AIR WAR COLLEGE

AIR UNIVERSITY

2035 BIODETERRENCE:

PROBLEMS AND PROMISES FOR BIODEFENSE

by

Patrick C. Burke, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

17 February 2010

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the USG 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.

CONTENTS

BIOGRAPHY

Lieutenant Colonel Burke is currently a student at the Air War College, Maxwell Air Force Base, Alabama. Prior to the College, he served as the Commander of the 322d Basic Military Training Squadron, Lackland Air Force Base, Texas. He is an acquisition and space professional and has served as a Test and Aircraft Integration Program Manager with the Advanced Medium Range Air-to-Air Missile Joint Systems Program Office, Squadron Maintenance Officer on C-130s as part of the command's Broadening Experience Special Tour program, Program Manager for an ACAT 1C classified space program, Air Force Special Programs air staff officer, and Deputy Division Chief of Systems Engineering for the Future Imagery Architecture, National Reconnaissance Office. Lt Col Burke holds a bachelor's in engineering from the United States Air Force Academy, master's in business administration from the University of West Florida, master's in military operational art and science from the Air Command and Staff College and is a graduate of the Defense Systems Management College's Advanced Program Manager Course. He is married with three children.

I. Introduction

Can the U.S. deter nation, group, or individual actors from employing bioweapons in 2035? The intent of this paper is to inform the debate and influence the way the United States thinks about bio-defense. At the very least the paper aims to better understand the problem by looking at deterrence against nations, groups, and even individual actors from employing bioweapons. The paper illuminates the stakes involved in future bioattack, and characterizes where the world of accelerating technology, communication, and information will likely lead the U.S., relative to further exploration for the efficacies of deterrence. The paper specifically explores potential deterrence strategies by examining the roots, driving forces, and potential actors. Finally, it examines potential enforcement methods to further support deterrence. This paper begins by assessing shifts in recent history that have led to a relook at deterrence strategies.

The combination of ever-growing WMD potential and the renewed attention to the nuclear realm has spawned a revitalization of the concepts of deterrence. Historically, deterrence has been coupled almost exclusively with the nuclear realm. The revitalization has also been tied to America's war weariness and a call for new strategies to engage with the world short of major armed conflict and regime change as experienced in Afghanistan and Iraq.[1] These latter strategies have proven to be overly costly in lives and treasure with 5,308 fallen as of 16 January 2010[2] and exceeding a trillion dollars with FY2010 appropriations.[3] Raised tensions and discontent with foreign occupation have placed the U.S. at a greater risk of being the target of a bioattack. Given the current strain on the US national treasury from both domestic economic issues and heavy war bills, the strategy of deterrence has great promise and warrants closer examination. Certainly with the ever-growing WMD potential for devastating impacts, a layered, broad spectrum deterrence strategy holds great promise.

In recent years, writing and research on the threat of bioweapons has exploded. The realization of the vulnerability of the United States to asymmetric threats such as the horrific 9/11 attack which left over 3,200 dead, or the 2001 anthrax attacks on U.S. government and business officials which left five dead, could in themselves be an explanation for this explosion in interest.[4] Both of these attacks caused widespread panic and a loss of confidence in U.S. national security and supporting intelligence apparatus. Furthermore, these attacks revealed that the U.S. is ill-equipped and thus vulnerable to this class of threat. These attacks, and specifically the anthrax attacks, show that it is not a question of "if" for bioterrorism, but when and what next?

The world has changed immensely since the end of the Cold War. This shift has released old tensions and created new ones as the world adjusts to the new forces of globalization and a sole remaining superpower. Since the end of the Cold War the U.S. has shifted its national security focus from the monolithic Soviet Union, to the tougher and more diverse problem set of climate change, pandemics, proliferation of WMD, failed and failing states, rising powers with sophisticated weapons, rogue states, and most notably a host of non-state actors to include Islamic extremists like Al Qaeda who are avowed to harm Americans wherever possible.[5]

In accelerating this picture to 2035, these same types of challenges and protagonists will likely be present; however they will exist in a world typified by a rate of technological change few people dare to imagine. In Joel Garreau's nonfiction book, *Radical Evolution*, he describes the four technologies of genetics, robotics, information and nanotechnology or GRIN, whose catalytic effect on one another, propelled by information, will accelerate change like never before, causing the curve of change to grow ever steeper.[6]

By analyzing the potential impacts of a 2035 bioattack, this paper examines what is at stake, the investments feeding this potential threat, and also current threats as a departure point in looking more knowingly toward the future. It further looks at the nature of bioweapons and potential characteristics of the 2035 biothreat. Finally, it briefly looks at the deterrence strategies of transparency alongside diversity of action as a potential means to a more cost-effective and viable biodefense strategy.

II. What's at Stake?

As Malcolm Gladwell describes in his book, *The Tipping Point,* unexpected things can happen from otherwise expected events when the tipping point is reached.[7] The term "tipping point" was coined by epidemiologists to describe conditions where "small changes will have little or no effect on a system until a critical mass is reached. Then a further small change 'tips' the system and a large effect is observed."[8] Likewise, bioattacks have great potential to destabilize the country if critical pieces of the nation's infrastructure are affected--reaching "the tipping point." Findings from the 2008 National Infrastructure Advisory Council's final report shed some light into this potential reality as discussed in the next section.

Critical Infrastructure

A biological event whether natural or manmade will certainly test the critical infrastructure of the United States and the world. In accordance with the National Infrastructure Advisory Council;[9] "To avoid an economic and social catastrophe, biological preparedness demands full participation from the public and private sectors."[10] Key findings of the survey highlight the critical interdependencies across service sectors and the vital dependencies U.S. society has on key products, services, and workers that produce them and the transportation system that moves them.[11] Detailed findings from this report can be found in Appendix 1 of this paper.

The number of casualties from a bioattack necessary to undermine critical infrastructure could be far lower than thought given the U.S. population's reliance on key services. If the biological agent (natural or man spawn) were highly virulent and contagious, causing second and subsequent waves of devastation until an adequate vaccination could be developed and distributed, millions to tens of millions could perish.[12] Aside from totally overwhelming the U.S. health care system, there would be catastrophic shock waves caused by subsequent effects. The effects would certainly cause the government to close off the financial markets before they bottomed out. Even with these measures, it is easily imagined that the United States would face the potential for economic collapse, rivaling anything experienced by this nation. Martial law would likely be declared to prevent utter chaos and anarchy. Government actions to prevent future attacks would cause a monumental loss of civil liberties, dwarfing security measures like the Patriot Act[13] in their wake. Even after eventual recovery, the nature of American democracy would be changed forever. Biothreats present an imperative to the United States to pursue all avenues for a stronger biodefense. The U.S. cannot solve this problem alone and must seek cooperation around the world for global health and security.

World Leadership

Powerful movements are at work in the world of bioresearch. The U.S. is but one of many actors at work. Since 2001, the U.S. alone has spent an average of $6.33 billion per year on biodefense.[14] The 2009 budget saw an increase to a total of $8.973 billion, which notably consisted of a $2.175 billion contribution to Project BioShield.[15] Although the United States leads the world in biodefense investments, many of these efforts are still perceived by senior officials to be greatly underfunded to include the areas of infectious disease surveillance, medical countermeasures, defense of food and agriculture, and public health preparedness.[16] These

issues continue to cause concern among U.S. researchers. Part of the solution will come from both national and international cooperative efforts for global health and biodefense. With a dominant portion of investment in this area, the U.S. is clearly poised to take a leadership stance in garnering wider cooperation for responsible research and related accountability as a nation. Further, the U.S. must seek wider cooperation and leverage to ensure other nation states continue to address the conditions within their state to prevent rogue groups or individuals from pursuing biological means to their ends. The goal of collaboration is to make the world a smaller and smaller place for bad actors to try and operate in.

Current Threats

Looking to the future and understanding what is at stake requires a frame of reference based on a picture of the present threat. Dr. Venkayya, the former Special Assistant to the President and Senior Director for Biodefense at the White House Homeland Security Council, highlighted in a December 2009 interview that "There are already plenty of threats today that are very concerning and could have very devastating effects."[17] Currently, numerous naturally occurring biological threats exist to include anthrax, cholera, plague, foot-and-mouth disease (livestock) and smallpox. The Joint Chief of Staff declared in 1996 that anthrax is the number one threat to the U.S. military.[18] Current threats are: "Pathogenic to humans, transmissible by aerosol, and effective at low doses; they cause severe disease; they have high rates of disease following infection; and they are easily and rapidly produced and are concentrated and environmentally stable."[19] Not only do these pathogens exist, but numerous types of biological agents are weaponizable or have been weaponized in the past. These include the weaponization of toxins, chemical agents, bacterial agents, and viral agents.[20]

The Former Soviet Union's (FSU) extensive bioweapons program included employment of sophisticated cruise missile technology[21] for delivery and also "space capsule-like" payload protection in bioweapon rockets to increase delivery survivability.[22] It is doubtful that these programs or crucial remnants of them will not continue within Russia despite current treaty obligations or political declarations.[23] Also of concern are that many Russian scientists, out of work and underutilized after the collapse of the Soviet Union, need to find employment. In their search for jobs, these scientists could be creating new bio-capacity in marginal states.[24,25] These scientists are vulnerable to "well funded" supporters like Iran (aggressive recruitment offering $6,000/month pay) or other nation states or non-state actors alike who wish to start or augment their own bioweapons programs.[26] The current threat is real. Any nation state has a lot to lose in the world's eye if they employ bioweapons. The focus for nation states is therefore on accountability of their people and their "wares" in preventing any use of bioweapons. The next section of this paper will explore the characteristics or nature of bioagents that make them such a viable and dangerous threat.

III. The Nature of Bio

This section describes the nature of biological threats and how dual-use research, their formidable attributes, and their WMD potential make them a threat the United States must address. As a weapon of mass destruction, these agents have a destabilizing potential that requires both national and international steps to deter would be aggressors.

"Dual-Use" Research

Global health and wellness necessitates biological research. Further, the bioresearch industry covers a broad spectrum of commerce with applications ranging from agriculture, health, material science to even bio-computing. However, this natural path for industry can have equal

potential for "bad" purposes. Dr. Venkayya clearly stated, "You can't lock up technology. All of the biological technology is dual-use and virtually indistinguishable from offensive purposes, save who is doing it."[27] The same facility and equipment can be used for both good and bad purposes. Further, given these facts, export controls are not effective. All of the equipment for biological research is dual-use and widely available via primary or secondary markets. The availability of equipment creates a formidable problem for biodefense and its objective to prevent an attack or at least greatly mitigate the effects of an attack.

How are Bioweapons Different from other Weapons?

The "dual-use" research aspect of biological agents certainly sets them apart from other potential weapons. Nuclear technology has shared a somewhat similar kinship to bioresearch in its ties to peaceful production of energy, given the physics of "weapons grade" activities vs. "non-weapons grade" is understood. However, unlike nuclear or kinetic weapons, biological weapons pose a much more difficult problem in discovery and attribution. As mentioned, numerous naturally occurring pathogens can easily cause a pandemic if harnessed and used for a harmful effect. An engineered or genetically modified influenza for example, could present itself very similarly, but be much more lethal than the natural variety. This similarity would have a masking effect for a time until laboratory research could be conducted. The time delay would make attribution a much more difficult problem.

Toxins, as another example, can take a couple of days to manifest symptoms, making attribution more difficult. The United States recognizes this uniqueness and has invested in a brand new biological forensics center as part of the Homeland Security Biodefense Complex.[28] This facility is called the National Bioforensic Analysis Center (NBFAC), which is part of the Department of Homeland Security's National Biodefense Analysis and Countermeasures Center

(NBACC). The center was designated in Presidential Directive "Biodefense for the 21st Century," as the lead federal facility "to conduct and facilitate the technical forensic analysis and interpretation of materials recovered following a biological attack in support of the appropriate lead federal agency."[29] The other part of the NBACC is the Biological Threat Characterization Center (BTCC) which "will conduct studies and laboratory experiments to fill in information gaps to better understand current and future biological threats, assess vulnerabilities, conduct risk assessments, and determine potential impacts...."[30] The investment in these facilities which targets attribution, clearly distinguishes bioweapons from other types of weapons. The next section will further distinguish bioweapons from other weapons.

Attributes of Bioweapons

As discussed previously, even current biothreats have the potential to unleash havoc as never before witnessed. The future of bioterror is even more deadly. An even wider repertoire of bioweapons will likely exist in 2035; however, they will differ in some important ways. Agents will be "smarter", they will be "tailored", and they will be far deadlier than anything known to date. A preview of these weapons was delivered by former Chief Scientist and First Deputy Director of the Former Soviet Union's clandestine Biopreparat operations (only half of the known Soviet bioweapons program) who defected to the U.S. and revealed much of the breadth of the Soviet's higher than Top Secret "Special Interest" programs.[31] Most notably the program had improved "battle strains" of anthrax, a super-plague, and a Russian strain of tularemia. Dr. Alibekov, who now goes by Ken Alibek, states that these three agents "could overcome all immune systems and current medical treatments" and has further revealed that genetic engineering was being employed, leading to new life forms with the goal of targeting for more desired lethal effects.[32] Supporting these findings, though not conclusive, were reports from

former Soviet-era testing facilities in Kazakhstan that were opened to U.S. teams supporting dismantlement efforts.[33] Kazakhstan was relatively transparent in their efforts to reveal and address this unprincipled period in their history.[34]

Dr. Alibek also stated that the goal of their "chimera" viruses was to insert genes from one virus to another to create an even more lethal virus. Alibek revealed that further work on other viruses was being targeted to modify the smallpox virus, which has otherwise been eradicated from the world's population.[35] Even in the unmodified variety, a release of smallpox would have devastating effects worldwide. To illustrate the reality of genetically modified organisms one need only look to macro bio-agriculture companies like Monsanto, who has used genetic modification widely in agriculture to develop new crops like "Round-Up Ready" soybeans, which survive heavy use of the "Round-Up" herbicide to increase farm yields.[36] The latter example highlights the fact that genetic modification is already a part of everyone's lives. Further, genetically modified material can be patented, which supports and protects continued strong investment in this realm.

Genetically engineered pathogens will be a much more difficult challenge than, for example, the relatively stable non-contagious anthrax variety used in the 2001 U.S. anthrax attacks. Genetically engineered pathogens will have tailored characteristics making them more effective as a potential weapon of mass destruction. By the year 2035, with the amount of money pouring into bio-research of all kinds coupled with the synergy of knowledge availability, bioagents of all types will have the potential to have increased transmissivity, be more contagious, and have increased survivability.[37] The latter characteristic will make it easier to store, transport, and deliver a bioagent. Further advances will make bioagents resistant or immune to known vaccines and antibodies, harder to detect and diagnose, and more lethal.[38]

The targetable characteristic will be driven by investments in medical research such as research for cancer treatment/cures. Researchers have successfully used gold nanoparticles to deliver DNA molecules into cancer cells to defeat the cancer.[39] With that said, there is a brewing synergistic storm between the three fields of genetics, nanotechnology, and robotics (the GNR storm) which includes the powerful information enabler/multiplier that will propel bioscience in unexpected ways and at an unprecedented pace.[40]

The emerging field of synthetic biology has already created bacteria that seek and invade tumor cells and yeasts that produce the antimalarial drug precursor artemisinic acid.[41] Dr. Jay Keasling, a professor of biochemical engineering at the University of California at Berkeley, is involved with putting together "a kind of foundry of biological components--BioBricks."[42,43] Keasling and others in the field "see cells as hardware, and genetic code as the software required to make them run."[44] Further, Specter reports that with enough knowledge and computer control support, these BioBricks will not only be able to alter nature, but guide human evolution.[45] Part of the referenced knowledge base comes from projects like the Human Genome Project (HGP) which was completed in 2003 after 13 years of work.[46] The project was coordinated by the U.S. Department of Energy and the National Institutes of Health (NIH). These are just a few examples of ongoing projects that begin to break down the "costs of entry" into the bio realm. The growing ubiquity of information will only add to lowering these "costs of entry."

In further discussions with scientists at Los Alamos National Laboratories, there is a growing fear that too much information is out there and available to literally anybody with a credit card.[47] It would be far more responsible to address the ethical, legal, and social issues prior to making this type information available indiscriminately. This discussion is a common theme in

providing some sort of responsible control mechanisms to this arena. Other mechanisms to foster restraint are discussed in the next section.

IV. Deterrence by Dissuasion and Denial

As the stakes of defending the U.S. against Weapons of Mass Destruction (WMD) and Knowledge-enabled Weapons of Mass Destruction or (KMD)[48] are so high, relying on a single approach for biodefense could have catastrophic results. Specific to bioweapons, the availability of bioresearch knowledge via the internet is fueled by ever-growing budgets in bioresearch and indiscriminate postings of "dual-use" data and techniques. These realities have greatly lowered the "cost of entry" and greatly raised the capabilities of even the "lone wolf" individuals operating out of their basement. Readily available knowledge propels the potential lethality, giving individuals and groups "state-level" potential for destruction. This access to information has opened up a new vulnerability that is only limited by ones imagination for devastation. This unyielding fact demands a layered and diverse approach to biodefense.

In looking at the problem of "covering the waterfront," the United States must target the attributes of the future biothreat. These attributes must be targeted using varying levels of force across the spectrum of deterrence. Using Shaud's deterrence model, deterrence spans from dissuasion to denial to the threat of punishment, where the level of force increases from no force "soft techniques" to hard kinetic forces in the move to punishment.[49] The purpose of this section is not to be encyclopedic, but rather to provide a taste of potential actions or tools that help make up a layered and vigorous response for policy makers, military strategists, technologists and scientists alike.

Definitions

In discussing deterrence a few important definitions are provided to establish a common framework of understanding. As brute force has fallen out of favor, the United States must use **coercive** strategies "to convince an adversary to change its behavior by manipulating the costs and benefits of NOT doing as demanded."[50] Two types of coercion are defined below:[51]

> 1) **Deterrence** - the coercer believes that the adversary INTENDS to act in an unacceptable manner and demands that the adversary REFRAIN from acting.
>
> 2) **Compellance** - the coercer demands that the adversary change his behavior, do something new

In accordance with former CINCSAC, General Russ Dougherty, "**Deterrence** = Capability x Will." General Dougherty further defines deterrence as "preventing an action by promoting fear in the other's mind" and holds that this can be done by "dissuasion (psychological effects), denial (defend by presenting an adversary with barriers), and finally by using a credible threat where an adversary must think and believe you will use your capability against them."[52] The latter term of "credible threat" will be extended in this research to mean threat of credible punishment. *Joint Publication 1* discusses in its "Range of Military Options" section that **deterrence** "helps prevent adversary action through the presentation of a credible threat of counteraction. Deterrence is just one of "ongoing activities to establish, shape, maintain, and refine relations with other nations and domestic civil authorities..."[53] This paper now addresses the coercive strategies of dissuasion, denial, and punishment as part of the spectrum of deterrence.

In thinking about deterrence it is important to note that "the old nuclear paradigm is not effective against emerging weapons of mass destruction, new conventional threats, and non-state actors."[54] There are new relationships that did not exist or were not relevant during the Cold

War era, for example, State vs. Group, State vs. individual, group vs. group, and group vs. individual. The most notable concern is the rising relative power of groups and even individuals who will have access to or can themselves develop "nation state" capabilities, largely through "knowledge-enabled" means. Developing a deterrence strategy will be useful, but it must be part of a system of layered strategies to include a grand strategy of addressing the root causes of violence using all of the United States' national instruments of power.[55] The next section will discuss the "system of violence" to help address these root causes.

The "System of Violence"

In order to devise an effective deterrence strategy it is important to understand the "root cause(s) that underlie the bad behavior one wants to deter. One such construct that was outlined in a 2009 NATO Joint Capabilities Development and Experimentation Conference exploring deterrence operation used a model for the "System of Violence."[56] This model creates a construct of "Roots, Transformations, and Actors" in creating a framework to understand the environment which produces violence.[57] In developing a long-term solution to bring peace to the "System of Violence," the root(s) or underlying cause(s) for the violent behavior must be addressed. These roots can span from ideological incompatibilities to economic upheaval.[58] It will also be important to understand the external forces that influence and contribute to these underlying causes along with the actors involved. The "Transformations" or other forces that propel or foster the "roots" of violence can come from failed governance, backlash to globalization, or external influences that reinforce unlawful actions.[59]

During the Cold War, the United States focus was almost wholly consumed by the Soviet Union , however the breadth of actors potentially threatening the U.S. and its national interest

have grown to include non-state actors, such as religious extremist groups and individuals. The rogue individual or fanatical group will always hold an inordinate amount of power for their size, as it is always easier to destroy than to build. These type actors can use technology like "jujitsu" to transgress against power as science fiction writer William Gibson was referring to when he said "the street has its own uses for things -- uses the manufacturers never imagined."[60]

Transparency

In 2035, many of the same strategies that exist today to deter biological attacks will be available. Presently, the United States relies on vaccines to ward against particular threats such as smallpox and anthrax for deployed troops. Stockpiling such vaccines is another strategy employed to deter those who seek to target the US with these type biological attacks. In terms of preemptive strategies, transparency has much potential to deter future biothreats. The United States has underutilized the advantages to be gained by being militarily transparent. So what is transparency and how do we use it? The *Compact Oxford English Dictionary* defines "transparent" as "allowing light to pass through so that objects behind can be distinctly seen" and as "obvious or evident."[61] Military transparency, simply defined, refers to the act of a country to make its strategic intention and military strength known to others thereby reducing suspicion and increasing mutual trust.[62] Most recently, in U.S. news, China has been criticized for a lack of transparency, and has been called to increase its military transparency.[63] Transparency has obvious implications for nations, but how can it deter groups or individuals? The next section presents a potential answer to this problem.

Transparency and Architecture

In Richard Oliver's book, *The Biotech Age,* he contends that current medicine attempts to find a "weapon" to use against various illnesses and diseases, however in the future, diseases will be

prevented by genetically "architecting" against it.[64] In thinking about preventing bio-threats, it may be possible to "architect" against them as well. If a particular nation "armed" itself by genetically altering the DNA of its citizenry, in other words, altering the "architecture" of the biological makeup of its citizenry, some threats would become obsolete. Once a nation made it known that it had "armored" itself in such a way, it would be readily apparent to any potential enemy that it would need to or have to take a different approach. Transparency is a strategy that is currently employed to deter biological threats that will become even more important in the future and potentially more uncertain times. The Bulletin of Atomic Scientists recently published a call for increased transparency in biodefense efforts. The bulletin pointedly states:

> By being more transparent about biodefense research, states would increase international confidence that they are working to prevent the next biological attack and not contributing to it. Because the United States has the world's largest biodefense program, it must lead by example.[65]

When comparing the cost of biodefense strategies and deterrence, transparency is incredibly cost efficient. While we are currently investing billions of dollars on developing vaccines, drugs, and air samplers; transparency can be accomplished simply and affordably by the click of a button, sending an email to a few strategic parties. The combination of strategic preparedness such as having lab resources that can create vaccines in days, thereby eliminating the dramatic impact of bioattacks and strategic communication, broadcasting that the U.S. is prepared for an attack renders the attack useless.

Ethical (Legal) Treaties

The United States supports the efforts of the Biological and Toxins Weapons Convention,[66] but does not submit to verification by other countries. The concern is that being overtly transparent may reveal vulnerabilities, gaps or shortcomings that could in turn weaken U.S.

biological defense. This lack of transparency creates a double standard when the United States is seeking similar assurances through verification. The lack of a supported, confidence-building verification scheme creates uncertainty and risks of miscalculation.

In 2009 discussions during a global summit on climate change, President Obama clearly indicated that any accord must include a mechanism to review whether nations are keeping their commitments. Without it, any agreement would be "empty words on a page." The implications for verification of prohibition of the development of bioweapons should be similar, if not more immediate and dire. There is no formal verification regime to monitor compliance although "confidence building measures" are described in the convention.[67] Aside from signed treaties or conventions, which for the most part become ratified by participating states, "universal" professional ethics tools have great potential. Note: The Main Articles of the Biological and Toxin Weapons Convention can be found in Appendix 2 of this paper.

Ethical Code for Scientists

An ethical code for scientists has been discussed for many years and shows promise in support of ethical research of all types. The ethical code for scientists would be similar to the Hippocratic Oath of "do no harm," which dates back thousands of years to early Greek medicine. A push for adoption of a similar code for scientists appears to be gaining a foothold. Most recently, Sir David King, Britain's Chief Scientist announced a seven part ethical code for scientists that he hopes will be taught in schools.[68] His code calls for responsibility, rigor and respect and is suitable in his opinion for worldwide adoption.[69] One recent example that this concept is gaining momentum comes from a 2008 graduating class of Biomedical Scientists from the University of Toronto, Canada who declared an oath of ethical conduct, professing "pride, integrity, and pursuit for the "greater good."[70]

Informal Conferences

A powerful form of transparency and deterrence comes from participation in informal conferences, whether regional or international. Just bringing people to together to discuss this important topic shows a level of willingness to cooperate on the world stage. These conferences and supporting think tanks can be instrumental in advocating policy updates or implementation of new policies. Participation shows a willingness to partner and learn from other countries and assist in establishing normative behaviors of ethical and moral conduct. A few such groups include the Australia Group and the World Health Organization.

Scientific Standards

Another potential tool is the implementation of formal scientific standards for the conduct of research and testing, and also a definitized lexicon for discussing technologies, practices, and issues. This has the benefit of increasing the integrity of communication with one another and supports concise language in any conventions or treaties. Scientific standards could potentially support deterrence as an identifier "red flag" for people trying to operate in this realm who are not professionally tied to this community. If someone is trying to "cut corners" or appears to "not fit" into the community, those activities could be warning signals for reporting. There are other tools that can be implemented that support identifying or flagging personnel, such as establishing personnel controls.

Personnel Controls

Personnel controls are an area to be further reviewed and can work in concert with the "flagging" tool for identifying potential rogue behavior or the potential for rogue behavior. Once a person displays through action, behavior, or comment that they are potentially dangerous, they become "flagged" for further action to include making them an intelligence target. If a worker

who had access and knowledge of "sensitive" bioresearch data became disgruntled, they would be "flagged" as a piece of intelligence. From articles V and VI of the BTWC (See Appendix 2), there is language that supports these actions; the key is identifying and tracking bad actors.

Moral

Similar to and supporting the informal conference discussion, is the important tool of using the world's religious and spiritual leaders for strategic communication of the evils of using these specific type of weapons as they lend themselves to indiscriminate killing at potentially unseen levels. As many groups, such as Al Qaeda, are tied to religious extremism, requesting religious leader support could be a fairly high pay off area if, for example, the Muslim Imams around the world formally condemned such activity. These declarations could be coupled with responsible media and even cause some media venues like Al Jezeera to be more balanced and responsible in their reporting and world views. In any case, this resource could prove to be a powerful lever against one of the toughest set of actors to deter---extremist groups and individuals.

National Strategy

Declaring a U.S. national strategy for biodefense was a critical piece of dissuasion along the spectrum of deterrence. Prior to President Obama's release of the National Strategy for Countering Biological Weapons in November of 2009, national strategies more broadly addressed weapons of mass destruction with reference to chemical and biological types. The new 2009 strategy is specific to biological weapons, emphasizing the importance of this specific threat class. It is critical to have a plan to help guide investments and focus the nation on this growing threat. President Obama's strategy includes a number of specific objectives that support deterrence through denial and deterrence with transparency. Excerpt follows:[71]

Objective One: Promote global health security

Objective Two: Reinforce norms of safe and responsible conduct
Objective Three: Obtain timely and accurate insight on current and emerging risks
Objective Four: Take reasonable steps to reduce the potential for exploitation
Objective Five: Expand our capability to prevent, attribute, and apprehend
Objective Six: Communicate effectively with all stakeholders
Objective Seven: Transform the international dialogue on biological threats

Objective Seven can help enable all of the preceding objectives and is a critical piece of engaging with partners around the world. Partnering with allies furthers deterrence through robust cooperative efforts in support of U.S. National Strategy for Countering Biological Weapons. These partnering opportunities can come in many forms: e.g. supporting international forums for responsible conduct, sharing intelligence, sharing technology, and partnering in procurement. Two partnership examples can be found in Appendix 3.

When the concerted efforts of dissuasion and denial do not tilt the balance, the final weight for an adversary to consider along the deterrence spectrum is the credible backlash of swift and unrelenting punishment of those who would cross the threshold of unlawful behavior. The next section will discuss the sovereign enforcement tool.

V. Sovereign Enforcement--Deterrence by Punishment

In development of effective coercive strategies for sovereign enforcement or punishment, attribution is key. As former Biodefense director Dr. Venkayya stated, ""Deterrence and attribution should be used in the same breath."[72] It will be critical to let the world know that the U.S. has demonstrated capability to find would be perpetrator(s) and quickly. This next section will look at the difficulties and necessity of attribution along with the tool to interdict or eliminate threats.

Who is doing What?

Part of any successful coercive strategy will involve the reality that there will be serious consequences to any nation, group, or individual actor participating in rogue behavior. Critical to a punishment response will be the credible analysis to determine who is doing what. Without this data, the United States' reputation as a "just cause" actor will be tarnished, potentially feeding the conditions that cause an adversary into rogue behavior. Intelligence can come from many sources and will undoubtedly require a cooperative international arena to quickly track down and attribute rogue activities to the rightful party(s). Perpetrators may not always take credit for their maleficent behavior, making attribution more difficult. One technique to uncover illicit activities is called "flagging" where indicators are collected that relate to activities in the bio arena. When the actors, timing, or activities do not fit legitimate profiles then a "flag" is set for more scrutiny. These type operations take time, cooperation, and close networking and interoperability to be effective.

This paper has already discussed the bold step forward with the investment in the National Bioforensics Analysis Center, but there is still much work to be done to increase cooperation between the Center for Disease Control, DoD, and Department of Homeland Security in developing and harmonizing confirmatory processes.[73] There is much promise in this area with the explosion of information sources such as surveillance systems, biometrics, recognition algorithms, and sales data. By 2035, the only real "safe haven" for an individual actor may very well be their garage or basement. As futures analysts John Smart describes, the world will become increasingly visually and digitally transparent. The visual transparency will come from cameras, camera "traps" e.g. traffic cameras, and even in the clothes one wears.[74] Digital transparency will come from eternally saved e-mail, life blogs and life logs, and what he

describes as glogs, which includes a full spectrum of data from a person's life.[75] This may sound "Orwellian," but will be the result of ever increasing sensors, their netting, and the inevitable trade of privacy and personal freedom for security.

Interdict or Eliminate Threats

As mentioned, the investigative tool of flagging will only be enhanced by the accelerating increase in public transparency. Once identified, an individual or group can be interdicted and either persuaded to desist or eliminated if not further deterred. There has been some suspected precedence here by the Soviets during the Cold War when faced with the destabilizing entry of technologies associated with the Strategic Defense Initiative or "Star Wars" anti-ballistic missile technologies. Here it has been alleged that the Soviet Union secretively killed leading scientists and contributors in other nations to stymie progress on these programs.[76] Alternately, a state seeking to coerce another through punishment may use force against a variety of targets not directly connected with a traditional battlefield. Infrastructure attacks were used in former Yugoslavia to create a wedge between the people and the rogue government. Punishing force may also be used against targets connected with the adversary's ability to achieve its goals (e.g. Israel's strike against the Osirak nuclear plant in Iraq in 1982).[77] Clearly the stakes are high where bioweapons are concerned, requiring bold measures. The next section will explore a few "bold measures" in the form of new potential control regimes.

New Control Regimes

With the potentially extreme impacts of biotechnology a new set of control regimes should be looked at. As discussed, the dual-use nature of biotechnology creates a burden of responsibility for any peace-loving nation state. This burden could be addressed with concerted talks through both formal and informal summits and/or conferences to establish a common framework of

terminology and program review protocols for any work labeled as "dual-use." Along the same lines, any personnel associated with these programs would face a heightened level of scrutiny for their personal reliability akin to the U.S.'s DoD and DoE nuclear Personnel Reliability Programs or PRP. Further, any critical equipment could be controlled to prevent it from falling into malicious hands after a secondary market purchase i.e. the resale of bio-equipment after laboratory upgrades. Finally, the addition of local, state and national level legislation coupled with the addition of localized law enforcement tools (frontline forensic labs or law enforcement protection measures akin to military capabilities) would enhance responsible control of these technologies. These are just a few examples, for further research would be to explore the potential for more extreme measures to further deter illicit bio-activities.

VI. Recommendations

National defense is about risk management; therefore, the first recommendation is to fully understand what is truly at stake with a biological attack on the United States. The "impacts of occurrence" as surveyed in the National Infrastructure Report are still not fully understood and need to be further researched, documented and mitigated. The extreme "impact of occurrence" should draw commensurate financial support. William Forstchen's fictional book *One Second After* builds a similar case, vividly illustrating the devastating impacts to the U.S. from an asymmetric electromagnetic pulse (EMP) attack.[78] Further, recognition of the unique nature of bioweapons as a "knowledge-enabled weapon of mass destruction" should add to the call for expanded research in the evolving nature of this threat. The additional funding plan should address the unique attributes or characteristics of future potential bioweapons.

Second, continue a broad spectrum of deterrence options that recognize and tend to the root causes of violence. Most notably, these measures must address religious extremism and the

problems of occupying forces in culturally sensitive regions through moral suasion from religious leaders and the media. It must also continue and expand upon ethical fronts such as robust support to international treaties and conferences. The latter forum should advocate for scientific standards, ethical codes, personnel controls, and explore potential new control regimes at all levels of governance.

Third, the U.S. should aggressively pursue its national strategy to include stronger partnership efforts with responsible nations in an international effort to more vigorously deter the use of bioweapons. A specific national strategy for biodefense is good, but must expand and encompass leading the world's efforts by example.

Fourth and finally, the U.S. should pursue all of the above in a wrapper of transparency to let all would be nation, group, or individual actors who consider employing bioweapons, know that the ground is sour for the seeds of bioweapons. No single strategy can hold back the forces of technological change that empower these would-be actors, but in totality these measures can hopefully prevent or at least greatly mitigate the potential impacts.

VII. Conclusions

The realizations of a biological agent attack on the United States and its related shockwaves have already been felt. The U.S. has already taken some bold steps in building a better biodefense, however the nation has not gone far enough. It must realize that the threat and lethality of asymmetric attacks will only grow without deliberate communication and coordination on all fronts coupled with a well funded, defense-in-depth strategy for biodefense. When considering defense funding and the future, resources must be focused on the most effective means of deterrence thereby maximizing the return on investment. Utilizing the

advantages of international cooperation and strategic military transparency to its fullest certainly deserves more attention than what the United States has given it in the past. With that said, it will be important to continue biodefense efforts across a broad front, with diversity of measures being critical. The United States must target all attributes of the biothreat, using all available tools--from the cognitive realms of transparency and partnerships which have the potential to shape and dissuade, to the firm reality of denial and punishment through vaccinations and kinetic responses as necessary.

The U.S. must stay engaged world-wide and continue to lead biodefense efforts for a safer world. The very nature of bioweapons and the growing potential for bioterrorism presents a formidable problem for strategy makers. Biodefense is a global imperative and can be successful with a long term strategy led by the United States. The United States has a unique position as a beacon of freedom and opportunity and world leader as a military and economic superpower. The U.S. must take responsibility to lead the world in shaping a strategy that will provide defense in-depth against any potential use of a bioweapon. This strategy must harness and couple all instruments of power... from diplomatic/cognitive to kinetic. As stated by journalist Thomas Friedman, "If we don't visit bad neighborhoods, they will surely visit us."[79]

Appendix 1

Key Findings from the National Infrastructure Advisory Council.[80]

- Interdependencies across critical infrastructure sectors are exceptionally high in a biological event and must be fully understood. The interdependent relationships most often cited were for the basic municipal and other infrastructure support requirements, including energy, information technology, communications, and water.
- Subtle interdependencies between critical goods and services and the critical infrastructure worker, including basic physical security requirements, financial services for businesses and workers, and food and healthcare to sustain workers and their families, are no less important than the direct inter-dependencies.
- Supply chain interdependencies, specifically the essential role transportation plays as a bridge between all levels of the supply and distribution chain, are yet another venue to be further studied and understood.
- Basic critical infrastructure sectors generally provide a limited number, but critical number of goods and services (e.g. potable water and wastewater treatment, electrical generation and distribution, and postal and shipping services).
- Some sectors, including Food and Agriculture, Commercial Facilities, and Chemical, manufacture and distribute goods that may require thousands of line items of goods to be assessed and prioritized to determine each one's criticality. More research is needed to better prioritize these sectors and their goods and services.
- There are numbers of geographically sparse, single-source businesses (e.g. baby formula producers) and goods/services (e.g. chlorine for water treatment, ATM maintenance) that represent potential single points of failure.

Appendix 2

Main Articles of the Biological and Toxins Weapons Convention (BTWC)[81]

Article I defines the scope of the BTWC's prohibition (the so-called general purpose criterion). This includes all microbial and other biological agents or toxins and their means of delivery. Subsequent Review Conferences have reaffirmed that the general purpose criterion encompasses all future scientific and technological developments relevant to the Convention. The objects themselves (biological agents or toxins) are not prohibited, only their purpose. Permitted purposes are defined as prophylactic, protective and other peaceful purposes. The objects may not be retained in quantities that have no justification or which are inconsistent with the permitted purposes.

Article II requires each State Party, no later than nine months after entry into force of the Convention, to destroy or divert to peaceful purposes all agents, toxins, weapons, equipment and means of delivery specified in Article I.

Article III prohibits States Parties from transferring or otherwise encouraging other states or organizations to acquire any of the agents, toxins, weapons, equipment or means of delivery specified in Article I.

Article IV requires States Parties to take any necessary national measures (e.g., passage of national laws) to prohibit and prevent the misuse of biological agents, toxins, weapons, equipment and means of delivery within their territories. Only a small number of States Parties have implemented this provision.

In **Article V**, States Parties undertake to consult with one another and to cooperate in solving any problems that may arise in relation to the Convention.

Under **Article VI**, any State Party finding another State Party acting in breach of the Convention may lodge a complaint with the United Nations Security Council. States Parties will cooperate in carrying out any investigation the Security Council may initiate on the basis of the complaint. The Security Council will inform States Parties of the results of the investigation.

In **Article VII**, States Parties undertake, if requested, to assist any Party which the Security Council decides has been exposed to danger as a result of violation of the Convention.

Article VIII stipulates that nothing in the Convention shall in any way limit or detract from obligations assumed under the Geneva Protocol.

Article IX commits States Parties to continue negotiations in good faith towards a chemical weapons convention.

In **Article X**, States Parties undertake to facilitate the fullest possible exchange of equipment, materials and scientific and technological information for the use of biological agents and toxins for peaceful purposes.

In **Article XII**, provision is made for a conference of States Parties to the Convention to review the operation of the Convention, with a view to assuring that the purposes of the preamble and the provisions of the Convention, including the provisions concerning negotiations on chemical weapons, are being realized. Such review shall take into account any new scientific and technological developments relevant to the Convention. Such Review Conferences have been held at five yearly intervals and have agreed Final Declarations which have contained extended understandings of the Convention.

Appendix 3

Samples for International Partnership

Rapid Detection

France awarded a contract to EADS for part of its "DETECBIO" system. [82] The €35M contract is for the design and production of the SAMOA (Systeme d'Alerte MObile Avancee, Advanced Mobile Alert System), which will provide the French Army with systems for detecting and identifying biological warfare agents for the protection of their deployed forces and critical sites.[83] With France having recently joined the military alliance portion of NATO there is certainly opportunity for technology sharing or possibly a multi-national program to reduce R&D and/or procurement costs. This would also increase/enhance the interoperability of participating nation's deployed forces. In general, if countries are similarly equipped or capable, they are more likely to use their forces in support of each other.

Rapid Identification

The U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID)[84] has a course to teach students how to rapidly identify biological agents in the field using deployable laboratories. The course is called the "Field Identification of Biological Warfare Agents" (FIBWA) and is the only one of its kind in the DoD.[85] The course teaches some advanced techniques such as how to extract genetic material (DNA and RNA) along with a technique called polymerase chain reaction or PCR, which is used to identify the extracted genetic material in as little as two to four hours.[86] As these capabilities continue to advance it will be important to have a level of transparency here to let would be adversaries know their intended efforts will be foiled and ineffective.

Bibliography

Belasco, Amy. "The Cost of Iraq, Afghanistan, and Other Global War on Terror Operations Since 9/11." Congressional Research Service Report for Congress, 28 Sep 2009.

Bozheyeva, Gulbarshyn, Yerlan Kunakbayev, and Dastan Yeleukenov. *Former Soviet Biological Weapons Facilities in Kazakhstan: Past, Present, and Future*, The Center for Nonproliferation Studies (CNS) at the Monterey Institute of International Studies, June 1999.

Center for Nonproliferation Studies, Monterey Institute of International Studies, "Cruise Missiles and Unmanned Aerial Vehicles Deployed in the Middle East," n.p.

Center for Nonproliferation Studies. Inventory of International Nonproliferation Organizations and Regimes, BTWC, http://www.nti.org/e_research/official_docs/inventory/pdfs/btwc.pdf, last updated on 27 June 2009 (accessed 22 Jan 2010).

Centers for Disease Control and Prevention (CDC) website. (2003). *Critical incidence protocol*. http://www.bt.cdc.gov (accessed November 24, 2009).

Clarke, Richard A. *Breakpoint*, New York, NY: G.P. Putnam's Sons, 2007.

Cleland, Cathy, Dr., Blue Horizons briefing and interview at Los Alamos National Laboratory, NM, 2009.

Davis, Jim A. and Barry R. Schneider. *The Gathering Biological Warfare Storm*, Westport, CT: Pradger, 2004.

Davis, Jim A. and Johnson-Winegar, Anna R. "The Anthrax Terror: DOD's Number-One Biological Threat," *Aerospace Power Journal*, Winter 2000, 15-29.

"Disarmament of the Biomedpreparat complex in Stepnogorsk," Report of the Joint Kazakhstan-United States Commission, November 19-20, 1996.

Doctrine for the Armed Forces of the United States, Joint Publication 1, 14 May 2007.

Doyle, Charles. "The USA PATRIOT Act: A Sketch**,"** CRS Report for Congress, April 18, 2002.

Eckert, Paul. "Pentagon criticizes China on military transparency." Reuters.com, http://www.reuters.com/articlePrint?articleID=USTRE5205PX20090325 (accessed November 24, 2009).

Ewing, Humphry Crum, Cruise Missiles: Precision Countermeasures, Bailrigg Memo 10, Lancaster, UK: Centre for Defence and International Security Studies, 1995.

"Faces of the Fallen." The Washington Post online, http://projects.washingtonpost.com/fallen/ (accessed 16 Jan 2010).

Garcia, Deborah Koons. *The Future of Food*, Lily Films, 2004.

Forstchen, William R. *One Second After*, Tom Doherty Associates, LLC, 2009.

Garreau, Joel. *Radical Evolution: The Promise and Peril of Enhancing Our Minds, our Bodies--and What It Means to Be Human*, 2005.

Gibson, William. "Rocket Radio," *Rolling Stone*, June 15, 1989.

Gladwell, Malcolm. "The Tipping Point," *The New Yorker*, June 3, 1996.

Human Genome Project homepage, http://www.ornl.gov/sci/techresources/Human_Genome/home.shtml (accessed 25 Nov 2009).

Joy, Bill. "Why the future doesn't need us," Wired magazine, 8.04, http://www.wired.com/wired/archive/8.04/joy_pr.html.

King, David. "An ethical code for scientists," transcript of interview on ABC Radio National Science Show, 6 Oct 2007, http://www.abc.net.au/rn/scienceshow/stories/2007/2049039.htm.

Kinnan, Scott Colonel, "Deterrence Operations: Summary briefing from NATO Joint Capabilities Development and Experimentation (CD&E) Conference, Center for Strategy and Technology, Maxwell AFB AL, Fall 2009.

Kurzweil, Ray. *The Singularity is Near: When Humans Transcend Biology*, New York, NY: Viking, 2005.

Linden, Carrie Vander, "Bio-Warfare Detectives," *Soldiers*, May 2005.

Lindley, Dan. *Promoting Peace with Information: Transparency as a Tool of Security Regimes*, Princeton, NJ: Princeton University Press, July 17, 2006.

Manshu, Xu Major (People's Liberation Army). "An Analysis of Military Transparency." National Defense University, 2009.

McFedries, Paul. "Tipping Point," http://www.wordspy.com/words/tippingpoint.asp (accessed 12 Dec 2009).

McIlroy, Anne. "Scientists get their own Hippocratic oath," Globe Life, from Globe and Mail website, http://www.theglobeandmail.com/life/article692696.ece.

Milanovich, Fred, "Reducing the Threat of Biological Weapons," https://www.llnl.gov/str/Milan.html.

Military Technology, MILTECH. "EADS Wins French Bio Detection Award,", 5/2009.

Mizrach, Steve, "Did 22 SDI Researchers really ALL Commit Suicide?" http://www.fiu.edu/~mizrachs/sdi-deaths.html (accessed on 17 Dec 2009).

Mizrach, Steve. "Technology and Transgression," http://www.fiu.edu/~mizrachs/tech-trans.html, (accessed on 17 Dec 2009).

Monterey Institute of International Studies, Cruise Missiles and Unmanned Aerial Vehicles (UAV) Deployed in the Middle East, http://cns.miis.edu/wmdme/crui_dep.htm, February 8, 2000.

National Infrastructure Advisory Council, "Chemical, Biological, and Radiological Events and the Critical Infrastructure Workforce, Final Report and Recommendations by the Council," Jan 08, 2008.

Oliver, Richard W. *The Biotech Age: The Business of Biotech and How to Profit from it*. New York, NY: The McGraw Hill Companies, 2003.

Purkitt, Helen E. Biowarfare Lessons, Emerging Biosecurity Issues, and Ways to Monitor Dual-Use Biotechnology Trends in the Future, Institute for National Security Studies, USAF Academy, Colorado, INSS Occasional Paper 61, September, 2005.

Sands, Amy Ph.D. Center for Nonproliferation Studies, Monterey Institute of International Studies, "Deconstructing the Chem-Bio Threat," Testimony before the U.S. Senate Foreign Relations Committee, March 19, 2002.

Shaud, John A., PhD and Lowther, Adam PhD. "Deterring Nonstate Actors," Air Force Research Institute, Maxwell Air Force Base, Alabama, November 2009.

Smart, John. "Building Global Immunity: Anticipating, Preventing and Responding to Super empowered Individuals and Groups in a Metaverse Society," Blue Horizons 2008–CSAT, briefing given at Maxwell AFB, Montgomery, AL, Nov 2008.

Specter, Michael. "A Life of Its Own: Where will synthetic biology lead us?" *The New Yorker*, September 28, 2009.

The Biological and Toxins Weapons Convention Website, http://www.opbw.org/convention/conv.html (accessed in November 2009).

The Bulletin of Atomic Scientists. "Biodefense efforts need transparency." Vol. 64, No.5, November/December 2008.

The Center for Arms Control and Non-proliferation, "Federal funding for Biological Weapons Prevention and Defense, Fiscal Years 2001 to 2009, April 15, 2008 (revised May 27, 2008).

The Center for Arms Control and Nonproliferation, "Understanding President Bush's FY2009 Biodefense Budget Request." Briefing to Capitol Hill, http://www.fas.org/blog/ssp/2008/06/understanding-president-bushs-fy2009-biodefense-budget-request.php, 12 June 2008.

The Compact Oxford English Dictionary of Current English. http://www.askoxford.com/results/?view=dev_dict&field-12668446=transparent&branch=13842570&textsearchtype=exact&sortorder=score%2Cname (accessed 8 Feb 2010).

The Department of Homeland Security Website. Fact Sheet on the National Biodefense Analysis and Countermeasures Center. http://www.dhs.gov/files/labs/gc_1166211221830.shtm (accessed 21 Jan 2010).

"The National Strategy for Countering Biological Threats," National Security Council, The White House, November 2009.

The National Security Strategy of the United States of America, March 2006.

Unclassified Report to Congress on the Acquisition of Technology Relating to Weapons of Mass Destruction and Advanced Conventional Munitions; submitted by the Deputy Director of National Intelligence for Analysis, 1 January-31 December 2004.

Venkayya, Rajeev M.D., Former Senior Director for Biodefense (HSC) for the Bush Administration, interview by the author, 27 December 2009.

Zinkovich, L., Malvey, D., Hamby, E. and Fottler, M. "Bioterror Events: Preemptive strategies for healthcare executives." *Hospital Topics: Research and Perspectives on Healthcare*. Vol. 83, (3), 2005.

Endnotes

[1] Shaud, John A., PhD and Lowther, Adam PhD. "Deterring Nonstate Actors," Air Force Research Institute, Maxwell Air Force Base, Alabama, November 2009, pg. 3.

[2] "Faces of the Fallen." The Washington Post online. http://projects.washingtonpost.com/fallen/ (accessed 16 Jan 2010).

[3] Belasco, Amy. "The Cost of Iraq, Afghanistan, and Other Global War on Terror Operations Since 9/11." Congressional Research Service Report for Congress, 28 Sep 2009. pg. 1.

[4] Davis, Jim A. and Barry R. Schneider. *The Gathering Biological Warfare Storm*, 2004, pg. 11.

[5] The National Security Strategy of the United States of America, March 2006, pg. x.

[6] Garreau, Joel. *Radical Evolution: The Promise and Peril of Enhancing Our Minds, our Bodies--and What It Means to Be Human*, 2005, pg. 4.

[7] Gladwell, Malcolm. "The Tipping Point," *The New Yorker*, June 3, 1996.

[8] McFedries, Paul. "Tipping Point," from WordSpy internet site, accessed on 12 Dec 2009 at http://www.wordspy.com/words/tippingpoint.asp

[9] The National Infrastructure Advisory Council conducted an extensive survey across the critical infrastructure to identify key resources needed to respond to or recover from a biological event; though focused on a pandemic influenza, its findings would be beneficial, if not central to an alternative form of biological event.

[10] National Infrastructure Advisory Council, "Chemical, Biological, and Radiological Events and the Critical Infrastructure Workforce, Final Report and Recommendations by the Council," Jan 08, 2008.

[11] National Infrastructure Advisory Council, "Chemical, Biological, and Radiological Events and the Critical Infrastructure Workforce, Final Report and Recommendations by the Council," Jan 08, 2008.

[12] The U.S. Census Bureau recently released population estimates for Combined Statistical Areas (formerly known as Metropolitan Statistical Areas), Metropolitan Areas (stand-alone or components of CSAs), and Micropolitan Areas. The top thirty U.S. metropolitan areas range from New York with almost 22 million to San Antonio with 1.9 million people. This data was based on mid-year 2006 population estimates and was accessed from http://geography.about.com/od/lists/a/csa2005.htm; article dated 22 July 2009.

[13] "Congress passed the USA PATRIOT Act (the Act) in response to the terrorists' attacks of September 11, 2001. The Act gives federal officials greater authority to track and intercept communications, both for law enforcement and foreign intelligence gathering purposes. ~ Excerpt from Congressional Research Service Report to Congress, 18 April 2002.

[14] The Center for Arms Control and Non-proliferation, "Federal funding for Biological Weapons Prevention and Defense, Fiscal Years 2001 to 2009, April 15, 2008 (revised May 27, 2008).

[15] Project BioShield is a ten year program run under the Department of Homeland Security. Project BioShield's aim is to acquire medical countermeasures to Chemical, Biological, radiological, and nuclear agents for civilian use.

[16] The Center for Arms Control and Nonproliferation, "Understanding President Bush's FY2009 Biodefense Budget Request." accessed at http://www.fas.org/blog/ssp/2008/06/understanding-president-bushs-fy2009-biodefense-budget-request.php, dated 12 June 2008.

[17] Dr. Rajeev Venkayya, Former Senior Director for Biodefense (HSC), interview by the author, 27 December 2009.

[18] Davis, Jim A. and Dr. Anna Johnson-Winegar. "The Anthrax Terror: DOD's Number-One Biological Threat," *Aerospace Power Journal*, Winter 2000, pg. 15.

[19] Centers for Disease Control and Prevention (CDC) website. (2003). *Critical incidence protocol*. http://www.bt.cdc.gov (accessed November 24, 2009).

[20] Zinkovich, L., Malvey, D., Hamby, E. and Fottler, M. Bioterror Events: Preemptive strategies for healthcare executives. *Hospital Topics: Research and Perspectives on Healthcare*, 2005.

[21] In accordance with the National Intelligence Center (NAIC), ten other countries along with the U.S. have Land-Attack Cruise Missiles (LACMs) to include China, France, Germany, Sweden, Italy, Israel, Russia, South Africa, and the UK. Further, many of these countries export these wares to countries the U.S. considers "rogue nations" to include Iran, Iraq (pre-OIF), North Korea, and Syria.

[22] Davis, Jim A. and Barry R. Schneider. *The Gathering Biological Warfare Storm*, 2004, pg 167.

[23] Center for Nonproliferation Studies, Monterey Institute of International Studies, "Cruise Missiles and Unmanned Aerial Vehicles Deployed in the Middle East," n.p.

[24] Sands, Amy Ph.D. Center for Nonproliferation Studies, Monterey Institute of International Studies, "Deconstructing the Chem-Bio Threat," Testimony before the U.S. Senate Foreign Relations Committee, March 19, 2002.

[25] Scientists from South Africa (clandestine Project Coast terminated in 1993) and former Yugoslavian scientists and workers (1991 breakup left three chemical weapon facilities) also became available for hire following dismantlement of their weapon programs.

[26] Ibid.

[27] Dr. Rajeev Venkayya, interview by the author, 27 December 2009.

[28] "NBACC is part of a nationwide group of institutions that collectively are referred to as the Homeland Security Biodefense Complex. The Complex includes the Plum Island Animal Disease Control Center, the Biodefense Knowledge Center, the national laboratories, and the university-based Homeland Security Centers of Excellence." ~ Excerpt from DHS website referenced in Endnote #29 below.

[29] The Department of Homeland Security Website. Fact Sheet on the National Biodefense Analysis and Countermeasures Center. http://www.dhs.gov/files/labs/gc_1166211221830.shtm (accessed 21 Jan 2010).

[30] The Department of Homeland Security Website. Fact Sheet on the National Biodefense Analysis and Countermeasures Center. http://www.dhs.gov/files/labs/gc_1166211221830.shtm (accessed 21 Jan 2010).

[31] Davis, Jim A. and Barry R. Schneider. *The Gathering Biological Warfare Storm*, 2004, pg 175.

[32] Ibid.

[33] Kazakhstani Biowarfare facilities belonged to various parts of the Soviet Biowarfare structure and reported to different central authorities in Moscow. The four main facilities were the Vozrozhdeniye Island open-air test site in the Aral Sea, the Scientific Experimental and Production Base (SNOPB) in Stepnogorsk, the Scientific Research Agricultural Institute (NISKhI) in Gvardeyskiy, and the Anti-Plague Scientific Research Institute in Alma-Ata.

[34] "Disarmament of the Biomedpreparat complex in Stepnogorsk," Report of the Joint Kazakhstan-United States Commission, November 19-20, 1996.

[35] Davis, Jim A. and Barry R. Schneider. *The Gathering Biological Warfare Storm*, 2004, pg. 175.

[36] Garcia, Deborah Koons. *The Future of Food*, Lily Films, 2004.

[37] Cleland, Cathy, Dr. (PhD in Biochemistry), Blue Horizons briefing and interview at Los Alamos National Laboratory, NM, 2009.

[38] Ibid.

[39] Clarke, Richard A. *Breakpoint*, 2007, pg 309.

[40] Garreau, Joel. *Radical Evolution: The Promise and Peril of Enhancing Our Minds, our Bodies--and What It Means to Be Human*, 2005, pg. 4.

[41] Clarke, Richard A. *Breakpoint*, pg 309.

[42] Tom Knight, a senior research scientist at M.I.T, helped invent the field name of "BioBricks" or biological components (Specter, 2009).

[43] Specter, Michael. "A Life of Its Own: Where will synthetic biology lead us?" *The New Yorker*, September 28, 2009.

[44] Specter, Michael. "A Life of Its Own: Where will synthetic biology lead us?, 2009, Pg. X.

[45] Ibid.

[46] Human Genome Project homepage, http://www.ornl.gov/sci/techresources/Human_Genome/home.shtml (accessed 25 Nov 2009).

[47] Cleland, Cathy, Dr., Blue Horizons briefing and interview at Los Alamos National Laboratory, NM, 2009.

[48] The latter term, KMD, has been recently coined to distinguish those weapons of mass destruction that have emerged with the acceleration of availability of knowledge alone, i.e. not requiring rare materials or elaborate facilities. Sourced from: Joy, Bill. "Why the future doesn't' need us," Wired magazine, 8.04, http://www.wired.com/wired/archive/8.04/joy_pr.html. pg. 4.

[49] Shaud, John A., PhD and Lowther, Adam PhD. "Deterring Nonstate Actors," Air Force Research Institute, Maxwell Air Force Base, Alabama, November 2009, pg 13.

[50] Kinnan, Scott Colonel. Center for Strategy and Technology, Maxwell AFB AL, "Deterrence Operations: Summary briefing from NATO Joint Capabilities Development and Experimentation (CD&E) Conference, Fall 2009, slide 3.

[51] Ibid.

[52] Ibid.

[53] *Doctrine for the Armed Forces of the United States, Joint Publication 1*, dated 14 May 2007, pg x.

[54] Kinnan, Scott Colonel. "Deterrence Operations," 2009, slide 5.

[55] Kinnan, Scott Colonel. "Deterrence Operations," 2009, slide 5.

[56] Kinnan, Scott Colonel. "Deterrence Operations," 2009, slide 13

[57]Ibid.

[58] Ibid.

[59] Ibid.

[60] Gibson, William. "Rocket Radio," *Rolling Stone*, June 15, 1989.

[61] The Compact Oxford English Dictionary of Current English. http://www.askoxford.com/results/?view=dev_dict&field-12668446=transparent&branch=13842570&textsearchtype=exact&sortorder=score%2Cname (accessed 8 Feb 2010).

[62] Manshu, Xu Major (People's Liberation Army). "An Analysis of Military Transparency." National Defense University, 2009, pg 1.

[63] Eckert, Paul. "Pentagon criticizes China on military transparency." Reuters.com, http://www.reuters.com/articlePrint?articleID=USTRE5205PX20090325 (accessed November 24, 2009).

[64] Oliver, RichardW. *The Biotech Age: The Business of Biotech and How to Profit from it*. The McGraw Hill Companies, New York, 2003.

[65] *The Bulletin of Atomic Scientists.* "Biodefense efforts need transparency." Vol. 64, No.5, pg. 6. November/December 2008.

[66] As of 27 June 2009, there were 176 states who had signed The Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction—also known as the Biological and Toxin Weapons Convention (BTWC). 163 countries had ratified their signature.

[67] Center for Nonproliferation Studies. Inventory of International Nonproliferation Organizations and Regimes, BTWC, last updated on 27 June 2009, http://www.nti.org/e_research/official_docs/inventory/pdfs/btwc.pdf (accessed 22 Jan 2010).

[68] King, David. "An ethical code for scientists," transcript of interview on ABC Radio National Science Show, 6 Oct 2007, http://www.abc.net.au/rn/scienceshow/stories/2007/2049039.htm.

[69] Ibid.

[70] McIlroy, Anne. "Scientists get their own Hippocratic oath," Globe Life, from Globe and Mail, published on 20 June 2008 and last updated 30 March 2009, http://www.theglobeandmail.com/life/article692696.ece.

[71] "The National Strategy for Countering Biological Threats," National Security Council, The White House, November 2009, outline page.

[72] Dr. Rajeev Venkayya, interview by the author, 27 December 2009.

[73] Ibid.

[74] Smart, John. "Building Global Immunity: Anticipating, Preventing and Responding to Super empowered Individuals and Groups in a Metaverse Society," Blue Horizons 2008–CSAT, briefing given at Maxwell AFB, Montgomery, AL, Nov 2008.

[75] Ibid.

[76] Mizrach, Steve PhD. "Did 22 SDI Researchers really ALL Commit Suicide?" http://www.fiu.edu/~mizrachs/sdi-deaths.html (accessed on 17 Dec 2009).

[77] Kinnan, Scott Colonel. "Deterrence Operations," 2009, slide 4.

[78] Forstchen, William R. *One Second After*, Tom Doherty Associates, LLC, 2009.

[79] Friedman, Thomas. Direct quote from author and journalist Thomas Friedman, taken from National Strategic Decision Making lecture, Air War College, Maxwell AFB, AL, Fall 2009.

[80] National Infrastructure Advisory Council, "Chemical, Biological, and Radiological Events and the Critical Infrastructure Workforce, Final Report and Recommendations by the Council," Jan 08, 2008.

[81] Sourced from The Biological and Toxins Weapons Convention website at http://www.opbw.org/convention/conv.html (accessed in November 2009).

[82] The DETECBIO system consists of a network of environmental monitoring sensors, means of identifying biological agents, and an information and supervision system. It is being developed with the Pasteur Institute, the French Atomic Energy Commission, and other subject matter experts.

[83] "EADS Wins French Bio Detection Award," Military Technology, MILTECH, 5/2009, pg 91.

[84] USAMRIID is a partner in the National Interagency Biodefense Campus at Fort Detrick, MD.

[85] Linden, Carrie Vander, "Bio-Warfare Detectives," *Soldiers*, May 2005, pg 43.

[86] Linden, pg 44.