

AU/AFFP/MIAMI/2002

AIR FORCE FELLOWS PROGRAM

AIR UNIVERSITY

**COUNTER-BIOTERRORISM US
INTELLIGENCE CHALLENGES**

by

Howard Kirk Mardis, Lt Col, USAF

A Research Report Submitted to the Faculty
In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Susan Martin

Maxwell Air Force Base, Alabama

April 2002

Distribution A: Approved for public release; distribution is unlimited

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Table of Content

Contents	Page
Disclaimer	ii
Tables	vi
Preface	vii
Abstract	viii
Introduction and Overview	1
The Counter-Bioterrorism Mission Thread	2
Background	5
What Are Biological Weapons	5
Biological Weapon Liabilities	7
History of Biological Warfare	8
More Recent Biological Weapon Concerns	9
The Bioterrorism Process	11
Bioterrorism Threat: Issues for Analysis	17
Analysis of Threat is Limited	17
Developing BW Capability is Getting Easier for Terrorist	18
Changing Face of Terrorism: Impact on Bioterrorism	19
Trends in Terrorism	19
Bioterrorist Groups: What Makes Them Different	20
Biological Weapons Convention and State Programs: Intelligence and Bioterrorism	
Implications	22
State Programs: Key to Bioterrorism	23

BWC Impact on State Deterrence and Intelligence	24
BWC Inspection Could Help Thwart Bioterrorism	25
Bioterrorism: Weapon of Mass Destruction or Disruption?	26
Intelligence Community at a Crossroad	31
Transnational Threats: Top Intelligence Priority	31
Community Under Attack	32
Must Understand Capabilities and Intentions	34
Breaking Community Organizational Barriers	35
Improvements to Intelligence Foundation	39
Customer Relationship Challenges	39
Information Management Initiatives	41
Need for New Information Structure	42
Need For Dedicated Information Managers	44
Information Brokers	46
Human Resource Challenges	47
Functional Intelligence Improvements for Transnational Challenges	53
Collection Challenges	53
Surprise! HUMINT is Critical	54
Super Collection Managers	56
Analytical Challenges	57
Leveraging Outside Expertise	57
Tools to Do the Job	60
Background Intelligence	61

Cultural Intelligence	62
Credit for Continuous Customer Collaboration Reporting Stats	63
Open Source Intelligence: Underutilized Source	64
Recommendations	69
US Response and Intelligence Community Recommendations	69
Reorganization	69
Mission Thread-Centric	69
Fighting the Barriers	70
Information Management Transformation	70
Innovative Human Resource Management	70
Open Source Integration	70
Intentions are Key to Deterrence	71
Integrated HUMINT	71
Summary and Conclusions	72
Real Threat	72
Intelligence is Key to Counter-Bioterrorism	72
There Are No Silver Bullets	73
Glossary	75
Bibliography	76

Tables

Page

Table 1: Characteristics of Biological Warfare Agents 6

Preface

This paper reviews some of the major counter-bioterrorism challenges the US intelligence community currently faces. It also provides background on biological weapons and bioterrorism useful to understanding intelligence challenges. I chose to research and write about this topic because the threat of bioterrorism poses one of the greatest challenges to the future of US national security. Equally important is my conviction that US intelligence can play a decisive role in helping to deter and if necessary preempt bioterrorist acts. In reviewing the threat and associated community challenges, I hope to offer some useful background material and practical recommendations to intelligence and policy leaders that will help make US intelligence more effective in fighting transnational issues like bioterrorism. I am also firmly convinced that deterring and preventing bioterrorist attacks should be one of the top priorities of the US intelligence community.

First and foremost I would like to thank my advisor, Dr. Susan Martin, for her tireless guidance and exceptional support. I would also like to thank several of my intelligence community peers, who will remain nameless for security reasons, for their assistance despite wartime schedules. I would also like to thank Ms Patrice Morgan for editing assistance and excellent suggestions for improving this paper. I could not have completed this project without the unparalleled support from Dr. Andy Gomez, Dean, School of International Studies, University of Miami. Finally, I would like to thank my wife Yvette and daughter Haley for their support on the home front, without which I could not have undertaken and completed this research project.

Abstract

This paper discusses challenges the US intelligence community faces in helping to counter bioterrorism—a real and emerging threat that has the potential to cause mass destruction in the United States. It includes background material on a number of issues related to the threat of bioterrorism to help the reader understand why the bioterrorism threat is real, why it may be growing, and why it could potentially inflict mass destruction. As part of this process the paper reviews key factors associated with bioterrorism threat analysis.

This paper argues that US intelligence is at a crossroad, facing a number of challenges including the need to improve its foundation. To make the system more dynamic and efficient, the intelligence community needs to foster a more innovative customer-relationship management system and adopt more aggressive information management and human resource management strategies. Improvements in these key areas of the intelligence foundation will lead to enhancements in a wide variety of intelligence missions—not simply counter-bioterrorism. When faced with transnational issues like bioterrorism, this paper recommends that the community needs to be more focused on contributing to the success of specific mission threads, as opposed to a myopic focus on individual organizational success. A focus on applying organizational expertise and talents to specific mission threads, like bioterrorism, will serve as a catalyst to meaningful improvements in to traditional intelligence collection and analytical functions. It will also lead to smart incorporation of new intelligence procedures and ideas such as harnessing the potential of Open Source Intelligence.

This paper argues that collectively addressing these challenges will allow the intelligence community to focus more effectively on emerging threats and help deter and, if necessary, preempt bioterrorist attacks. It contains recommendations on enhancing intelligence areas to help counter any future bioterrorist more effectively. These improvements will not only enhance the counter-bioterrorism mission but many will directly benefit other intelligence missions.

Comprehensive review of some specific intelligence issues, especially those involving collection sources and methods, was not possible in an unclassified study.

Chapter 1

Introduction and Overview

The United States stands alone as the world's sole superpower in post the Cold War international security environment. Its military, economic, and political power is unparalleled on the world stage. Despite its dominating global position, the events of 9/11 demonstrated that the United States is vulnerable to asymmetrical enemy attacks that can have a disruptive and potentially destructive direct impact on US citizens' daily lives. Of all possible asymmetrical attacks, bioterrorism poses one of the most significant dangers to the security to US citizens and their way of life. Given such dangerous threats, the US national security establishment has a great deal of work to do to effectively deal with transnational threats like bioterrorism.

In order to become more effective in the post-Cold War environment, the intelligence community (IC) needs to focus on enhancing foundational elements like customer relationship management, information management and human resource management. Many of these improvements will not only benefit the counter-bioterrorism mission thread, but also other transnational mission threads such as counter drug operations, organized crime, and information operations. The IC also should institute more specific improvements to collection and analytical functions.

Transnational threats involve groups who are organized along sub-national lines that are often global in nature. Viewed from a regional or even purely functional perspective they may appear small or insignificant. Al Qaida terrorists who were casing US military activities in Singapore prior to 9/11 were probably characterized by Pacific intelligence agencies as more of a concern than a direct threat. However, the Al Qaida activities, when viewed as part of transnational terrorist threat, illuminate a larger and more threatening organization. Working

transnational mission threads like bioterrorism requires in-depth actions from a wide variety of US government agencies and organizations, and perhaps more importantly, outside expertise.

There is no need for radical reorganization or creation of many new organizations. By the time intelligence leaders spend precious resources and expend limited energy in trying to “grow” new organizations they can transform current organizations with the infusion of necessary resources and targeted expertise.

The IC needs to focus on enhancing current organizational capabilities by making them more efficient, more integrated, and more teamwork oriented. By focusing on specific contributions to specific mission threads, intelligence organizations can develop more responsive and meaningful collection and analytical capabilities. Many of these improvements can be technology-based and will certainly require resources but one key for a more responsive IC will be agile and risk-taking leadership at all levels.

The Counter-Bioterrorism Mission Thread

Various missions of the US government have sub-missions whose responsibility is shared by multiple agencies or organizations. The primary mission forms a thread of responsibilities and required actions that are woven throughout the bureaucracy at not only the federal but the state and local levels also. In the case of the counter-bioterrorism mission, there are four sub-missions.¹ These sub-missions are deterrence, preemption, domestic response, and attribution.

Each of the sub-missions of counter-bioterrorism involves multiple organizations with specific responsibilities. For example, the domestic response sub-mission consists of rapid identification of pathogens used in an attack and consequence management. There are a variety of government players who have domestic response roles in the event of a bioterrorist attack. At the local level, public health officials are responsible for reporting outbreaks and initial response

efforts. The federal government is responsible for maintaining some vaccines and providing assistance in pathogen identification. All levels of government must play a role in developing and maintaining a good epidemiological surveillance system to allow for rapid identification of disease outbreak. Collectively these responsibilities contribute to the counter-bioterrorism mission thread.

This process is commonly known as the interagency process because it requires a considerable amount of teamwork across government organizations to successfully accomplish any mission or any sub-mission. Effective accomplishment of any mission requires substantial coordination and inspired leadership because at the end of the day, mission accomplishment requires people from different organizations, to perform complimentary tasks, in pursuit of a common objective. As we will see, technology is a major facilitator but another important factor is team-focused leadership, characterized by agility and flexibility.

Understanding the concept of mission threads is critical to any examination of US instruments of foreign policy to include intelligence. The US IC supports all four counter-bioterrorism sub-missions. The first is to deter biological attack. If deterrence fails, the second is to support preemptive efforts. If preemption fails and terrorists successfully execute a biological attack, the third sub-mission is domestic response. The fourth and final sub-mission intelligence can support is identification of perpetrators and all the actions it can lead to-- apprehension, prosecution, punishment.

This final mission actually supports deterrence efforts. Each counter-bioterrorism sub-mission reinforces the others. If the US takes a hard line, aggressively prosecuting and punishing terrorist and those who support them, it may help deter future terrorism. These sub-missions fall under the authority of several different government organizations but collectively

they form one mission thread to protect US citizens from the threat of bioterrorism and are vital to America's national security.

Notes

¹ Other papers that outline counter bioterrorism sub-missions are Dickinson, Lansing E., (Lt Col). "Military Role in Countering Terrorist use of Weapons of Mass Destruction", Air War College, April 1999, 27 and Carter, Ashton, B. "The Architecture of Government in the Face of Terrorism", International Security, Vol. 26, No. 3 (Winter 2001/02), 16. Deterrence, Preemption, Response, and Attribution sub-missions are common themes in these studies.

Chapter 2

Background

Recent events have heightened fears about terrorist use of biological weapons. To fully understand the daunting task involved in countering bioterrorism, it is important to understand the bioterrorism threat. This requires an understanding of the characteristics of BW as well as the history of their use. In addition, examining the processes associated with using a biological weapon provides insight into the means a bioterrorist would be required to follow, and thus illustrates potential points at which the US could intervene to prevent attacks. Understanding this background data on BW will assist one in fully appreciating the intelligence challenges associated with bioterrorism.

What Are Biological Weapons

Biological weapons are “devices intended to deliberately disseminate disease-producing organisms or toxins in food, water, by insect, or as an aerosol.”² These weapons contain agents that can be categorized into two basic groups—microorganisms and toxins. Microorganisms are the living germs that produce hazardous and lethal diseases and toxins.³ These agents can be used to kill or incapacitate people and animals and destroy crops. Naturally occurring microorganisms that can cause disease are known as pathogens. Besides causing diseases, pathogens are dangerous because they are self-replicating. Due to this characteristic even limited exposure can lead to incapacitation or death. Furthermore, contagious pathogens are the most dangerous because simple human contact can rapidly spread them, leading to epidemic outbreaks, potentially resulting in a number of catastrophic events.⁴ Table one list primary biological agents, their untreated effects, and potential for epidemic spread.

BIOLOGICAL WARFARE AGENTS CHARACTERISTICS⁵

Table 1: Characteristics of Biological Warfare Agents

Types Agents *	Untreated Effect	Potential for Epidemic Spread
Bacteria Anthrax	Lethal	Negligible
Tularemia	Incapacitant-lethal	Negligible
Plague	Lethal	High
Cholera	Incapacitant-lethal	High
Glanders	Lethal	Negligible
Clostridium Perfringens	Incapacitant	Negligible
Brucellosis	Incapacitant	Negligible
Shigellosis	Incapacitant	Possible
Q Fever	Incapacitant	Possible
Toxins Botulinum toxin	Lethal	None
Ricin toxin	Lethal	None
Staphylococcal nterotoxins	Incapacitant	None
Mycotoxins	Incapacitant-lethal	None
Marine Neurotoxins	Incapacitant-lethal	None
Aflatoxin	Incapacitant-lethal	None
Bioregulatory Peptides	Incapacitant-lethal	None
Viruses Venezuelan Equine Encephalitis	Incapacitant-lethal	Possible
Smallpox	Lethal	Very High
Marburg/Ebola	Lethal	Possible
* In many cases the more commonly known disease is listed rather than the actual causative agent.		

A biological agent alone is not a weapon. It becomes a weapon when it is capable of being delivered and disseminated. The delivery mechanism could be as sophisticated as an intercontinental ballistic missile or if the agent is contagious, as basic as a single individual passing through a crowd. The combination of an agent and a delivery mechanism constitute a biological weapon.⁶

Chemical agents are different primarily because they are man-made, quick acting and there is no chance of secondary spread.⁷ Biological and chemical agents are often used interchangeably when discussing weapons of mass destruction. Their differences are significant, and chemical agents pose less of a threat than biological agents. Most importantly, biological agents are much more toxic than chemical agents. A chemical attack can shut down city blocks. A biological attack can threaten a city.⁸

Biological Weapon Liabilities

Much has been written about biological weapons being the “poor man’s” preferred weapon of mass destruction. While this may be true, such assertions often leave one to think that biological weapons are simple to develop and employ. Relative to nuclear weapons, biological weapons may be simple, but to be truly effective they still require expertise in agent development and, equally important, delivery mechanisms. There are several factors to consider when discussing the ease with which biological weapons can be successfully employed.

In her study on the role of biological weapons on international politics, Susan Martin points out that biological weapons have many “liabilities”. First, biological weapons are inherently unstable. Getting a weaponized agent from the laboratory to the battlefield or intended target while maintaining its virulence is no easy feat. Second, while storing the weapons may be easy (refrigeration is the preferred method), successfully transporting and

delivering them in its virulent form is very difficult and requires fairly sophisticated scientific knowledge and equipment. Finally, agents can lose their effectiveness when they encounter sunlight, heat and other adverse environmental conditions. These impediments can be overcome with scientific methods such as agent encapsulation, but this requires expertise not often found outside of the labs of western biotechnology firms.⁹

Perhaps the best example illustrating the difficulty terrorists have in using biological weapons is the case of Aum Shinrikyo. According to Amy Smithson, Director of the Chemical and Biological Weapons Nonproliferation Project at the Henry L. Stimson Center, “no individual or group has approached the replication of Aum’s constellation of technical skill, intent, and resources directed toward a viable unconventional mass casualty threat,” yet they were unsuccessful in using biological weapons. The Aum experience “disproves the assertions that acquiring and spreading these agents is a shake-‘n-bake easy.”¹⁰

History of Biological Warfare

Biological warfare is not new. Early examples include the use of infected cadavers at the siege of Kaffa in the 14th century and British attempts to infect American Indians with smallpox during the French-Indian war. During World War II the Japanese had an extensive biological weapons program along with plans to use them, but dissemination problems thwarted their efforts. For example in 1942, during biological operations in China, the Japanese accidentally killed 1,700 of their own troops.¹¹ Allegedly, the Soviets used biological weapons in the battle of Stalingrad but they too experienced problems with self-infection due to shifting winds. Both the US and Russian had extensive programs during the Cold War. In 1969 President Nixon initiated a unilateral halt of the US program which helped lead to the way to the Biological Weapons Convention (BWC) in 1972. (The relationship of the BWC to intelligence operations

will be discussed later in this paper.) Today 163 nations are signatories to the convention.¹²

History has proven that biological weapons are not very effective on the conventional battlefield. More recent events have heightened the concern that biological weapons are more useful to terrorists planning asymmetrical attacks.

More Recent Biological Weapon Concerns

Four more recent events have heightened concern that the United States could become the target of biological terrorists. The first of these events was the sarin gas attacks on the Tokyo subway system in 1995 by Aum Shinrikyo, a Japanese cult group. The group proved that scientific experts working in weapon labs could operate undetected for years, despite a number of nefarious acts such as purchasing a Russian military helicopter to use as a weapons delivery system.¹³ At the time, the US did not see the group as a threat to any of its military activities in Japan or the Far East. The bottom line is that a fairly sophisticated bioterrorist group worked right under the nose of a key ally and was not detected until it launched a devastating chemical attack.¹⁴ While the group was ultimately unsuccessful in bioterrorism, it demonstrated its capacity to develop agents. Had Aum not been discovered after the sarin subway attack, they may have ultimately carried out a successful biological attack.¹⁵

A second event was the stunning revelation of the size and extent of the Soviet biological weapons program. It included over 50 facilities and 65,000 employees, among those 9,000 key scientist and engineers, according to Russian defector Ken Alibek. The collapse of the Soviet Union and the subsequent dismantling of much of their program led to a potential proliferation of bioweapons expertise to potential enemies of the US.¹⁶ This expertise could be used to assist terrorist groups or states that support them in developing bioweapons to be used against the United States.

A third alarming event in the last 10 years is Iraq's ability to conceal an extensive biological weapons program despite the United Nations' aggressive inspection regime that was put in place following the Gulf War to destroy Iraq's NBC weapons. While the US suspected Iraq had biological program as early as 1990, the extent and details of the program were not revealed until General Hussein Kamel defected in 1995—four years after inspection program began. Many argue that Iraq initiated an aggressive campaign to thwart UN inspection efforts in 1997 because it was close to discovering Iraq's biological weapon program. This led to US military strikes in 1998 and the subsequent end to the UN inspection process.¹⁷ While Iraq's chemical and nuclear programs were largely dismantled as a result of the UN inspection program, its biological program remains a mystery and potentially went unscathed in the first four years of the inspection regime. Given the absence of inspectors over the last three years and Iraq's willingness to pursue NBC weapons at any cost during the inspection regime, logic suggests that Iraq's BW program is firing on all cylinders in the absence of inspectors on the ground. With US talk of an Iraqi regime change as a primary national security objective, the prospect of Iraqi employment of biological weapons in any future conflict must be considered a highly probable option. Use of biological weapons (BW) by a state at war with the US is beyond the scope of this paper. However, Iraq's support of terrorism combined with its BW arsenal could increase the likelihood of bioterrorism against the US if Iraqi-US tensions significantly escalate.

Finally, the events of 9/11 and the subsequent anthrax attacks revealed the US domestic vulnerabilities to bioterrorism. For the first time, American citizens came under a deadly bioterrorist attack. While there is still much to be learned about this attack, it clearly

demonstrated that even a limited attack using an unsophisticated delivery system, the US Postal Service, can disrupt millions of Americans' daily lives and even result in some fatalities.

Americans understand the threat of bioterrorism now better than ever. History has shown that BW is not effective in conventional military settings. Recent events suggest that biological weapons are increasingly more likely to be used against the US homeland than deployed against military forces.¹⁸ Today more than any other time in history the bioterrorist threat is real because enemy asymmetrical attacks are effective when weighed against directly facing the overwhelming power of US military forces.¹⁹

The Bioterrorism Process

Understanding the basic process a terrorist must undertake to effectively deliver a biological weapon is important background when studying bioterrorism intelligence challenges. But before we can look at the process, it is important to look at a definition of bioterrorism.²⁰ While there is no commonly accepted definition of bioterrorism, Seth Carus, defines it as “the threat or use of biological agents by individuals or groups motivated by political, religious, ecological, or other ideological objectives.”²¹

The process of bioterrorism includes a number of acts that precede actual weapons employment. Many of these steps also apply to terrorist groups that pursue other weapons, but a review of each step helps to clarify the bioterrorist process. Some groups will clearly skip some of these steps, while others may take additional precautions. Each step should be well understood by US intelligence specialists as they try to identify potential bioterrorist groups and their success or failure moving through the bioterrorism process.²²

The first step in the process is group formulation. Terrorist groups are formed based upon common values and motivations, some of which are directly related to their willingness to

use BW. During this phase, their objectives and means of reaching them, are formulated to include decisions about employing various types of weapons. More violent and less politically motivated groups may be the most willing to pursue BW. Liabilities associated with BW may dissuade other groups from deciding to use them. For example, if a terrorist group is concerned about executing precise attacks, the lack of predictability associated with BW may prevent it from trying to use them. The latent effect of BW may discourage terrorists who desire immediate and dramatic results. On the other hand, highly infectious agents may be best suited for apocalyptic terrorists who care little about personal risks or precisely employing a weapon.

A decision by a terrorist group to use BW leads to more specific acts such as planning and information gathering on potential targets. It is during this phase that terrorists identify methods for acquiring and/or developing biological weapons. The next step is to acquire the material and equipment for weapons production or to obtain assistance from a state-sponsor for BW. For those groups seeking state sponsorship, any negotiations will certainly be conducted covertly, perhaps with an elaborate cover to avoid detection. For groups trying to manufacture their own weapons, this phase includes laboratory selection and development and acquisition of specific types of weaponization equipment. During the production phase, certain terrorists must take protective/security measures to protect scientists and the surrounding areas and to conceal weapons fabrication. Following production or state transfer of weapons, terrorists may choose to test and evaluate weapons or they may simply accept the inherent risk of not testing and go ahead and deploy or preposition weapons. The next step is actual use or employment of the weapon. Delivery may be followed by exploitation efforts such as political bargaining or threatened use of follow on attacks to create even more fear or panic.

Each step in the bioterrorist process offers an opportunity for the IC to uncover threats and employ counter-bioterrorism tools to prevent attacks. Perhaps most importantly, strong intelligence can support instruments of deterrence, ensuring that each step of the bioterrorism process is deterred and that if deterrence fails, preventative actions can be quickly employed. Comprehensive intelligence will greatly benefit response and consequence management efforts (pathogen identification, treatment, and clean up). Investigation for attribution will require detailed intelligence if follow-on actions are to be timely and effective.²³

Notes

² Inblesby, Thomas V., Tara O'Toole and Donald A. Henderson, "Preventing the Use of Biological Weapons: Improving Response Should Prevention Fail." Available <http://www1.journals.uchicago.edu/CID/journal/issues/v30n6/00065.text.html>.

³ Mayer, Terry N. "Biological Weapons—The Poor Man's Nuke." Research Report, Maxwell AFB, Ala.: Air War College, April 1995.

⁴ Carus, W. Seth. *The Illicit Use of Biological Agents Since 1900*. Center of Counterproliferation Research, National Defense University. February 2001.

⁵ Office of the Secretary of Defense. "Proliferation: Threat and Response." January 2001, 113.

⁶ Carus.

⁷ Martin, Dr. Susan B. "The Role of Biological Weapons in International Politics: The Real Military Revolution." Forthcoming article in the *Journal of Strategic Studies*, Spring 2002. In her article Dr Martin makes a compelling argument that the very nature of Biological Weapons (they can multiply and mutate) make them prime deterrent weapons of choice for some countries and that this will have major impact on the future of international relations

⁸ Office of the Undersecretary of Defense for Acquisition and Technology. "DoD Responses to Transnational Threats." Vol. 1. Defense Science Board 1997 Summer Study Task Force. December 1997.

⁹ Martin.

Notes (continued)

¹⁰ Smithson, Amy and Leslie-Anne Levy. “Ataxia, the Chemical and Biological Terrorism Threat and the US Response.” Stimson Center Report 35. Henry L. Stimson Center, 2000.

¹¹ Williams, Peter and David Wallace, *Unit 731: Japan's Secret Biological Warfare in World War II*. New York: The Free Press 1989.

¹² Stockholm International Peace Research Institute Home Page (SIPRI). Available <http://projects.sipri.se/cbw/docs/bw-btwc-sig.html>. Accessed 21 April 2002.

¹³ Falkenrath, Richard A., Robert D. Newman and Bradley A. Thayer. *America's Achilles' Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack*. Cambridge, Massachusetts: The MIT Press, 1998.

¹⁴ Falkenrath, 22.

¹⁵ On March 15, 1995 five days before the deadly sarin attacks on the Tokyo subway systems the Aum Shinrikyo group reportedly attempted an aerosol botulinum toxin attack in the subway system. The attack failed reportedly due to second thoughts by the terrorist who was supposed to execute the attack. The terrorist filled the delivery devices—briefcases fitted with sprayers—with water instead of the toxin solution. While we will never know for sure, it is possible that the group was getting dangerously close to successful BW attacks.

¹⁶ Smithson, Amy. “Toxic Archipelago: Preventing Proliferation from the Former Soviet Chemical and Biological Weapons Complexes.” Stimson Center Report 32. Henry L. Stimson Center, 1999.

¹⁷ Falkenrath, 255-258.

¹⁸ Notable exceptions to this assertion would be a desperate Iraqi or North Korean regime on the verge of collapse. One could argue that they would be willing to use BW on the battlefield if leadership felt seriously threatened in a conventional conflict.

¹⁹ Inblesby.

²⁰ The Department of Defense official definition of Terrorism is “the calculated use of violence or threat of violence to inculcate fear: intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.” Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms*.

²¹ Carus.

Notes (continued)

²² Powers, Michael J. CBACI, Deterring Terrorism with CBRN Weapons: Developing a Conceptual Framework, Feb 2001, 5

²³ Powers.

Chapter 3

Bioterrorism Threat: Issues for Analysis

As discussed in Chapter 2, recent events suggest bioterrorism events are becoming increasingly more likely. Former Senator Sam Nunn stated he is “convinced the threat of biological weapons attack on the US is as urgent as it is real.”²⁴ Three issues are contributing to an increased threat of bioterrorism. The biotech revolution is making weapons increasingly easier to manufacture and disseminate. The face of terrorism is changing, leading to more lethal methods of expression and making BW an attractive option. Finally, a Biological Weapons Convention without a comprehensive verification process hinders counter-proliferation efforts and poses few obstacles to state sponsorship of bioterrorism. Not only is the threat becoming more real, but its potential to inflict devastation on the US way of life suggests it should be treated as a potential weapon of mass destruction.

Analysis of Threat is Limited

While bioterrorism has received a great deal of attention since the events of 9/11, up until that time there was limited study of associated threats. Prior to 9/11, the likelihood of a catastrophic bioterrorist attack was considered a low probability high consequence event. Efforts to respond to such an attack were examined in a few exercises but comprehensive threat analysis and associated response planning was lacking. In fact, the first comprehensive study on the cases of bioterrorism and their impact was not conducted until 1995.²⁵ Since then, Seth Carus from National Defense University has created the most comprehensive review of the history of bioterrorism and biocrimes.²⁶ The US government needs to place more emphasis on comprehensive threat analysis of bioterrorism. This analysis should include concern the

following three issues: the impact of the biotechnology revolution on BW development, the changing face of terrorism, and the role of state programs in assisting terrorists.

Developing BW Capability is Getting Easier for Terrorist

Significant advances in biology in the last three decades have made it easier to develop BW. First, there is more expertise than ever. In the US alone between 1966 and 1994, PhDs in biology increased by 144 percent. The underlying expertise for developing nefarious biology is increasing.²⁷ In the early 1980s there were a handful of employees working in the US biotech industry. In 1996 the Biotechnology Industry Organization estimated that 1,287 US biotech firms employed 118,000 people.²⁸ The global nature of these firms suggests biotech expertise will continue to expand overseas. Second, information and knowledge on developing agents is readily available. Undergraduate and graduate students can learn the details of laboratory-scale fermentation processes through university courses. The Internet contains basic information on how to manufacture biological agents. Finally, the biotech revolution has led to exciting genomic discoveries that have revolutionized health care. However, these same discoveries applied to an offensive BW effort, can produce weapons that will complicate identification, resist treatment, and increase virulence.²⁹ Collectively biotech advances have increased the availability of BW, which in turn have increased the opportunities for terrorists to acquire BW. It should be noted that as the US responds to the increased BW threat, the same biotech breakthroughs that make weapons development easier could also make biodefense technologies more effective.

Changing Face of Terrorism: Impact on Bioterrorism

In order to understand the bioterrorism threat, it is necessary to understand trends in terrorism. Not all terrorist groups will be interested in BW. Trying to make a distinction between groups willing to pursue BW from groups unwilling to use them is not easy. Carefully analyzing their objectives may offer the best hope of identifying the most dangerous groups to include those willing to pursue BW. In order to understand why the bioterrorism threat is increasing, it is useful to review the changing face of terrorism. These changes may correlate with the increasing likelihood of bioterrorism. It is also important to distinguish between different types of bioterrorists.

Trends in Terrorism

There are some ominous trends in terrorist group actions that suggest bioterrorism may emerge as a weapon of preference. Terrorists are more prone to initiate indiscriminate attacks and their “motivations are changing in a way that makes mass-casualty attacks more likely.”³⁰ In short, recent terrorist acts demonstrate that some groups care less about who and how many they kill.

Some of the most notable examples are the US embassy bombings in Africa in 1998 and the attacks of 9/11. The goal in both attacks was to kill as many people as possible to punish America. Attacks occurred during business hours to maximize casualties, there were no political demands leading up to the attacks, there were no public claims of attacks to gain political attention. Although one could argue that Al Qaida has demanded withdrawal of US troops from Saudi Arabia as a political demand, there has been little serious political activity leading up to attacks. Al Qaida and other extreme terrorist groups may indeed have political objectives, but elements of their network operate in the “apocalyptic” realm. As a result, groups may begin to

take on a dual character, containing leaders with traditional political objectives who use members with extreme views to execute increasingly lethal attacks. Regardless of ultimate political aims, terrorist groups are becoming more lethal.

Terrorism experts argue that in recent years there are four factors that are driving terrorists to adopt more lethal weapons.³¹ The first is radical religious motivation. For example, the religious conflict in Kashmir between Hindu and Islamic factions has led to increasingly deadly attacks against India. The second factor is local opposition to US hegemony and military presence in areas with no historical US presence. The best example is the US presence in the Arabian Peninsula and Persian Gulf that has led to fatal attacks by Al Qaida on the United States at home and abroad. Other areas of US expansion that could increase regional resentment include the Central Asian States. A third factor is evidence that amateur terrorists have little fear of detection or little concern for self-preservation. A good recent example is the suicide attack on a Tampa, Florida skyscraper by a young pilot that fortunately failed to inflict mass casualties. The final factor increasing the lethality of terrorism is racial and ethnic hatred. The current Palestinian-Israeli crisis demonstrates a Palestinian willingness to adopt increasingly lethal measures. The increasingly lethal nature of terrorism may make BW more acceptable to some terrorist groups.

Bioterrorist Groups: What Makes Them Different

Given the increasing lethality of terrorism, it is important to examine potential differences between terrorist groups that use BW and those that do not. Examining group objectives may help to highlight differences between these two groups. It will also help to distinguish among different types of bioterrorist groups. Based upon limited examples like Aum Shinrikyo, groups willing to use BW may have more apocalyptic than political aims. Small

fringe groups with very specific objectives may lean toward adopting BW. Additionally, BW terrorist groups will probably contain more radical and fringe membership. This new breed of terrorist willing to use bioweapons can be divided into four basic categories: fundamentalist and religious groups; racist and antigovernment groups; millenarian cults; and “amateur” terrorists.³²

To date, there is no commonly accepted profile a bioterrorist group, but in his bioterrorism study, Seth Carus uses group objectives to distinguish BW and non-BW groups. He points out that terrorists conduct attacks to intimidate governments or societies. Conversely, not all bioterrorists have an interest in influencing governments or societies, but simply want to carry out apocalyptic acts. Such acts may be more focused on destruction or punishment with little concern for political implications. To date no group has successfully carried out an apocalyptic attack, although Aum Shinrikyo probably came the closest. There is growing evidence that Al-Qaida was pursuing a biological weapons capability and one could make an argument, given the 9/11 suicide attacks, that they would have used it to punish the US.³³ Groups expressing apocalyptic philosophies will probably be more willing to explore BW use than groups with specific political objectives. Apocalyptic terrorism has major implications for the US IC because it is often bizarre in nature, difficult to analyze, and hard to predict when and where strikes will occur.³⁴

In some cases bioterrorist attacks may be conducted in secrecy and never acknowledged by some smaller fringe groups because they focus on achieving specific objectives versus making broader political statements.³⁵ The best example of such a group activity is the biological attack carried out by the Rajneesh Oregon cult group in 1984. They infected local restaurant salad bars with Salmonella bacteria in order to reduce voter turnout on Election Day.³⁶ Adopting bioterrorism to obtain a specific objective is also worrisome and difficult to anticipate

because groups conducting such attacks will probably be smaller and more secretive. US officials thought the infection at the Oregon salad bars was due to poor food safety standards rather than an intentional attack. Officials did not become aware of the attack until years later when group members confessed during plea-bargaining on other criminal charges.

The make-up of groups that are motivated to conduct bioterrorist acts may include individuals whose personalities are marked by desperation and insecurity. Their motivations will be less political and probably more religious-based—characterized by extremist acts and positions.³⁷ Radical or apocalyptic group objectives may be important indicators of a group's willingness to adopt BW as terrorism tool. While the number of groups with radical and apocalyptic aims may be small, the US must work hard to counter their efforts, because even one bioterrorist group has the potential to create a high-consequence event.³⁸

Biological Weapons Convention and State Programs: Intelligence and Bioterrorism Implications

In the BWC, signatory nations agree “to refrain from developing, producing, stockpiling, or acquiring biological or toxin weapons.”³⁹ However there is no verification process as part of the treaty.

In November 2001 a decision on adopting some type of verification protocol for the BWC was tabled and will be a key issue when parties to the convention meet in November 2002. Currently the US government opposes adopting a mandatory inspection regime for the 1972 Convention primarily because it fears the potential compromise of government biodefense and commercial proprietary information. The purpose of this section is not to debate whether the US should agree to a BWC inspection protocol, but rather to discuss the impact inspections could have on intelligence operations and bioterrorism.

Overall, an effective verification protocol would contribute to counter-bioterrorism efforts. It is important to examine the relationships among a BWC inspection process, state BW programs, intelligence operations, and terrorists when analyzing bioterrorist threats. An inspection protocol will deter states from pursuing BW, compliment intelligence operations, and decrease chances a terrorist will obtain BW.

State Programs: Key to Bioterrorism

While this paper focuses on bioterrorism, the US IC cannot comprehensively counter this threat without clearly understanding state biological weapons programs and their potential ties to terrorist groups. While the IC has traditionally focused on state programs, history indicates this effort can be improved. Both the Soviet and Iraqi biological programs remained largely undetected until defectors revealed their existence.⁴⁰

The most likely avenue for successful bioterrorism employment is state assistance. States have more resources and expertise to overcome formidable liabilities with manufacturing and delivering BW, than do terrorist groups. The best of example of the limitations of a terrorist group is Aum Shinrikyo. Despite having experts and resources, the group was unable to execute a successful biological attack in nine attempts.⁴¹ To effectively thwart bioterrorism, the community will have to continue to track state programs with an emphasis on possible terrorist links.

Most states are unwilling to face the condemnation and retaliation BW use would bring upon them. For those states willing to build programs, they are more likely to acquire BW for deterrence versus actual use. The changing face of terrorism suggests that groups would be more likely to use BW than states. Intelligence experts close to analyzing the problem refuse to discount the possibility of terrorists developing their own biological weapons regardless of the

liabilities.⁴² However, logic would suggest that the greatest threat of biological attack would come from a terrorist group sponsored by a state with a biological weapons program. The US IC backed by an effective BWC treaty could play a key role in deterring and preventing threats on the horizon.

BWC Impact on State Deterrence and Intelligence

The deterrent effect of on-site inspections would complement intelligence operations. While the BWC cannot guarantee detect of every violation of the convention, it could help highlight potential trouble spots.

The objective of a verification regime would be transparency of facility capabilities. At a minimum, where inconsistencies exist, the protocol can raise suspicions between the stated and actual purposes of sites. Even if visits to certain sites are prohibited by host nations, the inspectors can learn a great deal, allowing intelligence to focus on potential violators. Countries unwilling to allow inspection of certain facilities may preclude direct detection, but the refusal to allow inspections will raise red flags, alerting the IC to scrutinize potential violators. Precious intelligence resources could be focused on the most likely trouble spots. Without an effective inspection protocol, intelligence collection and analytical resources could be overwhelmed and, no matter what priority is placed on counter bioterrorism efforts, could be significantly hindered.

The most efficient way for proliferators to manufacture biological weapons is to utilize existing commercial plants. But if these plants are declared, a necessary step under the protocol, proliferators would be forced to move weapons manufacturing to clandestine sites, a feasible step but one which contains a number of risks and would produce signatures associated with suspicious activity. Examples of signatures are security, unexplained scientific equipment and staff, and special handling facilities. The signatures would raise suspicions and make it difficult

to conceal the clandestine sites, presenting further difficulties to proliferators. An effective inspection protocol will improve intelligence efforts and deter states from pursuing BW.

BWC Inspection Could Help Thwart Bioterrorism

The lack of verification could lead to greater state proliferation and ultimately spillover to terrorist groups. However, skeptics point out that the treaty has not been completely foolproof in halting BW programs. Both Russia and Iraq pursued massive programs despite both countries being signatories. Nonetheless an effective BWC inspection protocol would deter some states from pursuing BW programs and therefore limit possible avenues for terrorists to obtain state support. Furthermore, without an inspection regime, voluntary compliance may gradually erode. States that cannot afford nuclear programs could turn to BW as a weapon of deterrence, creating a potential for spillover to terrorist groups that they may sponsor.⁴³ One could argue that if more states pursue BW for deterrent purposes, it is simply a matter of time until one or two begin sharing materials and expertise with terrorists they may support.

A verification process would also direct attention to those states unwilling to submit to inspections. This may cause them to think twice about risking further exposure by sharing BW materials or expertise with terrorist they may not be able to control. The overall impact of a BWC inspection process will decrease the likelihood that terrorists will receive BW support from states. The lack of an inspection regime makes proliferation to terrorist groups an increasing likelihood.

While the US is focused on domestic response to a bioterrorist disaster, “it would be foolhardy to ignore the more important goal of cutting off the source by preventing the proliferations of biological weapons.”⁴⁴ An effective BWC backed up by aggressive intelligence offers the best opportunity to deter and if necessary prevent bioterrorist attacks.

Bioterrorism: Weapon of Mass Destruction or Disruption?

The fear and paralysis created by the limited anthrax attacks in the Fall of 2001 demonstrated to all the severe impact that even a small biological attack could have. An important question directly related to analysis of the bioterrorism threat is, “Do biological weapons in the hands of terrorist merit classification as weapons of mass destruction or are they less powerful weapons?”

The label applied to BW is important, because it will shape response efforts and influence resource allocation. In his keynote address at the 2002 Biological Threat Reduction Conference, Hans Mark reiterated the importance of words and labels when discussing weapons of mass destruction and potential response efforts.⁴⁵

Few can argue that the anthrax attacks did not cause a substantial terrorizing effect on the US population. While people were afraid of flying and returning to work in the nation’s skyscrapers due to the 9/11 suicide attacks, they were equally or perhaps more terrified to open their mail or visit theme parks or other venues with concentrated crowds due to fear of further biological attacks.⁴⁶

While the anthrax attacks impacted the psyche of the American population and shut down a number of facilities, one could argue this was more a disruptive rather than destructive event. Some would argue that the subsequent economic slump in the shipping industry was destructive but it was more temporary than permanent. However, in the worst-case, BW weapons in the hands of terrorists can be classified as potential weapons of mass destruction depending on the agent used, delivery method, and preparedness of the target. This assessment is due to the dysfunctional environment they could create and subsequent shutdown of the US infrastructure as opposed to physical destruction.

The exercise Dark Winter⁴⁷ clearly demonstrated the absolute panic that would ensue from an epidemic caused by a well-coordinated smallpox attack.⁴⁸ In testimony before the Senate Foreign Relations Committee on 5 September 2001, former Senator Sam Nunn emphasized that dealing with a contagious outbreak could easily lead to catastrophic consequences for the United States, including paralysis of travel, trade, and basically all human interaction.⁴⁹ Nunn argued that

bioterrorism is a unique threat because after an attack terrorists are no longer the enemies; your neighbors, co-workers, and family members carrying the disease are. Bombs are bounded in time and place—on the other hand BW is a silent, ongoing invisible attack. Some are highly contagious and spread in a flash—it can come in waves. It can pit Americans against Americans. He even describes the scene using biblical parallels found in Zechariah (8:10). Neither was there any peace to him that went out or came in for I set all men every one against his neighbor.⁵⁰

The decision-making environment of an unprepared society while under a contagious biological attack could lead to a series of increasingly impossible choices. They include decisions on ceasing interstate commerce, suspension of stock markets, suspension of international trade, determining who gets life saving vaccines in the face of public riots, curbing state and local powers, isolating certain communities, maintaining law and order in the face of anarchy, maintaining public confidence in government, and suspending all air traffic.⁵¹ Such scenarios could lead to widespread panic and a situation where panic itself becomes the more powerful weapon. This bleak picture demonstrates why biological weapons should be treated as potential weapons of mass destruction. While physical infrastructure may not be destroyed, under some of the worst possible scenarios, the US infrastructure could functionally be shut down. This could destroy the American way of life for years to come.

Those focused on planning counter-bioterrorism efforts need to be wary of freely accepting worst-case analysis on the impact of a biological attack. Worst-case analysis is just that, the potential worst case. It is important to emphasize that BW have yet to be demonstrated as weapons of mass destruction and not all agents are as dangerous as contagious ones like smallpox and plague. In addition, basing response and resource allocation against the worst case may not make the most sense, because it assumes that an adversary will flawlessly deliver the most virulent biological weapon.⁵²

Biological weapons should be labeled as potential weapons of mass destruction. In the final analysis, bioweapons in the hands of terrorists may not have the “firepower” of nuclear weapons. However, Senator Nunn’s point on their uniqueness and potential for initiating an environment of anarchy combined with a growing list of enemies willing to use them, make defense against them critical for US national survival. While the impact of their use is not nearly as catastrophic as nuclear weapons, they represent an emerging threat not only to US vital interests but the American way of life.

While the IC has historically committed resources to monitor BW proliferation efforts, including potential activity by terrorist organizations, these efforts were based upon the low probability that an event would actually occur. The biotech revolution, along with the changing face of terrorism and lack of an effective international inspection program to curb proliferation, suggests that the threat of bioterrorism is real and growing. The US IC has to make counter-bioterrorism one of its highest priorities because it is a real and growing threat that can lead to mass destruction.

Notes (continued)

²⁴ US Senate Committee on Foreign Relations, Hearing on The Threat of Bioterrorism and the Natural Spread of Infectious Diseases, 5 September 2001. Testimony for Former US Senator Sam Nunn.

²⁵ Purver, Ron. Chemical and Biological Terrorism: The Threat According to the Open Literature. Canadian Intelligence Service, June 1995.

²⁶ Carus.

²⁷ Falkenrath., 172.

²⁸ Falkenrath, 175

²⁹ Falkenrath, 175

³⁰ Lederberg, Joshua. Editor. *Biological Weapons: Limiting the Threat*. The MIT Press. Cambridge, Massachusetts. 1999. 290-291.

³¹ Falkenrath.

³² Lederberg.

³³ Gordon, Michael R. "US Says It Found Al Qaida Lab Being Built to Produce Anthrax." *The New York Times*, 23 March 2002., A1.

³⁴ Carus.

³⁵ Carus.

³⁶ Falkenrath. 35-36.

³⁷ Powers.

³⁸ Falkenrath.

³⁹ Ferguson, James R. "Biological Weapons and US Law," *Journal of the American Medical Association (JAMA)*, Vol. 278, No. 5 (August 6, 1997)., 357-360.

⁴⁰ Falkenrath, 68 and 256.

⁴¹ Subcommittee on National Security Veterans Affairs and International Relations, House Committee on Government Reform, Hearing on The Biological Weapons Convention Protocol: Status and Implications, 5 June 2001. Testimony of Barbara Hatch Rosenberg, PhD.

Notes (continued)

⁴² Author's interview and subsequent correspondence with current US government official interview, Miami Florida, 15 December 2001.

⁴³ For a discussion on likelihood of States pursuing BW for deterrent purposes see Martin, "The Role of Biological Weapons in International Politics: The Real Military Revolution."

⁴⁴ Rosenberg

⁴⁵ Mark.

⁴⁶ "Guests' Bags Inspected Before Entering Parks," News Channel 2000 Web Site,

Available <http://www.newschannel2000.com/orl/news/stories/news-100873020011009-091033.html>.

(Accessed October 9, 2001)

⁴⁷ Dark Winter was an exercise conducted in June 2001, which simulated a series of National Security Council (NSC) meetings dealing with a terrorist attack involving the covert release of smallpox in three American cities. The exercise was conducted by the Center for Strategic and Studies, the Johns Hopkins Center for Civilian Biodefense Studies, and the ANSER Institute for Homeland Defense Participants serving in the role of NSC members had served in previous cabinet level positions. While there were many lessons learned Senator Nunn (played US President) concluded, "that public health had become a national security issue, and that the US was unprepared." The scenario, while admittedly a worse case event, highlighted major US deficiencies in response capabilities and equally important the criticality of time-sensitive response.

⁴⁸ Nunn.

⁴⁸ Nunn.

⁴⁹ Nunn served as US President during the Dark Winter exercise and gained first hand knowledge of the potential catastrophic spiral a contagious biological attack could lead to.

⁵⁰ Nunn.

⁵¹ Nunn.

⁵² Mark, Dr. Hans. Comments as Keynote Speaker at Biological Threat Reduction Conference 2002. University of New Mexico, 14-15 March 2002.

Chapter 4

Intelligence Community at a Crossroad

Transnational Threats: Top Intelligence Priority

The intelligence community is at a crossroad. In the last two decades, traditional military threats like the Soviet and North Korean militaries have significantly declined. At the same time, transnational threats have emerged. Despite over ten years into the post-cold war environment, the US national security establishment has struggled to define vital US interests. The most dangerous threats have not always been clear despite US military and diplomatic forces working in overdrive to deal with regional and humanitarian crises in Somalia, Haiti, Iraq, East Timor, and Kosovo. The terrorist events of 9/11 have significantly highlighted new dangers associated with formerly murky threats. This has helped focus the national security establishment and specifically the IC on what are now recognized to be transnational threats to vital US interests. Transnational threats, long on the list of concerns of US intelligence, have been elevated in priority relative to traditional military concerns. Bioterrorism represents one potential transnational threat to the US.

Because the bioterrorism threat is real and can be classified as a potential weapon of mass destruction, dealing with it should be a high priority intelligence mission. Transnational threats like bioterrorism create new challenges for intelligence professionals. As was discussed in Chapter 1, because transnational threats operate in geographically and functionally diverse arenas, they require coordination across a diverse set of organizations trying to counter them.

Before discussing support and functional intelligence challenges, three underlying factors have limited the community's effectiveness in post cold war environment: attack from detractors, community inertia focusing on enemy capabilities versus intentions, and community

organizational barriers. Recognizing factors that create drags on intelligence effectiveness is important in understanding how the US can improve intelligence operations to include counter-bioterrorism missions.

Community Under Attack

Many pundits would argue that the current US IC might be incapable of countering future transnational threats. The list of well-publicized intelligence failures and embarrassments is long and fresh in America's conscience. Just a few examples include the Ames, Hansen, and Montes spy scandals, the surprise Indian nuclear test in 1998⁵³, and the failure to prevent terrorist attacks, including the terrorist attacks on US forces in Saudi Arabia, the US embassies in Africa, the USS Cole in Yemen and the attacks of 9/11.

There were no doubt failures during the Cold War, but the “*raison d’etre* of the intelligence community was never seriously questioned.”⁵⁴ Perhaps for every failure there are untold stories of intelligence successes—many of which we will never learn. Richard Betts, in his recent *Foreign Affairs* article titled “Fixing Intelligence,” illustrates the US intelligence community’s failure dilemma with an analogy to Major League Baseball’s best hitter.

The awful truth is that even the best intelligence systems will have big failures. The terrorists that intelligence must uncover and track are not inert objects; they are living, conniving strategists. They, too, fail frequently and are sometimes caught before they can strike. But once in a while they will inevitably get through. Counter-terrorism is a competitive game. Even Barry Bonds could be struck out at times by a minor-league pitcher, but when a strikeout means people die, a batting average of less than 1.000 looks very bad indeed.⁵⁵

There should be little doubt that the IC was a key weapon in winning the Cold War.⁵⁶ Russian military forces were under constant surveillance and the US clearly understood their

capabilities. The US built superior weapons, in part because US intelligence helped defense contractors build tanks, aircraft, and ships that could exploit enemy weaknesses. US precision combat strikes in Iraq, Kosovo, and Afghanistan would not have been possible without exceptional intelligence.⁵⁷ The community was instrumental in preventing terrorist plots that target New York City's tunnels in 1993, US jumbo airliners operating in Asia in 1995, millennium celebrations on the West Coast, and US forces in the Middle East in the summer of 2001.⁵⁸

The unrelenting criticism leveled at the intelligence community has distracted the community from doing its job.⁵⁹ One example is criticism of the community's relationships with unsavory characters who are paid sources of information. Many argue this has led to degradation of Human Intelligence (HUMINT) capabilities. (See detailed discussion in Chapter 6.) One of the wisest decisions the President and Congress made following the events of 9/11 was to indefinitely postpone an "intelligence investigation" on why the community failed to prevent the attacks. Investigations consume energy and resources. They also create a risk adverse environment. In the case of 9/11, an investigation could have diverted intelligence resources needed to help prevent further attacks and prepare for war in Afghanistan. On the other hand, investigations can serve an important purpose by identifying weaknesses and incompetence. However, they should be limited in scope and their timing should never adversely impact intelligence operations during wartime. Critics of the IC are not likely to go away. While they can serve a useful purpose, they should take a more balanced approach when grading the IC. The community must rise to the challenge of providing the nation with the best intelligence possible even in the face of criticism. The community leadership's masterful

performance in responding to the events of 9/11, despite some intense criticism, provides a model for future responses to perceived intelligence failures.

Must Understand Capabilities and Intentions

To effectively evaluate the bioterrorist threats intelligence professionals have to approach the problem from both perspectives of capability and intent. The IC has historically been better at evaluating capabilities than intentions. Prior to the Gulf War, the US understood Iraqi military capabilities but failed to fully analyze Iraqi intentions concerning Kuwait. This led to surprise when Iraq invaded Kuwait in 1991. This weakness is due in part to US technical collection systems being more focused on monitoring capabilities of large military forces and the difficulty associated with “collecting the thoughts” of adversary leaders. The community has an organizational inertia geared for analyzing threats based upon capabilities versus intentions. Analyzing intentions of terrorist groups will prove to be critical for counter-bioterrorism mission.

In an international environment containing dangerous threats at the sub-national level, intelligence weaknesses in determining enemy intentions can expose a nation to attacks. On the surface, tracking the bioterrorism problem appears almost impossible. The Department of Defense, in its annual 2001 proliferation study, points out the difficulty in tracking BW threats “because virtually all the equipment, technology and materials needed for biological warfare agent research and development and production are dual use.”⁶⁰ This allows some states and sub-national organizations to easily hide weapons production and BW capabilities. Group intentions to use BW, while difficult to discover, may offer the only chance at recognizing a warning.

So the IC must first try to determine what countries or groups have the capability to execute a biological attack. The list will constantly change and should be prioritized based upon

which country is best equipped to conduct an attack. Second on more importantly, the community should assess those on this list for their intent to use biological weapons. Previous discussion on trends in terrorism (See Chapter 3) is pertinent to such work. Additionally, assessing cultural intelligence (See Chapter 6) as it relates to those on the capability list will help assess the overall threat. Combining an assessment of capabilities and intentions will yield rich intelligence on possible bioterrorist.

For example, it is unlikely that the IRA would use BW even if it had the resources and technical capacity. Using BW could cost it international sympathy and support. On the other hand, Al Qaida may be willing to employ BW but lack the capability either due to funding or technical limitations.⁶¹ Groups that seek or have a BW capability and have shown intent to use should receive the highest attention of the US IC. This list should not be that long and, while it needs to be constantly evaluated and updated, should play a key role in focusing intelligence activities on those groups that require intense scrutiny. This could save numerous collection resources from unnecessarily gathering information on improbable threats.

Breaking Community Organizational Barriers

Because of the emergence of transnational threats, the IC needs professionals from multiple intelligence disciplines and disparate organizations working the same problem as a team. This team needs a clear mission leader to set priorities and directing operations. The most logical choice would be the Director of Central Intelligence with an organization lead from the National Counterterrorism Center.⁶² This sort of cross-agency effort requires technological connection, organizational commitment, and a highly trained and flexible workforce. Most importantly, for the IC to be internally and externally connected, and therefore be proactive and effective, it will require visionary and risk tolerant leadership.

In many cases, because of complex and overly protective security classifications, specialists cannot talk, share, or collaborate while working a similar mission such as bioterrorism. It is even more difficult to talk with traditional military customers. It is almost unheard of and impossible to share freely information with coalition and non-traditional intelligence consumers such as non-governmental organizations and other agencies. There are recent cases where certain intelligence agency analysts were prohibited from participating in appropriate classified chat sessions with coalition partners for fear of possible compromises. No one quantified the lost opportunity to share information and subsequent impact on operations.

The reason for not sharing data is more often than not an over reliance on risk avoidance when it comes to security. This is clearly a leadership issue. The cost of not sharing information and impeding the flow of critical and even non time-sensitive information is often not a key factor in determining information sharing arrangements. While protection of sources is vital, there may be times when risking the loss of a source is worth the cost when compared to potentially improving the analysis and information production by increased sharing of data. Leadership needs to be more risk tolerant in the effort to improve the flow of information. Stranded intelligence is of no value if it does not add value to mission accomplishment.⁶³ Protection of a source that produces information that never reaches a consumer is an exercise in futility. A new emphasis on risk tolerance should be applied to intelligence dissemination and sharing efforts. This will help eliminate organizational barriers that prevent seamless data sharing—a critical component for success in today's information intensive environment.

Policy barriers that impede flow of information need to be reexamined. Technologies exist today to allow intelligence specialists at every level to communicate instantaneously with other specialists and customers who apply information to a mission requirement. Microsoft's

NetMeeting allows families on personal computers to instantaneously share pictures, video chat, and review documents together--the IC could use an even more sophisticated system. While the community's infrastructure needs to be continually upgraded, it has the resources to create an environment of more freely flowing information.

Community leadership can begin to eliminate barriers by creating a culture of collaboration versus a reorganization campaign. Reorganizations are a lot like investigations, they can take a lot of time and their purpose more often than not is counterproductive. Leadership can create a collaborative culture by rewarding individuals and organizations that most effectively execute the transnational mission threads across a diverse landscape of mission players and organizations. In addition to the normal daily interactions, this includes encouraging periodic information and personnel exchanges, face-to face visits, and tours of respective operations. Such initiatives will foster team spirit along a mission thread despite multiple players from multiple organizations. More importantly, it will help establish a new culture that can foster world-class intelligence on a complex transnational threat.

Notes

⁵³ Best, Richard A., Jr. "Intelligence Issues for Congress" Congressional Research Service Issue Brief for Congress: The Library of Congress. January 2002.

⁵⁴ Falkenrath.

⁵⁵ Betts., 44

⁵⁶ Cooper, Mary. "Overview: After the Aldrich Ames Spy Scandal." *Congressional Quarterly Researcher*. Volume 6, No. 5. p. 100.

Notes (continued)

⁵⁷ There have no doubt been mistakes associated with precision bombings during these conflicts. The bombing of the Chinese Embassy during the Kosovo conflict is the most notable example. These mistakes were only temporary diversions and had no impact on conflict outcome.

⁵⁸ Betts, Richard K. "Fixing Intelligence". *Foreign Affairs*. January-February 2002.

⁵⁹ Mark.

⁶⁰ Office of the Secretary of Defense. January 2001.

⁶¹ The capacity of Al Qaida to employ biological weapons is currently being investigated by intelligence community. USCENTCOM has acknowledged in press conferences that BW/CW related equipment was discovered at Al Qaida sites in Afghanistan. For more information see "Biowar Fears Cloud US War Success," MSNBC Website. Available <http://msnbc.com/news/627086.asp>. (Accessed 23 March 2002).

⁶² The National Counterterrorism Center brings together assets from the CIA, FBI, State Department and other elements of the intelligence community to collectively work terrorism issues.

⁶³ In his book, *The Secret War Against Hitler*, author Bill Casey defined stranded intelligence as information that is collected but never disseminated to a consumer. Even in World War II, stranded intelligence was seen as a major problem with the intelligence process.

Chapter 5

Improvements to Intelligence Foundation

The IC needs to improve its foundation if it is going to effectively tackle transnational issues like bioterrorism. There are three primary areas for improvement. They include fostering a more dynamic customer relationship management strategy, applying state-of-art information management systems, and adopting a more progressive human resource strategy. These areas form a foundation upon on which a strong intelligence system can effectively operate. Each one needs to be dynamically managed and allow flexibility in response to a constantly changing international environment. Improvements in these areas will benefit all intelligence missions.

Customer Relationship Challenges

The primary objective of the IC is to maintain and improve an intelligence system that is continuously focused on customers' missions. Intelligence is meaningless unless it gives a policymaker or policy implementer an information advantage in completing their specific task or mission. Historically, intelligence flowed within a well-defined linear approach.⁶⁴ Consumers provided requirements to designated collection managers (usually organized by geographic theaters) who would then task collection organizations from multiple intelligence disciplines - Imagery Intelligence (IMINT), Signals Intelligence (SIGINT), and HUMINT to collect the information. Once collected, the data was typically reported to all-source analysts who then produced comprehensive reports sometimes known as finished intelligence. While this process may still have some value, given limited collection resources, it has two major flaws—it is not timely and it often may not satisfy the specific requirement the consumer originally levied. Additionally it can lead to the collection of “interesting” information that some organizations

turn into finished intelligence that customers have little of no need for -- needlessly “burning up” precious analytical resources.⁶⁵

To avoid these collection and production inefficiencies, intelligence organizations, both collection and analytical, must clearly understand both the customer’s mission and their ever-changing information needs. Intelligence specialists should focus not only on the information the customer needs but also on the context in which the customer will apply it.⁶⁶ Army Special Operations troops working counter-drug operations will need different types of intelligence based upon the different phases of their operation. During pre-deployment planning, they need the background intelligence on the deployment area to include terrain, transportation routes, capability of enemy forces, and overall enemy intentions. During the execution phase of their mission, their intelligence requirements become more granular and may change on a daily basis. One day they may need surveillance information on specific city blocks, including where the enemy can hide or escape. The next day they may need detailed data on helicopter landing zones in specific rural areas.⁶⁷

Such a sharper focus on a customer’s needs cannot be accomplished without constant intelligence-customer interaction supported by cutting-edge information management tools and techniques. Intelligence organizations should have dedicated customer relationship managers and specialists in continuous contact with consumers to ensure products and services are hitting the mark. They should be asking: What information gaps do customers have? What keeps customers up at night? These intelligence organizations, whether collection, analytical or others, should have the ability to tap outside experts at a moment’s notice to service customers needs.

Such close and even informal working relationships will dramatically enhance the flow of information. It will also lead to ever-improving products and services. In the Army Special

Forces example above, instead of digging through a thick report to find an answer on landing zones, the planner or tactical intelligence officer can e-mail or open an Internet chat session with a terrain analyst for that area and collectively they can determine the best helicopter landing zones. Besides saving time, such an informal network will train analysts on a customer's real information needs, improving focus on future projects. It will also help eliminate "stranded intelligence"—information collected but never disseminated or used. Such an environment will foster discussion groups, topical or mission-related Internet chat rooms (already very popular for transmitting real-time intelligence), or subscription services. In his study *The New Craft of Intelligence*, Robert Steele calls this information sharing system the diamond approach where customers, collection managers, collectors, and analysts all have direct access to one another.

Aggressive customer relationship initiatives like adopting the diamond approach for command and control will be vital for transnational missions like counter-bioterrorism. Transnational threats involve groups that are smaller, have lower signatures, can move quickly, and change tactics at a moments notice. This results in an environment where nuances matter more for transnational threats than traditional threats. A single Russian bioengineer traveling to a hostile country may be incredibly more significant today than 20 years ago. Increased interaction with intelligence professionals and their customers will help highlight such nuances and their potential significance. A good customer focus will also help shape effective information management and human resource management strategies.

Information Management Initiatives

Building a dynamic customer relationship management system is not possible without an equally dynamic information management system to support it. In addition to supporting improved intelligence-customer relationships, a dynamic information management system will

create additional benefits to all intelligence mission areas. It will help expand the intelligence knowledge base by facilitating information sharing with outside experts and improve access to open source material. It will also help the IC more effectively manage tactical and national intelligence integration. Finally it will contribute to the development of better analytical tools.

Today the business community has surpassed the government in key information management initiatives. Advances in computer technologies have allowed commercial enterprises such as customer marketing and telecommunications management firms to improve their ability “to process, analyze, and manipulate very large, heterogeneous multi-source databases”⁶⁸—a key requirement for the IC considering its remarkable dependence on information.⁶⁹ The IC must adopt commercial information management practices to become more efficient.

Executing any transnational mission like counter-bioterrorism in the IC will require access to an expanded list of available resources and partners.⁷⁰ Some of these include open source materials, foreign intelligence exchanges, and law enforcement experts of other US government agencies. Connecting the players and fostering a seamless work environment are keys to combating bioterrorism. The interagency process associated with countering bioterrorism is so complex that innovative information management tools are required if the US expects to effectively defeat the threat.⁷¹

Need for New Information Structure

Experts studying the information requirements as they relate to bioterrorism state that “correcting this problem will require nothing short of a revolution in the information management of the full IC, demanding a near total overhaul of its technological systems and security rules, new institutional structures, and a new generation of analysts and information

managers with very different skills.”⁷² Such drastic change are near impossible in any government bureaucracy and, to be fair, the IC was well on its way to adopting new information management initiatives prior to 9/11. Now they must expedite adoption and implementation of an improved information management system.

Intelligence personnel working the bioterrorism mission thread immediately need a robust capability to communicate while performing their daily tasks. Such an interconnected “bioterrorist” community of interest will make information more readily available, transferable, and actionable--all critical requirements if the community is going to effectively combat bioterrorism.

In 1997 the Defense Science Board began advocating a new Global Information Infrastructure to enable the US government to meet unique challenges posed by transnational threats. Their study presented a comprehensive list of system requirements that are still applicable today. They called for a system that provides:

an interactive, two-way global information system that would expand the available sources of information. This system would support gathering more data from the bottom up, exploiting international information sources, and two-way sharing of critical information with state, local, and international partners. It is also important to do net assessments on the transnational threat and US responses – to look at long-range moves, countermoves, and capabilities, and to evaluate US response capabilities over time. An analytic framework and better analytical tools are needed for planning and assessing the effectiveness of capabilities to gather, process, and disseminate information about these threats.⁷³

The idea is to build multi-tiered security architecture and two way distributed information system that, for example, would allow the Immigration and Naturalization Service officials to continuously share information with intelligence analysts tracking potential bioterrorist.⁷⁴ Such a Secure Transnational Threat Information Infrastructure will help ensure the full resources of governments, industry, and academia are “brought to bear on topics of common concern” such as

bioterrorism.⁷⁵ The improved structure includes technology and concepts. A successful example of such an information system is the US RIONET, designed to support counter-narcotics operations. The system demonstrates how the integration of information systems from multiple sources can bolster execution of a transnational threat.⁷⁶

There is some concern that commercial applications will not effectively work for the government, especially when dealing with national security issues. While there are unique security requirements for national security, private industry has integrated security into its information technology management. The IC may have to apply reasonable risk management principles when integrating the best commercial applications. This will involve analyzing trade-offs between robust information capabilities and security concerns.

While the technology for information management improvements exists, officials need to see that it is aggressively implemented. The more daunting challenge is the development of doctrine, policies, and tactics that leverage this technology. This may include relaxing some policy and security measures in the pursuit of better information sharing between intelligence specialists and their customers—a step sure to enable more effective prosecute the counter-bioterrorism mission.

Need For Dedicated Information Managers

It is time the IC develops information management specialists (with a mix of skills as a intelligence specialist and computer/communication specialists) who are trained and focused on efficiently managing information and fostering collaboration between intelligence professionals and customers. These professionals would serve as a bridge between the users of intelligence information management tools and technical professionals who install and maintain them. That would make sure not only the right tools were being used but help design and implement smart

information management tactics, techniques, and procedures. Information management is so critical it needs to become the full time job of dedicated intelligence professionals and the primary mission of sections within intelligence organizations. Such a commitment will ensure that the community is harnessing the full potential of information technology.

This could initially lead to increased cost but it could save money in the long run. One of the biggest and most costly shortfalls of recent information technology management initiatives has been an obsession with technology.⁷⁷ The IC has bought more technology than it really needs. In just about any intelligence operations center one can find “computer boxes” gathering dust. Intelligence professionals do not need more technology tools. They need tools that add value to their core competencies. Information managers could not only help them pick and develop the right tools, they could help eliminate unneeded and costly ones.

These information managers would help build a foundation for virtual counter-bioterrorism teams to include supporting functional missions of intelligence specialist. They would help collectors communicate more effectively with operators by developing improved concepts with users and picking the best technology with the help of system developers. They would help analysts producing background intelligence products distribute them quickly and in user-friendly formats to operators and decision makers. They would ensure that information is efficiently stored and available in a format for quick turnaround. They would help real-time intelligence collectors turn the results of the work into an information service for operators. In short, they would make sure that the intelligence system is efficient and continually monitoring the changing target environments.

Information Brokers

A related idea that should be explored is development of a team of information brokers—people who know all information sources available to apply to bioterrorism mission. These brokers would know who is the foremost expert in a particular field and could contact them on an as-needed basis. They would clearly understand the needs of a customer of bioterrorism products and alert them when valuable information can be applied to on-going missions. This obviously means brokers are closely tied to counter-bioterrorism operators from law enforcement, DoD and others. Information brokers would be different than information managers. Brokers would be focused on energizing the daily flow of information between intelligence professionals and consumers. Information managers' focus would be more long term, making sure the right infrastructure is in place for information brokers to do their job.

The Central Intelligence Agency (CIA) network of “Reports Officers” is a good current example of a community initiative to energize the flow of information. The officers review, prioritize, and distill collected information for timely distribution.⁷⁸ The community needs to look to other industries that have successfully employed the concept of information brokers and follow the models to include lessons learned.⁷⁹

The role of that of a financial broker is a good model to emulate. Financial brokers serve as a bridge between customers, and financial analysts and investment products (stocks, bonds, insurance). If a customer needs information, brokers help them get it. If the customer has simple questions, brokers can answer it on the spot. If the question is more complex, brokers can put customers in contact with financial experts or provide detailed reports. If a customer wants to buy a product, the broker has a network in place to get the right product for the best price. Such as system could enhance and streamline intelligence operations for transnational missions like

counter-bioterrorism. For example, a bioterrorism information broker could assist an Air Force C-130 squadron intelligence officer who is responsible for preparing aircrews supporting a domestic response to a bioterrorist attack. The broker could alert the intelligence officer to the details of the threat at hand, to include potential symptoms, making sure crews are attuned to hazards. The broker could recommend acquisition of intelligence products to provide more detailed information. If necessary, the broker can acquire and distribute the information for the intelligence officer. The broker would know where to get the information and be able to obtain it more efficiently than a squadron intelligence officer.

Information brokers would also have input into information management security decisions with the purpose of documenting the “information opportunity cost” of not connecting various players in the counter-bioterrorism mission. For example, intelligence analysts may want better connectivity and information sharing privileges with outside experts on the Plague. These experts may work at universities, biotech labs, or government labs outside the traditional ring of security. In conducting a security cost benefit analysis of such arrangements, information brokers could help quantify what information gaps would result without connection and information sharing. This could help leadership make a more informed decision. In the end, they may decide the security risk is too great, but at least they will fully understand the “information opportunity cost” of not connecting and sharing.

Human Resource Challenges

One of the keys to a strong intelligence foundation is a highly trained and motivated workforce. The rapidly changing international environment combined with the emergence of transnational threats requires a more progressive human resource strategy that produces the necessary expertise to deal with threats like bioterrorism.

Many of our bioterrorism analysts have virtually no formal training or practical experience in the biotech field. The intelligence community's traditional philosophy of hiring college graduates and growing its own analysts through in-house training and on the job experience is hampering its ability to build proactive bioterrorist initiatives.⁸⁰ The community can no longer depend upon on-the-job training to effectively develop analysts in the new high tech environment that analysts have to evaluate. The community needs to use biotech experts in every part of the intelligence cycle to help ensure effective mission accomplishment.⁸¹ A human resource strategy complimentary to the current one would be to hire some analysts at the mid-career point after they have achieved personal standing and complete fluency in the biotech or bioengineering fields at the expense of the private sector. One can make a strong argument that it is easier to train a biotech expert in the area of intelligence analysis than it is to train an intelligence analyst deeply in the subject matter of biotechnology.⁸² This will no doubt require substantial increases in salaries but if the community wants to effectively fight bioterrorism, it needs some of the top authorities in the biotech field working for the community full-time.⁸³ In this environment, some junior analysts could train under true experts in the field. In the end we need a good mix of both expert scientists and expert analysts.

Another way to increase the analytical talent would be to provide intelligence analysts study fellowships at leading academic institutions or internships in biotechnology firms to ensure we have personnel in touch with the cutting edge biological and scientific technologies and methodologies. If intelligence analysts spent one year working with companies that manufacture and use aerosol delivery systems, they could develop an expertise in what many believe to be the most likely delivery method of biological weapons. At the same time, they could develop a network of outside experts that could be utilized as information sources for years to come. Some

intelligence agencies send analysts to universities for regional studies. The community needs similar, albeit smaller, programs for biological sciences.

The IC also needs to foster the development of Intelligence Studies programs at American Universities, creating a quasi “intelligence community reserve officer training corps.” The community could use these programs as recruiting and training grounds for its most critical human resource requirements to include the biological sciences and information technologies. They could also help prepare the future work force for basic analytical and communication skills with a focus on intelligence related work. Some universities may eschew any connection with the community, but others are more focused on preparing students for specific government careers and would be open to IC help.⁸⁴ This could also foster improved language training, cultural intelligence studies, and basic information technology skills. The community should strive to create a culture on our campuses that respect and understand the vital intelligence mission of our nation. The best example of such a program is Mercyhurst College in Erie, Pennsylvania. As part of its History Department students can concentrate on a Research/Intelligence Analysts Program. When students from this program graduate, they have a reading competency in a foreign language, understanding of US and world history, knowledge of comparative governments, skills in oral and written reports based upon research correlation and analysis, and familiarity with computer skills and statistical techniques. The community is spending precious resources on new recruits to provide some of the same training. It will be worth the effort to assist in developing more programs along the model of Mercyhurst College to help tackle today’s and tomorrow’s complicated intelligence problems.⁸⁵

The IC could also reach out to universities that desire a lower profile relationship. The community could offer to send experts, including select retirees, to University international

relations and studies programs as guest speakers and lecturers. The speakers could serve to educate students on the role US intelligence in the world and create an interest in an intelligence career.

Notes

⁶⁴ Steele, Robert David. *The New Craft of Intelligence: Personal, Public & Political*. OSS International Press. 2002.

⁶⁵ Steele.

⁶⁶ Steele.

⁶⁷ Author's interview with Army Special Forces regional specialist, Miami Florida 15 March 2001.

⁶⁸ Falkenrath.

⁶⁹ Best.

⁷⁰ Office of the Undersecretary of Defense for Acquisition and Technology.

⁷¹ Falkenrath.

⁷² Falkenrath.

⁷³ Office of the Undersecretary of Defense for Acquisition and Technology.

⁷⁴ Office of the Undersecretary of Defense for Acquisition and Technology.

⁷⁵ Steele.

⁷⁶ Office of the Undersecretary of Defense for Acquisition and Technology.

⁷⁷ Steele.

⁷⁸ Report of National Commission on Terrorism. "Countering the Changing Threat of International Terrorism" Pursuant to Public Law 277, 105th Congress, June 2000, 16.

⁷⁹ Robert Steele, an intelligence expert and author of *The New Craft of Intelligence Personal, Public, & Political*, in calling for "new rules of engagement" in the intelligence community refers to information brokers as experts that "know who knows" about who can best collect on, analyze, or comment on a given area of interest.

Notes (continued)

⁸⁰ Steele.

⁸¹ In interviews with current DoD analytical personnel, there was some difference of opinion on just how much scientific expertise is needed in the analytical realm. The more senior analyst definitely felt more scientific help was merited. The more junior analyst pointed out that the focus should be on dramatically improving collection (specifically HUMINT) and without more collection there will be a shortage of scientific and technical data for experts to analyze. In fact, both are right and that the community should be improving HUMINT collection (priority one) to support counter-bioterrorism efforts while at the same time the building a strong analytical corps (priority two) capable of correlating and assessing complex issues (cultural and technical) associated with bioterrorism.

⁸² Steele.

⁸³ Steele.

⁸⁴ University of New Mexico Intelligence Studies Program Draft Pamphlet. March 2002. The University is developing both undergraduate and graduate curriculum to prepare interested students in the critical thinking and analytical skills with emphasis on the intelligence work. Part of the motivation behind the program is to give UNM students a professional advantage in competing for intelligence community jobs. Mercyhurst College in Erie, Pennsylvania offers the most comprehensive intelligence study program in the US.

⁸⁵ Mercyhurst College academic website. Available <http://www.mercyhurst.edu/Academics/riap.htm>.

Chapter 6

Functional Intelligence Improvements for Transnational Challenges

Over the last 50 years the US IC designed collection and analysis systems to target industrial sized NBC weapon manufacturing facilities primarily in the Soviet Union. Analysts depended on highly classified information from US collection systems—mostly national technical means. This yielded vital information but it could also miss nuances associated with transnational threats. As the Russian and Iraqi cases make clear, even US intelligence efforts to detect and analyze state programs has been less than perfect.

In general, intelligence systems were not equipped to detect, locate, and analyze small-scale BW programs of the sort that smaller transnational groups would maintain.⁸⁶ In addition, collection efforts paid little attention to open source information that could help identify communities most likely to foster terrorism or identify groups that at least discussed BW as potential tools in their arsenal.

With an improved intelligence foundation, the IC will be in a better position to implement new collection and analytical initiatives that will bolster counter-bioterrorism efforts. Better collection and analysis against potential bioterrorist is imperative and attainable. Integration of Open Source Intelligence (OSINT) will reinforce both collection analytical improvements.

Collection Challenges

The IC faces an uphill battle in its campaign to help counter bioterrorism—especially with a traditional collection system. As has been discussed, state BW programs are almost impossible to detect without an effective BWC verification system. While states can disguise programs inside of legitimate biotech facilities, the problem is even more challenging with non-

state actors. Their operations are likely to be smaller in scope and not have the same security and safety signatures that larger state programs have. Additionally, these bioterrorist groups can be more mobile and can operate almost anywhere in the world including the US. Aum Shinrikyo freely operated a BW laboratory right under the nose of Japanese authorities.⁸⁷ These pose daunting challenges for US intelligence collection but there are some steps the community can take to improve chances of detection.

Surprise! HUMINT is Critical

In the past year HUMINT has probably received more attention than any other intelligence issue. The media and other pundits have labeled it as the “silver bullet” for many intelligence shortfalls. Former and current intelligence experts that have focused on transnational issues are unanimous--HUMINT is the key to effectively counter bioterrorism. The good news is that US leadership has recognized the gapping holes in the nation’s HUMINT capability and is committed to addressing it.⁸⁸ The bad news is that restoring this capability is complex and time consuming, and HUMINT often fails to deliver meaningful intelligence—so it is no silver bullet. Unlike other collection disciplines, where applying resources almost guarantees a flow of collected information, developing a HUMINT capability takes years. The penetration of terrorist organizations, especially at the necessary level to gain valuable information, is difficult. Most organizations are small, disciplined, and alien. Finding a reliable US citizen willing to devote unknown years of his life and face the risk of death to gain access is not easy. Recruiting foreign sources may offer better chances of success but their reliability will always be an issue.⁸⁹

Even given these challenges, it is vital to restore US HUMINT capabilities. There are two things the United States can do to make HUMINT stronger. First, the community can ensure

that all HUMINT operations are well integrated with other collection disciplines and intelligence functions. Because it takes years to develop and is a high-risk endeavor, the IC must ensure all HUMINT operations are precisely targeted against key threats. The ultimate goal is not simply to increase the quantity of HUMINT operations, but instead to develop precise operations that yield high quality information that cannot be gathered from other collection disciplines. These disciplines include Open Source Intelligence that can help analysts discover the most likely sources of terrorism by reading local newspapers from foreign communities that spawn terrorists.⁹⁰

Second, the IC should be allowed to operate aggressively when recruiting informants with unique access to terrorists' plans and intentions. This may include putting actual terrorists and criminals on the US intelligence payroll. US law enforcement is routinely allowed to recruit criminal informants in order to pursue other major criminals. Working with these informants by no means suggests that the IC condones either the terrorists' past or future behavior. But if these unsavory informants can provide information to prevent terrorist attacks and save lives, a greater good will be served by working with them.⁹¹

If nothing else, increased HUMINT activity will help deter and even slow potential terrorists because they can no longer discount aggressive infiltration attempts of their group. While terrorists have always assumed enemy infiltration attempts, US enemies can be assured that the US is intensifying efforts to penetrate their groups. This intensified level of operations will increase their paranoia, security cost, and may decrease morale by creating an environment where no one can be trusted.

Almost every article and interview used in this research pointed to a need for better HUMINT as the number one tool to improve community efforts against bioterrorism.⁹² Despite

its complexity, latency, and uncertainty of success, it still offers the best long-term capability to deter and preempt terrorism. According to Richard Betts the “essence of the terrorist threat is the capacity to conspire.”⁹³ To this day the best way to counter them is through systematic HUMINT operations including penetrating their organizations, discovering their plans, and identifying the key players. Using this information, they can be eliminated by a variety of military or covert actions.

Super Collection Managers

More often than not intelligence collection works best when HUMINT, SIGINT, MASINT and IMINT work together to solve a problem. Traditionally, these disciplines were “stovepiped” along agency lines, often resulting in little coordination and even duplication of efforts.^{94 95} Over the last several years, great strides have been made to integrate these capabilities while working on various mission threads. Despite improvements, it is time to take collection integration to another level. The community needs to develop “super” collection managers with broadly expanded responsibilities. They should not only have tasking authority of selected traditional resources (authority they currently have) but authority to buy a wide variety of information to include commercial imagery and information from Internet resources. They should also have the capability to direct real-time collaboration and cooperation among the diverse collection resources to accomplish a specific mission.⁹⁶ HUMINT, SIGINT, Measurement and Signatures Intelligence (MASINT), and IMINT collectors on the front lines need to have continuous access to each other as well as “super” collection managers. Bioterrorist information brokers can serve as a bridge between these new collection managers and the customers they support. Like many other initiatives, this will require new information technologies and information management procedures. If “super” collection managers have

authority and capability to satisfy collection requirements through new and cheaper sources, this could free-up the more expensive and over-tasked classified collection systems, ultimately saving resources.

Analytical Challenges

Some former intelligence professionals feel the craft of analysis has been neglected in the IC. The House Permanent Select Committee on Intelligence has expressed concern about “a largely inexperienced workforce, lack of language skills, and limited in-country familiarity” when discussing IC analytical woes.⁹⁷ Some say this situation has crippled the IC’s ability to make comprehensive assessments, arguing that the true value of intelligence comes from analysis, not secret collection.”⁹⁸ As discussed earlier, there are specific acts along a timeline a bioterrorist must execute to successfully deploy a weapon. Understanding this process and its nuances is critical if intelligence analysts are to be effective in supporting counter-bioterrorism efforts.

The IC has shortfalls in scientific and technical analysis necessary to tackle complex bioterrorism issues.⁹⁹ It also needs to make better use of existing analytical tools that add value and eliminate duplicative systems. The community must develop a system that ensures production of the most critical background intelligence. Finally it needs to develop a new focus on cultural intelligence in applicable assessments

Leveraging Outside Expertise

Successful prosecution of the bioterrorism mission will require a more thorough understanding of the threats and necessary capabilities to effectively employ bioweapons. Today’s IC, especially on the military side of the business has taken a more generic focus on weapons of mass destruction (WMD) requiring analysts to be masters of the biological, chemical

and nuclear threats. Frequently, resources were too thin to develop robust WMD analytical expertise. Even today WMD experts are rare in the IC and there are even fewer who are true bioterrorist experts.¹⁰⁰ This often results in general reporting that lacks clarification and is difficult for customers to apply.¹⁰¹

As stated in Chapter 5 Innovative Human Resource Strategies, in some cases these analysts need a scientific background to be able to analyze the process. As an example, only a scientist who has the detailed knowledge and necessary skills to develop genetically engineered bio weapons could review a list of scientists and their backgrounds to assess the real capabilities of that group.¹⁰² Another example discussed earlier, where technical expertise would be critical, would be in evaluating threat capability based upon feasibility of aerosol dissemination. An individual with engineering experience in such equipment could evaluate purchase orders, licensing requests, or shipping data to determine if groups have this critical biological dissemination capability.

The IC needs to recruit and cultivate some of the top experts in the biotechnology field to serve as intelligence analysts. This could help create a situation where personal reputation becomes as visible, if not more so, than organizational reputation. People seeking knowledge and answers gravitate towards experts. Dr D.A. Henderson is a good example. He is a leading expert in the fight against infectious diseases. His expertise is sought due to his personal reputation versus the fact that he is Director of the Johns Hopkins Center for Civilian Biodefense Studies. The IC should recruit biotech “intellectual magnets” that private sector experts will gravitate toward, furthering increasing the free-flow of information.¹⁰³

The scientific and technical analytical experts could focus on nailing down group BW capabilities. Cultural intelligence analysts could focus on assessing intentions. Senior analysts

would focus on relationships between terrorist capabilities and intentions as well as ties to states with biological weapons to assess overall threat.

The community needs to build cooperative relationships with the private sector and universities to ensure the brightest minds are applied to the menacing threat of bioterrorism. In addition to permanently hiring some of the best in the biotech community the IC must build a web of collaboration with non-government entities on the front line of the biotech industry. The national expertise in biotechnology that is resident in academia and industry is the most extensive in the world.¹⁰⁴ US federal labs are already working closely with these scientists and some close government cooperation already exists. Additionally, the community should solicit their support in open source intelligence efforts in determining journals and publications of interests.

Another promising idea related to engaging the private sector is to make these groups part of an extended intelligence virtual working groups normally working at the unclassified level and at a classified level in cases of extreme emergencies. Given the uncertain nature of potential bioterrorism due to advances in genomic research, those working biodefense issues are entering a potentially uncertain era. Bioengineers equipped with genetic blueprints have ushered in an era of exponential growth in the field of biology, leading to potential exponential growth of threats.¹⁰⁵ Given the revolution in biology in the last 20 years, no government organization can hire experts in an infinite number of “impossible-to-anticipate” biological threat scenarios. One possible strategy is to develop a “scientific minuteman” corps of a number of experts who could serve as temporary consultants during peacetime and full-fledged partners during a bioterrorism crisis.¹⁰⁶

Tools to Do the Job

Analysts for this mission need to be focused and have the tools to do the job and be provided with the resources and opportunities to become experts in the biotech field. Due to the transnational nature of bioterrorism, geographically and functionally diverse events, from a wide variety of collection sources, must be tagged, correlated, and evaluated for relevance. These events need to be compared to indicator lists and placed in context with background intelligence to allow analysts to quickly identify anomalies and determine if they could signal a prelude to significant development or event. Automated pattern event analysis tools will be necessary to manage the information load and allow analysts to spend more time evaluating information than processing it.

Historically there have been few analytical tools available to allow current analysts to maximize their assessment efforts. As discussed earlier, it is not a lack of tools but a lack of the right tools that hold back analytical efforts. One solution would be to temporarily assign information managers to analytical cells and allow them to gather data on tool requirements first-hand. Based upon this first-hand evaluation of what type of tool would add value to the analytical process, information managers could work with information technology specialists to either select a commercial tool that satisfies the requirement or help them develop a new tool. Selecting commercial-off-the-shelf tools (COTS) should always be first choice. They are more supportable and almost always more user friendly. Analysts have little time to thoroughly document tool requirements, resulting in tools that “miss the mark.” Information managers can help make sure that tools are adding value instead of collecting dust.

The IC has more recently focused on developing tools that will allow analysts to quickly compare background intelligence (enemy doctrine, tactics and techniques, historical trends,

operational capabilities) with current intelligence (what the enemy is doing and has done in the last 72 hours). Other tools the community continues to pursue include data mining, data warehousing, intelligent agents for information fusion, intelligent data base triggers, and groupware to support distributed collaboration among analysts.¹⁰⁷ These tools will be critical to equip analysts engaged in counter-bioterrorism efforts.

Background Intelligence

Unfortunately resources for producing background intelligence often take a back seat to current intelligence efforts because, given limited resources, crisis operations must always be supported first. In the last ten years international crises and military commitments have strapped intelligence resources, leaving few resources available for in-depth intelligence work.

The lack of resources for background intelligence efforts (known in the IC as production) can lead to negative trends in the long term. Good background intelligence facilitates good current intelligence.¹⁰⁸ It should be easily retrievable and easy to fuse into current intelligence reporting. Analysts writing current reports can be more efficient when armed with background intelligence because they will have to do less research, they can quickly place current events in proper context, and even plug modules of pertinent background intelligence into current intelligence products. Another important point is that background intelligence should be focused on specific and on-going customer information requirements. The community should not simply produce background intelligence based on collection capabilities but should focus instead on specific customer needs.

Academia, industry, and government agencies not directly associated with the IC are better equipped for completing some types of unclassified study requirements. The community is pursuing such initiatives under a program known as Global Coverage and should continue

expanding them.¹⁰⁹ A good example where the community could use good background intelligence is epidemiological surveys. Such products could provide analysts with a baseline on disease patterns that could prove to be critical to in their efforts to survey the landscape for anomalies. While the IC cannot do these, it must encourage and in some case commission such studies.¹¹⁰

Background intelligence products need to be developed on what it takes to acquire, produce, maintain and deploy bioweapons to include required expertise, equipment, and materials. Such products will help analysts build indicator lists of what one would expect to see if bioterrorist operations are being initiated. Maintenance of this list would be a dynamic process as analysts become more sophisticated in assessing bioterrorist threats.

Cultural Intelligence

Equally important in assessing bioterrorist threats is assessing the intentions of suspect groups and the underlying factors that enable their recruitment, allow them to raise money, and justify using such dangerous weapons. This effort would overlap and leverage existing analysis of terrorist groups developed by more general IC terrorism assessments.

To effectively target transnational threats, the analytical community can no longer afford to focus solely on states and their actions. In today's global environment many of the activities in the religious, economic, and social communities are just as important to monitor for indications of emerging threats. Analysis must go two steps down to sub-actors within nation-states and non-government organizations to be effective in understanding cultural undercurrents.¹¹¹ Islamic religious leaders in both Pakistan and Saudi Arabia and drug kingpins in Latin America are all good examples of sub-actors who play major roles in transnational

issues. The US must do a better job of trying to understand what motivates them and more importantly paying attention to their motivations and intentions.

Some argue that to have an effective cultural intelligence capability, IC members must be native speakers and “have in-depth understanding of the history and religion” for their respective area of responsibility. At a minimum the senior analysts need to have this portfolio.¹¹² The community must put more resources in analyst language and cultural immersion programs, while at the same time recruiting a more ethnically diverse workforce that already speaks the language and understands the culture.

Credit for Continuous Customer Collaboration Reporting Stats

As discussed earlier the IC must build stronger customer ties. The issue is worth further discussion as it specifically relates to analysts. An analyst’s success should be directly tied to his or her customer’s success. Such a focus on teamwork on dealing with a common mission thread will help analysts focus efforts on a specific mission versus solely on their intelligence organization. Leadership should involve customers in the individual analyst’s evaluation process, reinforcing and institutionalizing individual mission thread loyalty. This loyalty is not meant to degrade the identity of intelligence organizations—in fact it will make organizations even more critical customer partners, elevating their standing in the IC. Such a mission-focused approach will lead to simplification in traditional reporting and dissemination.

In fact it will necessitate that analyst improve the timeliness and relevance of their work. Dissemination focus should shift from periodic reports to a continuous flow of information service reports (e.g. e-mails, chat sessions, discussion boards, video teleconferences, and computer desktop collaboration) resulting in precise transfer of intelligence that is “just in time and just enough.”¹¹³

Open Source Intelligence: Underutilized Source

In today's information-based environment, OSINT--newspapers, periodicals, pamphlets, books, radio, television and the Internet web sites--can no longer be considered an afterthought in intelligence collection efforts. Many of the countries and groups related to the bioterrorist problem are much more open about their objectives and what motivates them. While they may be secretive about specific biological capabilities, they often talk about their catastrophic intentions. In 1999 Usama Bin Laden publicly defended the right of Muslims to use NBC weapons.¹¹⁴ Another example of the value of open source material in assessing terrorist group intentions is Aum Shinrikyo. Throughout the 1990s, Aum Shinrikyo engaged in public discussions about NBC weapons via the Radio in Russia, on the Internet, and in a number of publications. Amazingly, the cult's public rhetoric coincided with a number of unsuccessful biological attacks in Japan. Yet US intelligence was not aware of the group until the deadly sarin attacks on the Tokyo subways in 1995.¹¹⁵ Admittedly, there may be more rhetoric than substance in terrorist press releases and propaganda, but the IC must factor it into bioterrorism threat analysis.

A number of activities related to the bioterrorism process take place in the commercial environment or unclassified government environment. The 1997 the US Defense Science Board referred to these sources as parallel information that may include transaction databases containing equipment and material purchases, shipments or permit applications or public health records. There is a distinct possibility that one of the 9/11 hijackers was treated for cutaneous anthrax in a Florida hospital in June 2001.¹¹⁶ Perhaps a better epidemiological surveillance network combined with interagency sharing of open source data would have alerted authorities to a potential threat.

Aggressive OSINT efforts can be a double-edged sword. While they may lead to a reduction in the need for classified collection efforts (spies and satellites) they most certainly will increase processing cost.¹¹⁷ This shift in balance from almost exclusive reliance on classified collection to more of a dependence on open sources should reduce work for overburdened national collection systems. In the long term, it could help reduce costs, because collection satellites are much more expensive than sophisticated processing equipment. But even if the number of satellites were reduced, it will take years to realize the cost savings from their reduction.¹¹⁸ In the short term, Open Source integration will increase the cost for processing and storage equipment that will filter the thousands of pages of unclassified information, automatically translate it for analytical review, and then tag and store it for future use. While more dependence on open source materials may not lead to cost savings, it will help create a more focused and less task-saturated environment for agents and satellites.

Notes

⁸⁶ Falkenrath.

⁸⁷ Falkenrath.

⁸⁸ Deutch, John and Jeffrey H. Smith. "Smarter Intelligence." *Foreign Policy*. January-February 2002.

⁸⁹ Betts.

⁹⁰ Deutch.

⁹¹ Report of National Commission on Terrorism.

⁹² Some examples include US government official interview with the author and subsequent correspondence, Miami Florida, 15 December 2001. Defense Science Board, 1997. Falkenrath, 283.

⁹³ Betts.

⁹⁴ Falkenrath.

Notes (continued)

⁹⁵ The term “stovepiped” is used to describe the lack of coordination among collection disciplines, especially at the working levels. In a worst case example a SIGINT collector and a HUMINT collector could be working on the same target, producing reports, and not even be aware of each other’s mission. The basic idea is that historically, a “stovepiped” environment organized along collection disciplines prevented synergy and mutual support between collectors. While many view this as a current problem, the intelligence community has dramatically improved information sharing among collectors from different disciplines—especially along common mission threads. However, there is more work to be done to eliminate “stovepipes.”

⁹⁶ Steele.

⁹⁷ Best.

⁹⁸ Steele.

⁹⁹ Author’s interview with current US government official, Miami Florida, 22 March 2002.

¹⁰⁰ Author’s interview and subsequent correspondence with current US government official , Miami Florida, 21 March 2002.

¹⁰¹ Combating Terrorism: Observations on Biological Terrorism and Public Health Initiatives, (Testimony, 16 March 1999, GAO/T-NSIAD-99-112), 6.

¹⁰² Fraser, Claire M. and Malcolm R. Dando, “Genomics and Future Biological Weapons: The Need for Preventive Action by the Biomedical Community.” Available at <http://www.nature.com>. (Viewed on 25 November 2001). Dennis, Carina. “The Bugs of War.” *Nature* Vol. 411. 17 May 2001: 223.

¹⁰³ Steele.

¹⁰⁴ Defense Science Board.

¹⁰⁵ Garrett, Laurie. “The Nightmare of Bioterrorism.” *Foreign Affairs*. January-February 2001. 76.

¹⁰⁶ Steele.

¹⁰⁷ Defense Science Board.

¹⁰⁸ Author’s interview with current US government official , Miami Florida, 22 March 2002.

¹⁰⁹ Author’s interview and subsequent correspondence with current US government official , Miami Florida, 21 March 2002.

Notes (continued)

¹¹⁰ Defense Science Board.

¹¹¹ Steele.

¹¹² Steele.

¹¹³ Steele.

¹¹⁴ Office of the Secretary of Defense.

¹¹⁵ Falkenrath.

¹¹⁶ MSNBC News Service, Biowar Fears Cloud US War Success. 23 March 2002. Available at <http://msnbc.com/news/627086.asp>.

¹¹⁷ Best.

¹¹⁸ Steele.

Chapter 7

Recommendations

US Response and Intelligence Community Recommendations

The US government must develop an aggressive and comprehensive strategy that includes deterrence, preemption, domestic response, and attribution. US intelligence must expand and develop capabilities to support each one of these sub-missions. It is likely that intelligence will be most decisive in deterrence and preemption.

The US IC was moving in right direction prior to 11 September in trying to effectively deal with transnational threats--just not fast enough. The tragic events have not only shifted policies but mindsets, providing the catalyst for changes that are necessary if the community is going realize success in countering bioterrorism.

Reorganization

The IC should avoid wholesale reorganizations or the creation of large new organizations. Reorganizations are exhausting and can become the primary focus of the workforce and consume precious resources at a significant cost to the mission. The primary objective of leadership should be focused on bringing the key players in the bioterrorism mission thread together virtually.

Mission Thread-Centric

The IC must become more mission thread-centric versus organization-centric. Virtual organization along a mission thread like counter-bioterrorism will create new synergies among organizations and functions. The interagency process will become the norm instead of the exception.

Fighting the Barriers

The community must continue to remove barriers to meaningful information exchange among sister intelligence agencies, between the community and other government agencies, and between the community and the private sector. Director Tenant said it best in the immediate aftermath of 9/11 in an effort to energize the agency's efforts in the war on terrorism—"If there is a bureaucratic hurdle leap it."¹¹⁹ The bioterrorism mission in the IC requires a similar sense of urgency to remove organizational barriers in order to more effectively deter or prevent attacks.

Information Management Transformation

Information management technology and procedures must receive more emphasis and resources in the IC. New technology is facilitating unparalleled opportunities to manage intelligence more effectively. Information systems have never been more important to creating actionable intelligence. The community needs dedicated information professionals to build "information bridges" and innovative procedures to maximize the timeliness, accessibility, and usefulness of intelligence to customers.

Innovative Human Resource Management

The IC needs to adopt more flexible human resource strategies to shape a workforce optimized to work the counter-bioterrorism mission. These strategies include recruiting world-class scientists, granting employee internships in biotechnology firms, and fostering the development of intelligence studies in the nation's universities.

Open Source Integration

The community should continue integrating and expanding OSINT in all aspects of intelligence operations. While there have been great strides in past decade, especially in the analytical area, information sources are exploding and the community will be challenged to

develop processing capabilities to separate the pertinent intelligence from the clutter of data. OSINT will prove to be a key contributor in providing background intelligence related to the threat of bioterrorism.

Intentions are Key to Deterrence

The community must put on a “full court press” to improve its ability to determine terrorist motivations and intentions. If the community can identify the most radical groups, it will allow an even more intense focus on determining potential bioweapons capabilities and help establish a web of deterrence around the most dangerous threats. Integrated HUMINT capabilities are key to this effort.

Integrated HUMINT

Once HUMINT sources are established, the community must ensure they are integrated with other collection disciplines and with tailored analytical teams. Revitalizing HUMINT is the most critical area for intelligence improvement but as the collection structure expands, equal attention must be placed on integration. Without integrated HUMINT, the best technical collection systems will not be optimized, the best information system will have little intelligence to manage, and eager scientific and cultural analysts will have little to study.

Notes

¹¹⁹ Betts.

Chapter 8

Summary and Conclusions

Real Threat

The threat of bioterrorism in the US, while often inflated by media and popular culture, is real and growing. It will be fueled by a revolution in biotechnology and the growing number of more violent terrorists who may see biological weapons as their best choice for asymmetrical attack.¹²⁰ The lack of an effective BWC verification regime only increases the likelihood of terrorists obtaining BW. Bioterrorism has the potential capacity to inflict mass destruction on US society. While the argument on whether bioterrorism is a weapon of mass destruction or a weapon of mass disruption, it is almost universally accepted that the US government must take a comprehensive approach to counter-bioterrorism.

Intelligence is Key to Counter-Bioterrorism

Almost all biodefense experts agree that intelligence is the first line of defense against bioterrorism.¹²¹ At the same time, these experts argue that the community cannot continue with business as usual and successfully manage or defeat this threat. Former Senator Sam Nunn states, “bioterrorism is different from other security threats; and to fight it, we need a different set of tools than the ones we’ve been using.”¹²² Other leading studies point to improved intelligence as the foundation for any effective counter bioterrorism strategy.¹²³ At the same time, there have been a number of calls since the end of the Cold War to retool the IC.¹²⁴

To effectively execute the counter-bioterrorism mission, the IC must work to eliminate drags on effectiveness, improve the intelligence foundation, and overcome functional challenges. A mission thread-centric approach is essential, and will serve as a catalyst to improve both the

foundation of the intelligence structure and functional processes. It will also help to expose inefficient and unneeded intelligence processes.

There Are No Silver Bullets

Good intelligence will not stop all bioterrorism, but it will make the tasks of conducting it more expensive and cumbersome.¹²⁵ This alone makes the intelligence mission critical. In the final analysis, intelligence is but one tool to fight bioterrorism. It will play a leading role in deterring and preventing attacks in the future. There will no doubt be some failures that result in successful strikes--the IC no matter how good or how well equipped cannot remove all risk to the American people.¹²⁶ The real measure of success will be the limitation of threats and, when attacks do succeed, providing responders with an information advantage in treatment and containment missions. Intelligence success will also be measured by its ability to help law enforcement and military forces lock-up or eliminate the perpetrators.

Improved intelligence will enlighten and guide US counter-bioterrorism efforts. In writing about nuclear weapons in his book *Indefensible Weapons*, Robert Jay Lifton stated that in many cases, there appears to be an extraordinary impact made upon people simply by new information... new information makes contact with amorphous fears...the menace one has known, but kept hidden comes in the open. And there is a beginning sense that one might, just possibly, be able to do something about it¹²⁷

There should be little doubt that an IC, keenly focused on the bioterrorism threat, will expose the menace and allow the full resources of the US government to do something about it.

Notes (continued)

¹²⁰ See Martin for discussion on motivations for nation states to acquire BW. For discussions on the impact of biotechnology on terrorism see Walt, Stephen. "Beyond Bin Laden Reshaping US Foreign Policy." *International Security*, Vol. 26, No. 3 Winter 2001/02: 59.

¹²¹ Deutch.

¹²² Nunn.

¹²³ Falkenrath, 277 and Lederberg 306.

¹²⁴ Betts, Richard K. "Fixing Intelligence." *Foreign Affairs*. January-February 2002, 43. Richard A. Best, Jr. "Intelligence Issues For Congress." Congressional Research Service Issue Brief for Congress: The Library of Congress. January 2002. Mary H. Cooper, "Overview: After the Aldrich Ames Spy Scandal." *Congressional Quarterly Press*. Volume 6, No. 5, 2 February 1996, 99. John Deutch and Jeffrey H. Smith, "Smarter Intelligence." *Foreign Policy*. January-February 2002. Robert David Steele. *The New Craft of Intelligence: Personal, Public, & Political* OSS International Press. 2002.

¹²⁵ Smithson, Amy. Prepared Statement Before the Senate Committee on Governmental Affairs Subcommittee on International Security, Proliferation, and Federal Services. 12 February 2002.

¹²⁶ Deutch.

¹²⁷ Lifton, Robert Jay, and Richard Falk R. *Indefensible Weapons: The Political and Psychological Case Against Nuclearism*. New York: Basic Books, 1982.

Glossary

BW Biological Weapons

BWC Biological Weapons Convention

CIA Central Intelligence Agency

COTS Commercial-Off-The-Shelf

DOD Department of Defense

HUMINT Human Intelligence

IC Intelligence Community

IMINT Imagery Intelligence

MASINT Measurement and Signatures Intelligence

NBC NUCLEAR BIOLOGICAL CHEMICAL

OSINT Open Source Intelligence

RIONET SEE PAGE 54

SIGINT Signals Intelligence

WMD Weapons of Mass Destruction

Bibliography

Best, Richard A, Jr. "Intelligence Issues For Congress." Congressional Research Service Issue Brief for Congress: The Library of Congress. January 2002.

Betts, Richard K. "Fixing Intelligence." *Foreign Affairs*. January-February 2002.

"Biowar Fears Cloud US War Success," MSNBC Website
(<http://msnbc.com/news/627086.asp>) (Accessed 23 March 2002).

Carter, Ashton, B. The Architecture of Government in the Face of Terrorism,
International Security, Vol. 26, No. 3 (Winter2001/02)

Carus, W. Seth. *The Illicit Use of Biological Agents Since 1900*. Center of
Counterproliferation Research, National Defense University. Washington, D.C. February 2001.

"*Combating Terrorism: Observations on Biological Terrorism and Public Health
Initiatives*," (Testimony, 16 March 1999, GAO/T-NSIAD-99-112),

Cooper, Mary H. "Overview: After the Aldrich Ames Spy Scandal." *Congressional
Quarterly Press*. Volume 6, No. 5, 2 February 1996, 99.

"*Countering the Changing Threat of International Terrorism*," Report of National
Commission on Terrorism. Pursuant to Public Law 277, 105th Congress, June 2000.

Deutch, John and Jeffrey H. Smith, "Smarter Intelligence." *Foreign Policy*. January-February 2002.

Dickinson, Lansing E., (Lt Col). Military Role in Countering Terrorist use of Weapons of Mass Destruction, Air War College, April 1999, 27

"*DoD Responses to Transnational Threats*, Vol. 1. Defense Science Board 1997 Summer Study Task Force. Office of the Undersecretary of Defense for Acquisition and Technology. December 1997.

Falkenrath, Richard A. Robert D. Newman, and Bradley A. Thayer. *America's Achilles' Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack*. The MIT Press. Cambridge, Massachusetts. 1998.

Ferguson, James R., "Biological Weapons and US Law," *Journal of the American Medical Association (JAMA)*, Vol. 278, No. 5 (August 6, 1997), 357-360.

Garrett, Laurie. "The Nightmare of Bioterrorism." *Foreign Affairs*. January-February 2001.

Gordon, Michael R., "US Says It Found Qaida Lab Being Built to Produce Anthrax." *The New York Times*. 23 March 2002, A1.

“Guests’ Bags Inspected Before Entering Parks,” News Channel 2000.COM Web Site,
(<http://www.newschannel2000.com/orl/news/stories/news-100873020011009-091033.html>) (Accessed October 9, 2001).

Inblesby, Thomas V., Tara O’Toole, and Donald A. Henderson, “Preventing the Use of Biological Weapons: Improving Response Should Prevention Fail,”
(<http://www.l.journals.uchicago.edu/CID/journal/issues/v30n6/00065.text.html>)

Joint Publication 1-02, DoD Dictionary of Military and Associated Terms.

Lederberg, Joshua. Editor. *Biological Weapons: Limiting the Threat*. The MIT Press. Cambridge, Massachusetts. 1999.

Mark, Dr. Hans. Comments as Keynote Speaker at Biological Threat Reduction Conference 2002, University of New Mexico, March 14-15 2002.

Martin, Dr. Susan B. “The Role of Biological Weapons in International Politics: The Real Military Revolution.” Forthcoming article in the *Journal of Strategic Studies*, Spring 2002.

Mayer, Terry N. “Biological Weapons—The Poor Man’s Nuke.” Research Report, Maxwell AFB, Ala.: Air War College, April 1995.

Mercyhurst College academic website. (<http://www.mercyhurst.edu/Academics/riap.htm>)

MSNBC News Service, "Biowar Fears Cloud US War Success." 23 March 2002.

(<http://msnbc.com/news/627086.asp>)

Lifton, Robert Jay, and Richard Falk R. *Indefensible Weapons: The Political and Psychological Case Against Nuclearism*. New York: Basic Books, 1982

Proliferation: Threat and Response, Office of the Secretary of Defense, January 2001.

Smithson, Amy. *Toxic Archipelago: Preventing Proliferation from the Former Soviet Chemical and Biological Weapons Complexes*. Stimson Center Report 32. Washington, D.C.: Henry L. Stimson Center, 1999.

Smithson, Amy. Prepared Statement Before the Senate Committee on Governmental Affairs Subcommittee on International Security, Proliferation, and Federal Services. 12 February 2002.

Steele, Robert David. *The New Craft of Intelligence: Personal, Public, & Political*. OSS International Press. 2002.

Stockholm International Peace Research Institute Home Page (SIPRI)
(<http://projects.sipri.se/cbw/docs/bw-btwc-sig.html>) Accessed 21 April 2002

University of New Mexico Intelligence Studies Program Draft Pamphlet. March 2002.

US government official interview with the author and subsequent correspondence, Miami Florida, 15 December 2001.

US government official interview with the author, Miami Florida, 22 March 2002.

US Senate Committee on Foreign Relations, Hearing on The Threat of Bioterrorism and the Natural Spread of Infectious Diseases, 5 September 2001, Testimony for Former US Senator Sam Nunn.

Walt, Stephen, "Beyond Bin Laden Reshaping US Foreign Policy." *International Security*, Vol. 26, No. 3 Winter 2001/02.

Williams, Peter, and David Wallace, *Unit 731: Japan's Secret Biological Warfare in World War II* (New York: The Free Press 1989) p 64, 69.