The United States," *Air Force Magazine: Journal of the Air Force Association* (April 2001), 16 September 2001, [http://www.afa.org/magazine/April 2001/0401hart.html](http://www.afa.org/magazine/April%202001/0401hart.html).
17. *The Washington Post* (Washington, DC), 26 September 2001.
18. Ibid.
19. Ibid.
20. *The Washington Post* (Washington, DC), 22 September 2001.
21. *The Washington Times* (Washington, DC) 22 September 2001.
22. MSNBC Live Coverage: "America On Alert," 24 September 2001
23. Jonathan B. Tucker and Amy Sands, "Terrorists Would Be Unlikely to Use Biological or Chemical Weapons," *At Issue: Biological And Chemical Weapons* (San Diego: Greenhaven Press, 2001), 33.
24. Ibid.
25. *The New York Times* (New York, NY), 17 September 2000.
26. *The New York Times* (New York, NY), 19 September 1999.
27. Tucker and Sands, 30.
28. *The Wall Street Journal* (New York, NY), 25 September 2001.
29. Fox News Channel Live Coverage, 25 September 2001.
30. *U.S. News and World Report* (New York, NY), 16-23 August 1999.
31. Ibid.
32. Peter Pringle, "Is the Fear Of Biological Terrorism Justified?," *At Issue: Biological And Chemical Weapons* (San Diego: Greenhaven Press, 2001), 24.
33. U.S. Department of Defense, "Quadrennial Defense Review," 30 September 2001, <http://www.defenselink.mil>.
34. Stephen S. Hall, "The Media Direct U.S. Policy Regarding Biological and Chemical Weapons," *At Issue: Biological And Chemical Weapons* (San Diego: Greenhaven Press, 2001), 44.

35. Bruce B. Auster and Linda Fasulo, "Iraq Still Possesses a Biological and Chemical Arsenal," *At Issue: Biological And Chemical Weapons* (San Diego: Greenhaven Press, 2001), 94
36. *The Washington Times* (Washington, DC) 6 September 2001.
37. Anthony G. Macintyre, M.D., "Weapons of Mass Destruction Events with Contaminated Casualties – Planning for Health Care Facilities," *Journal of the American Medical Association*, no. 263 January 2000: 242-249.
38. Secretary of the Department of Health and Human Services Tommy Thompson, Statement Before The United States Senate Committee On Appropriations Subcommittee On Commerce, Justice, State, The Judiciary and Related Agencies, online transcript, 9 May 2001, <http://www.senate.gov/~appropriations/commerce/testimony/thompterr.htm>.
39. Ibid.
40. Ibid.
41. Dennis A. Henderson, Director of the Johns Hopkins Center for Civilian Biodefense Studies, interview with Michelle Williams, *Associated Press*, 5 February 2001.
42. Thompson Subcommittee Testimony.
43. Ibid.
44. Centers For Disease Control and Prevention (CDC), "National Pharmaceutical Stockpile Synopsis: A National Repository of Life-Saving Pharmaceuticals and Medical Material," online journal, Atlanta: CDC, 2001, <http://www.cdc.gov/nceh/nps/synopses.htm>.
45. *The Washington Post* (Washington, DC), 17 September 2001.
46. HHS Secretary Tommy Thompson, interview with Mike Wallace, "60 Minutes," CBS News, WKYW-TV, Philadelphia, 30 September 2001.
47. Kim Brennen Root, Spokeswoman for BioPort, interview with Reuters Limited, 26 September 2001.
48. Ibid.
49. *The Boston Globe* (Boston, MA), 29 August 2001.

50. "Analyst Predicts Growth For Weapons Detection Industry," *San Antonio Business Journal: The Essential Business Tool* 22 August 2001, 20 September 2001, <http://sanantonio.bcentral.com/sanantonio/stories/2001/08/20/daily14.html>.
51. Henry L. Hinton, Jr., Assistant Comptroller General, National Security and International Affairs Division, U.S. General Accounting Office, Testimony Before The U.S. House of Representatives Subcommittee on National Security, Veteran's Affairs, and International Relations, Committee on Government Reform, online transcript, 11 March 1999, <http://www.house.gov/reform/ns/press/test1.htm>.
52. Robert Lowry, "Information Warfare: Choose Your Weapon In The New Century, Wars Will Be Waged In Cyberspace, Biological Threats Will Be Replaced By Computer Viruses And E-Mail May Prove To Be A Lethal Weapon," *Global News Wire*, 1 December 2000, Lexus-Nexus Academic Universe.
53. *The Washington Times* (Washington, DC), 27 September 2001.
54. *Los Angeles Times* (Los Angeles, CA), 19 September 2001.
55. Gilmore Commission Second Annual Report To Congress.
56. MSNBC Live Coverage of Attorney General John Ashcroft's Press Conference, MSNBC, Washington, DC, 28 September 2001.
57. *The New York Times* (New York, NY), 5 October 2001.
58. Judith Miller, Stephen Engelberg, and William Broad, *Germs: Biological Weapons and America's Secret War* (New York: Simon and Schuster, 2001), 209.
59. Dr. K. Alan Snyder, "Great Quotes by Patrick Henry," 27 September 2001, <http://www.snyders.ws/alan/quotes/henry.htm>.
60. Dr. K. Alan Snyder, "Great Quotes by John Witherspoon," 27 September 2001, <http://www.snyders.ws/alan/quotes/witherspoon.htm>.
61. John Bolt, *Abraham Kuyper's American Public Theology* (Grand Rapids: Wm. B. Eerdmans Publishing Company, 2001), v.

SELECTIVE BIBLIOGRAPHY

- Alibek, Ken. *Biohazard: The Chilling True Story of the Largest Covert Biological Weapons Program in the World – Told From Inside by the Man Who Ran It*. New York: Random House, 1999.
- Bom, Philip. *The Coming Century of Commonism: The Beauty and the Beast of Global Governance*. Virginia Beach: Policy Books, Inc., 1992.
- Bracken, Paul. *Fire In The East: The Rise of Asian Military Power and the Second Nuclear Age*. New York: HarperCollins, 1999.
- Bush, George, and Brent Scowcroft. *A World Transformed*. New York: Random House, Inc., 1998.
- Butler, Richard. *The Greatest Threat: Iraq, Weapons of Mass Destruction, and The Crisis of Global Security*. New York: Public Affairs, 2000.
- Cimbala, Stephen, ed. *Clinton and Post-Cold War Defense*. Westport: Praeger, 1996.
- Combs, Cindy. *Terrorism in the Twenty-First Century*, 2d ed. Upper Saddle River: Prentice Hall, 2000.
- Connell, Jon. *The New Maginot Line: A Documented Exposé Of Our Fatally Flawed Defense System and What We Can Do About It*. New York: Arbor House, 1986.
- Erbschole, Michael. *Information Warfare: How to Survive Cyber Attacks*. New York: McGraw-Hill, 2001.
- Gaddis, John Lewis. *The United States and the End of the Cold War: Implications, Reconsiderations, Provocations*. New York: Oxford University Press, 1992.
- Gray, Chris Hables. *Postmodern War: The New Politics of Conflict*. New York: Guilford Press, 1997.
- Hamza, Khidhir. *Saddam's Bombmaker: The Terrifying Inside Story of the Iraqi Nuclear and Biological Weapons Agenda*. New York: Scribner, 2000.
- Holt, Pat. *Secret Intelligence and Public Policy: A Dilemma of Democracy*. Washington, D.C.: CQ Press, 1995.

- Hulnick, Arthur. *Fixing The Spy Machine: Preparing American Intelligence for The Twenty-First Century*. Westport, Praeger, 1999.
- Jordan, Amos, William J. Taylor, and Michael J. Mazarr. *American National Security*, 5th ed. Baltimore: The Johns Hopkins University Press, 1999.
- Kagan, Donald, and Frederick W. Kagan. *While America Sleeps: Self-Delusion, Military Weakness, and the Threat to Peace Today*. New York: St. Martin's Press, 2000.
- Kissinger, Henry. *Diplomacy*. New York: Simon and Schuster, 1994.
- Kolata, Gina. *Flu: The Story of the Great Influenza Pandemic of 1918 and the Search for the Virus That Caused It*. New York: Simon and Schuster, 1999.
- Lavoy, Peter, Scott D. Sagan, and James J. Wirtz, eds. *Planning The Unthinkable: How New Powers Will Use Nuclear, Biological, and Chemical Weapons*. Ithaca: Cornell University Press, 2000.
- Leonhard, Robert. *The Principles of War for the Information Age*. Novato: Presidio Press, Inc., 2000.
- Lugo, Luis E., ed. *Religion, Pluralism, and Public Life: Abraham Kuyper's Legacy for the Twenty-First Century*. Grand Rapids: William B. Eerdmans Publishing Company, 2000.
- Miller, Judith, Stephen Engleberg, and William Broad. *Germs: Biological Weapons And America's Secret War*. New York: Simon and Schuster, 2001.
- Netanyahu, Benjamin. *Fighting Terrorism*. New York: Farrar, Straus, and Giroux Inc, 1997.
- Osterholm, Michael, and John Schwartz. *Living Terrors: What America Needs to Know to Survive The Coming Bioterrorist Catastrophe*. New York: Delacorte Press, 2000.
- Richelson, Jeffrey. *The U.S. Intelligence Community*, 4th ed. Boulder: Westview Press, 1999.

VITA

Brian Robert Calfano was born on January 14, 1977 in Evesham Township, New Jersey. He was raised in Trenton, New Jersey, and attended high school at Hamilton High School West.

He studied musical theater, radio/TV production, and classical voice in college before entering Rider University's Department of Political Science in January 1999. In May 2000, he defended successfully an undergraduate honors thesis on the Christian Right and American Politics. In August 2000, he graduated *Summa Cum Laude* and with honors in political science from Rider University in Lawrenceville, New Jersey.

In August 2000, he entered the School of Government of Regent University in Virginia Beach, Virginia. His graduate accomplishments include a published book review on asymmetric security threats, as well as a research internship at the Joint Forces Staff College of National Defense University in Norfolk, Virginia.

In May 2002, with a cumulative GPA of 4.0, he graduated Regent University with an MA in Public Policy. Brian resides currently in Fort Worth, Texas, and is working on a Ph.D. in political science at the University of North Texas.