Description of document: Title of Thesis: Intelligence Support to The Life Science Community: Mitigating Threats Posed By Bioterrorism, 2004. Released by the Office of The Director of National Intelligence (ODNI)

Requested date: 18-September-2017

Release date: 04-December-2024

Posted date: 23-December-2024

Source of document: FOIA Request
Director, Information Management Office
ATTN: FOIA/PA
Office of the Director of National Intelligence
Washington, D.C. 20511
Email: ODNI_FOIA@odni.gov

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC

3 December 2024

Reference: ODNI Case No. DF-2022-00321

This letter provides an interim response to your Freedom of Information Act (FOIA) request to the Defense Intelligence Agency (DIA), dated 18 September 2017, requesting 18 specific theses written by students at the National Intelligence University. As previously noted by DIA, DIA transferred these cases to the Office of the Director of National Intelligence (ODNI) in 2022.

ODNI processed this request under the FOIA, 5 U.S.C. § 552, as amended and located 17 of the theses requested. Note, despite a thorough search, "Rationing the IC: The Impact of Private American Citizens on the Intelligence Community" was not located.

This interim response provides a response on ten of the theses. During the review process, we considered the foreseeable harm standard and determined that certain information must be withheld pursuant to the following FOIA exemptions:

- (b)(3), which applies to information exempt from disclosure by statute. Specifically, the National Security Act of 1947, as amended:
  - Section 102A(i)(l), 50 U.S.C. § 3024(i)(1), which protects information pertaining to intelligence sources and methods; and
  - Section 102A(m), as amended, 50 U.S.C. § 3024(m), which protects the names and identifying information of ODNI personnel.
- (b)(6), which applies to information that, if released, would constitute a clearly unwarranted invasion of personal privacy.

Be advised, we continue to process your request. If you are not satisfied with this response, a number of options are available. You may contact me, the FOIA Public Liaison, at ODNI_FOIA_Liaison@odni.gov, or the ODNI Requester Service Center, at ODNI_FOIA@odni.gov or (703)-275-1313. You may also submit an administrative appeal to the Chief FOIA Officer, c/o Chief, Information Management Office, Office of the Director of National Intelligence, Washington, DC 20511 or emailed to ODNI_FOIA@odni.gov. The appeal correspondence should be clearly marked "Freedom of Information Act Appeal of Adverse Determination" and must be postmarked or electronically transmitted within 90 days of the date of this letter.

Lastly, the Office of Government Information Services (OGIS) of the National Archives and Records Administration is available with mediation services and can be reached by mail at 8601

Adelphi Road, Room 2510, College Park, MD 20740-6001; telephone (202) 741-5770; toll-free (877) 684-6448; or email at ogis@nara.gov.

Sincerely,

Erin Morrison
Chief, Information Review and Release Group
Information Management Office

INTELLIGENCE SUPPORT TO THE LIFE SCIENCE COMMUNITY:

MITIGATING THREATS POSED BY BIOTERRORISM

by

[redacted]
Defense Intelligence Agency
PGIP-E Class 0201

Unclassified thesis submitted to the Faculty
of the Joint Military Intelligence College
in partial fulfillment of the requirements for the degree of
Master of Science of Strategic Intelligence

July 2004

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

ACKNOWLEDGEMENTS

I would like to extend my deep gratitude to following individuals who provided substantive insight, technical expertise, or general guidance: [redacted], for serving as my thesis chair and challenging me to apply a critical eye toward my research; [redacted] for serving as my second reader and encouraging me to 'push the envelope'; [redacted], for incredibly helpful discussions regarding the life science community; and [redacted], for his insights and support.

CONTENTS

LIST OF FIGURES

Figure **Page**

ABSTRACT

TITLE OF THESIS: Intelligence Support to the Life Science Community: Mitigating Threats Posed by Bioterrorism

STUDENT: [redacted]

CLASS NO: PGIP-E 0201 **DATE:** July 2004

THESIS COMMITTEE CHAIR: [redacted]

SECOND COMMITTEE MEMBER: [redacted]

This thesis set out to answer the following research question: Can the U.S. intelligence community mitigate threats from bioterrorism by supporting efforts of the U.S. life science research community to address public concerns regarding misuse of openly communicated "dual use" research findings? The thesis concludes that a role does exist for the intelligence community to reduce current and emerging threats by engaging life scientists at a variety of levels. Moreover, the thesis identifies a number of long term benefits to the intelligence community that can only be realized through closer partnerships with life scientists and charges intelligence professionals to take the initiative in building relationships with leading life scientists from academia and private industry.

The attacks of September 11th and subsequent use of the U.S. Postal Service to deliver *Bacillus anthracis* (anthrax) in October 2001 have resurrected a decades-old debate regarding the potential for open communication of life science research findings to enable bioterrorists. How this debate is resolved likely will have significant implications for national security and could potentially impact the quality of U.S. biodefense and public health research programs. This thesis discusses how the intelligence community is

well positioned to support the scientific community as it seeks to achieve an optimal equilibrium between openness and security and outlines a few options for such support.

Specifically, chapter I provides a detailed review of the debate on scientific openness and national security that has occurred within the life science research community during the past fifty years. Chapter II underscores the implications of this debate upon the national security professional by exploring the potential for life science discoveries to impact biological warfare and the changes such advances will necessitate in all areas of biodefense. Chapter III provides examples of the type of support IC professionals can offer life scientists, including a recently declassified case study regarding al-Qaida exploitation activities, to ensure that any policies and procedures that are implemented are appropriate to the nature and level of the threat. Finally, chapters IV and V outline a strategy for life scientists to execute laboratory research that could mitigate biotechnology-enabled threats by enhancing the ability of intelligence analysts to more accurately assess threats posed by biological weapons.

CHAPTER 1

OPEN SCIENCE VS. NATIONAL SECURITY: AN OVERVIEW

INTRODUCTION

The al-Qaida attacks of September 11, 2001 and delivery of *Bacillus anthracis* (anthrax) via the United States Postal Service have triggered a significant increase in biodefense initiatives and reinvigorated a decades-old debate regarding the potential for openly published scientific findings to support the efforts of bioterrorists and biological warfare (BW) researchers. Progression of this debate towards resolution could be facilitated by input from US intelligence and national security professionals who likely possess insights that are not available to the general scientific community. Active participation and ongoing collaboration between the national security and bioscience research communities will be a key factor in minimizing current and future bioterror and BW challenges presented by proliferation of dual use research findings.

National security professionals have a critical role to play in helping life scientists secure the homeland against misuse of their research findings by malevolent actors. However, with the exception of some recent discussions, the relationship between the national security and life science communities has been nearly nonexistent; thus, initial approaches and interactions must be rationally planned and carefully executed to ensure that solid bridges are built between the two communities. To avoid promulgating misperceptions that may impede their ability to support the scientific community, national security professionals need to be thoroughly familiarized with the historic and current discussions among leading scientists regarding the potential for openly published research findings to inadvertently support BW or bioterrorism. This article provides an overview of the debate regarding restriction of scientific information of concern, summarizes more recent discussions among bioscience researchers, and outlines some basic options for the IC to assist the life science community.[1]

EARLY DISCUSSIONS OF NATIONAL SECURITY AND SCIENCE

Since the 1940's, the United States national security community has worked with scientific organizations and research communities to develop an established policy for identifying areas of basic and applied research where information controls may be required. Such research, historically related either to weapons development or sensitive nuclear technologies, has been designated as classified and had strict dissemination controls placed upon it. For example, prior to the US entry into World War II, physicists in the private sector researching nuclear fission voluntarily stopped publishing results in scientific journals for fear of contributing to Germany's nuclear bomb project.[2] In early 1940, the joint National Academy of Sciences (NAS) – National Research Council

[1] Dana Shea, "Balancing Scientific Publication and National Security Concerns: Issues for Congress," *CRS Report for Congress* (Washington, DC: Congressional Research Service, Library of Congress, 2003).

[2] Peter J. Westwick, "In the Beginning: The Origin of Nuclear Secrecy," *Bulletin of the Atomic Scientists* 56 (November, December 2000): 43-49.

(NRC) Advisory Committee on Scientific Publications was established to explore options for restricting publication on nuclear fission. During US involvement in World War II, this committee secured the cooperation of scientific journals in limiting the transfer of scientific information within the United States.[3]

Research into nuclear power is another area where information controls have been instituted. Private industry was permitted to explore limited applications of nuclear power under the Atomic Energy Act of 1954. Prior to this act, the federal government protected nuclear energy activities with security and secrecy programs. The Atomic Energy Act prohibited dissemination of nuclear research information from its creation regardless of who controls it.[4] Information developed in this area, even if developed privately without federal government aid, is regarded as "born classified." Importantly, when fundamental research is not classified, no other information controls are placed upon it.[5] However, the federal government retains authority over results that relate to atomic weapons, production of special nuclear material (SNM), and use of SNM in the production of energy.[6]

Although the controls established by the federal government to regulate the spread of nuclear research findings adequately mitigate security concerns presented by

[3] Rexmond C. Cochrane, *The National Academies of Sciences: The First Hundred Years, 1863-1963* (Washington, D.C.: National Academy of Sciences, 1978), 385-387; Shea, 2-6.

[4] See 42 U.S.C.S. 2014(y) (2003)

[5] Shea, 2.

[6] Harold Relyea, *Silencing Science: National Security Controls and Scientific Communication* (Norwood, New Jersey: Ablex Publishing Corporation, 1994), 94-96.

proliferation of specific nuclear technologies, they are challenged to provide similar protection against threats enabled by the life sciences. Federal regulations regarding nuclear research were implemented at a time when the fundamental research fields were relatively young and expertise was consolidated within a handful of talented minds. Thus, encapsulation of fission research was feasible through creation of mutually beneficial relationships between key scientists and the federal government. Having implemented regulations upon a research field in its nascent stages, it was possible for the federal government to support further research and development in an environment under security and classification control.

Importantly, key factors that permitted the restriction of nuclear findings without preventing further technological advances do not currently apply to the life sciences. With the exception of specific work pertaining to the former U.S. bioweapons program, halted in 1969 under executive order by President Richard Nixon, and a relative handful of biodefense projects, the vast majority of the life sciences have developed throughout the past half century without any restrictions or controls. Expertise is not maintained in the minds of a few talented scientists, but rather exists as an international network containing tens of thousands of researchers working to address fundamental questions across a broad spectrum of life science fields. Federally mandated containment is not the effective option it was sixty years ago.

Not only is generalized federal restriction of life science research impractical, it could be disastrous. Life science research builds upon multiple findings across a variety of seemingly unrelated fields in a manner not unlike a spider's web. Removing one strand of that web through federal restriction likely would have negative implications for the other fields within the web that are difficult to estimate. Even generalized restriction within fields with greatest application towards bioterrorism or BW could greatly hinder biodefense research efforts to develop medical countermeasures, including new vaccines and therapeutics. Before national security professionals can productively engage the scientific community regarding threats presented by the open publication of some research findings, there must be mutual agreement that the generalized federally-mandated restrictions used to contain nuclear research are not a viable option.

THE PRE-2001 LIFE SCIENCE/NATIONAL SECURITY DEBATE

Discussions regarding the impact of life science discovery upon national security first received major attention within the U.S. research community following key discoveries related to recombinant DNA research; specifically the development of readily applicable and reliable techniques to manipulate an organism's genetic material and elicit a novel effect. Genetic engineering and the creation of recombinant species were topics of great contention in the 1970s, resulting in calls for regulation of the methods for manipulating DNA and of experiments containing genetically engineered species.[7] To facilitate resolution of those concerns, a number of leading scientists in the field gathered at the Asilomar conference in Pacific Grove, California in 1975 to propose mechanisms for assessing and managing the risk and moving forward.[8]

---

[7] Shea, 6.

[8] Donald S. Fredrickson, "Asilomar and Recombinant DNA: The End of the Beginning" *Biomedical Politics* (Washington, DC: National Academy Press, 1991), 258-298; Donald S. Fredrickson *The Recombinant DNA Controversy, A Memoir: Science, Politics, and the Public Interest 1974-1984* (Washington, D.C.: ASM Press, 2001).

Asilomar conference participants drafted a consensus statement that called for a voluntary moratorium on certain aspects of recombinant research and an increase in personal security and containment requirements for related research areas. This consensus statement was the starting point for the rules developed by the National Institutes of Health's (NIH) Recombinant DNA Advisory Committee (RAC), which was formed to oversee such research.[9] The RAC and its decentralized Institutional Biosafety Committees have remained the basis for oversight regarding the safe conduct of recombinant DNA research within the United States and have served as a model used by nations around the world to regulate the creation of genetically modified organisms.[10]

In the early 1980's, concern that the ability of foreign students and scientists to access fundamental information across a wide breadth of scientific disciplines, including information that might be considered to fall under export control regulations, led to an effort by the DOD to restrict information presented in classrooms and conferences. To better understand the potential for open scientific communication to negatively impact national security by supporting foreign weapons programs, the DOD helped fund a study through the NAS. The NAS convened a panel of leading researchers to address this difficult policy issue in which "recent trends, including apparent increases in acquisition efforts by our adversaries, have raised serious concerns that openness may harm U.S. security by providing adversaries with militarily relevant technologies that can be directed against us."[11]

---

[9] Shea, 6.

[10] R. M. Atlas, "Public Health. National Security and the Biological Research Community," *Science* 298, no. 5594 (25 Oct 2002): 753-754.

[11] Frank Press, *Scientific Communication and National Security* (Washington, DC: National Academy Press, 1982), v.

The NAS-funded panel provided an extensive report that described a set of principles intended to "resolve the current dilemma."[12] Overall, the panel found that the potential for restrictive controls to weaken US security, military, and economic development by hampering our scientific advancement outweighed the benefit of not supporting the military programs of our strategic adversary. Upon reviewing scientific activities and fields, the panel identified three categories of information:

- Activities and findings in which the benefits of total openness overshadow their possible near-term military benefits to the Soviet Union.
- Areas of research for which classification is clearly indicated.
- Small "gray" area that lies between the first two and for which limited restrictions short of classification are appropriate.[13]

Furthermore, the panel provided a general series of guidelines to assist the federal government in categorizing research activities. According to the panel:

> No restriction of any kind limiting access or communication should be applied to any area of university research, be it basic or applied, unless it involves a technology meeting <u>all</u> the following criteria:
>
> - The technology is developing rapidly and the time from basic science to application is short;
> - The technology has identifiable direct military applications; or it is dual-use and involves process or production-related techniques;
> - Transfer of the technology would give the USSR a significant near-term military benefit; and

[12] NAS Panel on Scientific Communication and National Security, *Scientific Communication and National Security* (Washington, DC: National Academy Press, 1982), v.

[13] NAS Panel, *Scientific Communication and National Security,* 4.

- The US is the only source of information about the technology, or other friendly nations that could also be a source have control systems as secure as ours.[14]

The panel suggested that in dealing with technologies and research in the "grey" areas that receive federal funding, the government could ensure sufficient security by restricting the access of foreign students and researchers to the laboratory undertaking the research and stipulating a policy of federal review of research manuscripts and other products prior to publication or open dissemination. The panel's findings appeared to provide sufficient guidance for the federal government at the time to adequately address the underlying issue regarding Soviet acquisition of dual use technologies with military applications. The panel appropriately recommended that the federal government take the lead in implementing these suggestions, but stressed the critical need for partnership between the scientific and national security communities to ensure effective and appropriate implementation.

Following the findings of the NAS panel, President Ronald Reagan issued National Security Decision Directive 189 (NSDD 189), which reaffirmed standing U.S. policy regarding the flow of scientific information:

> It is the policy of this administration that, to the maximum extent possible, the products of fundamental research remain unrestricted. It is also the policy of this Administration that, where the national security requires control, the mechanism for control of information generated during federally-funded fundamental research in science, engineering, technology and engineering at colleges, universities and laboratories is classification. Each federal government agency is responsible for: a) determining whether classification is appropriate prior to the award of a research grant, contract, or cooperative agreement and, if so, controlling the research results through standard classification procedures; b) periodically reviewing all research grants, contracts, or cooperative agreements for potential classification. No restrictions may be placed upon the conduct or

[14] NAS Panel, *Scientific Communication and National Security*, 5.

> reporting of federally-funded fundamental research that has not received national security classification, except as provided in applicable U.S. statutes.[15]

NSDD-189 has not been superceded and remains the federal policy regarding controls on federally-funded research.[16] However, throughout the late 1980s and early 1990s, a handful of individuals have raised the possibility of increasing security by compartmentalizing research of concern. According to Raymond Zilinskas, "compartmentalization, a less restrictive form of secrecy, allows scientists to exchange data only if they can establish that their colleagues need the data to proceed with their research."[17] Although there was not much discussion regarding the feasibility of compartmentalization to protect dual-use research findings, this may be due to the fact that at that time neither the national security community, life science research community, nor the general public was particularly concerned about the issue.

Ultimately, although the Asilomar conference, NAS panel, and subsequent infrequent discussions of the 1970s-1990s provided some helpful insights and historic perspective for participants in the current debate, the efficacy of their proposed resolutions must be considered in a broader context and assessed through the kaleidoscope of history. In general, the recommendations and findings of these groups may have largely been superceded by events that have occurred during the period leading up to late 2001 or by the consideration of circumstances that did not apply to the narrow focus of prior discussions. For example:

---

[15] White House, Office of the President, National Security Decision Directive-189, 1985.

[16] B. Vastag, "Openness in Biomedical Research Collides with Heightened Security Concerns," *Journal of the American Medical Association* 289 (12 Feb 2003): 686, 689-90.

[17] R. A. Zilinskas and T. Wilson, "The Microbiologist and Biological Defense Research. Ethics, Politics, and International Security. Introduction," *Annals of the New York Academy of Sciences* 666 (31 Dec 1992): xi-xvii.

- Although researchers at Asilomar were able to assuage public concerns at the time through their consensus statement and subsequent work within the NIH, the central tenet of the conference's recommendations relied upon personal integrity and accountability to not misuse genetic engineering technology acquired through scientific exchange. Such agreements have not dissuaded the nefarious researcher; indeed, information regarding the former Soviet bioweapons program reveals a concerted effort to incorporate genetic engineering technology to enhance biowarfare threat agents.[18]

- Close analysis of the subtext of the 1982 NAS panel report on scientific communication and national security reveals that the panel was principally concerned with sciences and technologies other than the life sciences. The ability to quantitatively assess the time from basic observation to bioweapons application is inversely proportionate to the pace at which life science discovery is proceeding. Thus, discussions related to performing security assessments of life science findings need to consider the fact that their technological applicability is not as clearly defined as in many of the physical sciences.

- The NAS panel report focused exclusively on the potential for U.S. research to support U.S.S.R. militarization. The panel itself acknowledged the limitations of their recommendations: "there are clear problems in scientific communication and national security involving Third World countries. These problems in time might overshadow the Soviet dimension."[19] Clearly, U.S. national security priorities have moved beyond a singular focus against a monolithic adversary and now are focused on addressing a variety of relatively smaller threats from developing nations and rogue states.

In light of these observations and current threats to U.S. national security, revisiting the findings of the 1982 panel would be prudent.

[18] Kenneth Alibek, *Biohazard: The Chilling True Story of the Largest Biological Weapons Program in the World* (New York: Random House Inc, 1999); Igor Domaradskij and W. Orent, *Biowarrior: Inside the Soviet/Russian Biological War Machine* (Amherst, NY: Prometheus Books, 2003).

[19] NAS Panel, *Scientific Communication and National Security*, 7.

RESURRECTION OF THE LIFE SCIENCE/SECURITY DEBATE

Al-Qaida's attacks upon the World Trade Center and the Pentagon on September 11, 2001 fully indoctrinated the U.S.'s collective consciousness to the threats of the 21st century, resulting in a national homeland security initiative that may yet overshadow that of the World War II era. The subsequent mailing of envelopes containing anthrax refined into a highly aerosolizable powder in October 2001 indisputably demonstrated the U.S.'s vulnerability to bioterrorism. These two events, amplified in part by media sensationalism, established a public psyche sensitized to terrorism and a collective will to identify and address perceived vulnerabilities. In response to public concerns, legislators and executors have pursued aggressive approaches to homeland security. Public response to date suggests that people may be willing to accept federal security regulations in exchange for heightened personal security, particularly where the topic of bioterrorism is concerned.

In this new environment of heightened awareness, threat estimation, and vulnerability assessments, legislators and executors have increased scrutiny of potential sources of support for terrorists, including the openness of the life science research community. For example, in an effort to curb the flow of information that may be of high value to bioterrorists, the DOD drafted a report "Mandatory Procedures for Research and Technology Protection within the DOD," which outlined its plans to provide DOD program managers greater oversight regarding whether DOD-funded laboratories could publish some of their findings.[20] This proposal was met with harsh criticism from the scientific community and was eventually discarded.

In addition to the DOD, the NIH and Congress implemented new restrictions on federally-funded life science research laboratories that were targeted to mitigate the potential for bioterrorists to have access to dual use technologies. The *Public Health Security and Bioterrorism Preparedness and Response Act* required tighter laboratory security, government registration, and background checks for scientists and others handling any of more than three dozen potential bioterror agents identified on the Center for Disease Control's (CDC) "Select Agent List."[21] In addition, agencies such as the NIH for the first time considered supporting classified research. Following implementation of these new regulations, scientists began to express concern over claims that some biologists with government funding were being encouraged to rein in the full publication of their own work.[22] Following similar developments in the UK, some scientists became very concerned that the level of response may be disproportionate to the actual threat.[23]

Growing tension between some leading researchers and the federal government continued to escalate throughout the spring and summer of 2002, largely due to media reports that highlighted the dual use potential of a number of recent scientific publications. Examples include:

---

[20] David Malakoff, "National Security. Pentagon Proposal Worries Researchers," *Science* 296, no. 5569 (3 May 2002): 826.

[21] David Malakoff, "Bioterrorism. Congress Adopts Tough Rules for Labs," *Science* 296, no. 5573 (31 May 2002): 1585-87.

[22] Erika Check, "Biologists Apprehensive over US Moves to Censor Information Flow," *Nature* 415, no. 6874 (21 Feb 2002): 821.

[23] M. McCarthy and S. Ramsay, "Fears that Security Rules will Impede US and UK Science," *Lancet* 359, no. 9307 (2002 Feb 23): 679.

- In 2000, Australian researchers genetically engineered a strain of mousepox virus in a manner that inadvertently increased its virulence.[24] At the time, publication of their findings was met with harsh criticism.[25] This mousepox research and associated criticism were raised again in 2002 during additional debates on science and security.

- In July 2002, Researchers at the State University of New York at Stony Brook revealed their success at creating infectious poliovirus from artificially engineered DNA sequences.[26] Open publication of this article in the journal *Science* was viewed as enabling the proliferation of a methodology with high bioweapons potential.[27]

- Researchers at the University of Pittsburgh identified key proteins in Variola (smallpox) that contribute to the virus' virulence and demonstrated how to synthesize the virulence gene via genetic modification of smallpox's less deadly cousin *Vaccinia*.[28] The published report was the subject of a highly publicized news article that questioned the value of publishing discoveries that might aid bioterrorists.[29]

- Researchers at the University of Pennsylvania successfully developed a hybrid virus composed of an HIV core surrounded by the surface proteins of Ebola.[30] This new virus was capable of infecting lung tissue, potentially enabling aerosol delivery, and could facilitate the expression of foreign genes in infected cells. The published findings arguably provided a roadmap that nefarious researchers

---

[24] Ronald Jackson, and others, "Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox," *Journal of Virology* 75 (2001): 1205-1210.

[25] Joan Stephenson, "Biowarfare Warning," *Journal of the American Medical Association* 285, no. 6 (2001): 725.

[26] Jeronimo Cello, Aniko V. Paul, and Eckard Wimmer, "Chemical Synthesis of Poliovirus cDNA: Generation of Infectious Virus in the Absence of Natural Template," *Science* 297 (9 Aug 2002): 1016-1018.

[27] Rick Weiss, "Polio-Causing Virus Created in N.Y. Lab: Made-from-Scratch Pathogen Prompts Concerns about Bioethics, Terrorism," *The Washington Post,* 12 Jul 2002.

[28] Ariella M. Rosengard, Yu Liu, Zhiping Nie, and Robert Jimenez, "Variola Virus Immune Evasion Design: Expression of a Highly Efficient Inhibitor of Human Complement," *Proceedings of the National Academies of Sciences of the United States of America* 99 (25 Jun 2002): 8808-13.

[29] N. Boyce, "Speak No Evil: Should Biologists Publish Work that could be Misused?" *US News and World Report*, 24 Jun 2002.

[30] G. P. Kobinger, D. J. Weiner, Q. C. Yu, and J. M. Wilson, "Filovirus-Pseudotyped Lentiviral Vector Can Efficiently and Stably Transduce Airway Epithelia in Vivo," *Nature Biotechnology* 19, no. 3 (Mar 2001): 225-30.

could exploit to engineer a viral vector capable of efficiently delivering bioregulatory agents.

- Researchers in Germany published the creation of a DNA-based system for performing reverse genetics studies on the Ebola virus.[31] This system introduced the possibility of reconstituting live Ebola virus from DNA in the absence of a viral sample. Other researchers expressed concern that this information could lead to the artificial synthesis of the virus, increasing the potential for agent proliferation as DNA can be more safely transferred than viral samples.[32]

Dana Shea at the Library of Congress has nicely assessed the overall response: "these articles have led some to question the wisdom of openly publishing information that could be used to threaten national security."[33] An editorial in New Scientist stated that "this mind-boggling quantity of information is going to transform medicine and biology is beyond doubt. But could some of it, in the wrong hands, be a recipe for terror and mayhem?"[34] Maybe so. Bioethicist Arthur Kaplan from the University of Pennsylvania was reported as saying "we have to get away from the ethos that knowledge is good, knowledge should be publicly available, that information will liberate us. Information will kill us in the techno-terrorist age, and I think it's nuts to put that stuff on websites."[35]

Apparently, a number of members of Congress agreed with Kaplan. Following the variety of press reporting regarding the prevalence of dual use information being

[31] Victor Volchkov, and others, "Recovery of Infectious Ebola Virus from Complementary DNA: RNA Editing of the GP Gene and Viral Cytotoxicity," *Science* 291, no.5510 (9 Mar 2001): 1965-69.

[32] Sylvia Pagan Westphal, "Ebola Virus Could be Synthesized," *New Scientist*, 17 Jul 2002.

[33] Shea, 5.

[34] "Surfing for a Satan Bug. Why are we Making Life so Easy for would-be Terrorists?" *New Scientist*, 20 Jul 2002, 5.

[35] Eric Lichtblau, "Response to Terror; Rising Fears that What We do Know Can Hurt Us," *Los Angeles Times,* 18 Nov 2001, A1.

reported in scientific journals, a handful of members of Congress filed a resolution that criticized *Science's* publication of the synthetic creation of a poliovirus and called on journals, scientists, and funding agencies to exercise greater caution before releasing such information. The resolution was introduced by Representative Dave Weldon (R-FL) who, along with seven other congressmen, criticized *Science*'s publisher, the American Association for the Advancement of Science (AAAS) for publishing "a blueprint that could conceivably enable terrorists to inexpensively create human pathogens."[36] Weldon's resolution called on the executive branch to review current policies and ensure that information that could be useful to in the development of chemical, biological, or nuclear weapons is not made accessible to terrorists or countries of proliferation concern.[37]

In addition to Congressional interest, the Office for Homeland Security (OHS) announced that it would be considering initiatives to create a category of information that would be "sensitive, but unclassified" for application to a variety of dual-use topics, possibly including life science research of concern.[38] This naturally raised the levels of suspicion and concern among researchers that OHS might seek to make decisions that in their opinion would be more appropriately adjudicated by the National Institutes of Health (NIH).[39] Separately, the American Society for Microbiology (ASM) sent a letter to the National Academy of Sciences (NAS) requesting a meeting of biomedical publishers to discuss whether and how editors of leading research journals should publish

---

[36] J. Couzin, "A Call for Restraint on Biological Data," *Science* 297, 5582 (2 Aug 2002): 749-51.

[37] H.R. 514, 107th Congress.

[38] E. Check, "US Prepares Ground for Security Clampdown," *Nature* 418, no. 6901 (2002): 906.

[39] G. Brumfiel, "Mission Impossible?" *Nature* 419, no. 6902 (2002): 10-11.

research that might be co-opted by terrorists.[40] By fall 2002, the debate on scientific openness and national security had officially been reopened.

THE CURRENT DEBATE

As the federal government initiated its informal efforts to develop a strategy for addressing the issue of science and security in late 2002, insights were being offered from a variety of highly knowledgeable sources. Mitchel Wallerstein, former Deputy Assistant Secretary of Defense for Counterproliferation Policy proffered some guiding principles for the scientific community and federal government:

- First, open access to scientific knowledge on university campuses remains as important as it was twenty years ago;
- Second, the areas of scientific knowledge and/or technological application that are immediately applicable to the development of weapons of mass destruction (WMD) are already known;
- Third, carefully conceived restrictions on scientific and technical communications remain necessary but should be applied to substantially fewer areas of scientific inquiry and technology development than during the Cold War;
- Fourth, university faculties have a responsibility for imparting values that emphasize the positive role of S&T in addressing human needs, and the immorality of their use to cause mass casualties and human suffering.[41]

Wallerstein's first, third, and fourth recommendations may provide a good roadmap to address many underlying concerns. However, it may be a bit presumptive to assume that

[40] Couzin, 51.

[41] Mitchell B. Wallerstein, "Science in an Age of Terrorism," *Science* 297, no. 5590 (27 Sep 2002): 2169.

all "areas of scientific knowledge and/or technological application that are immediately applicable to the development of weapons of mass destruction (WMD) are already known." The central issue of exponential discovery in the fields of life sciences and their potential implications for a revolution in BW fundamentally requires a continuing reevaluation and identification of research disciplines with application to BW and biodefense.[42] Ideally, such evaluations should include insights from leading life science researchers actively engaged in "cutting edge" science as they will have the clearest insights regarding the technical capabilities and potential limitations of biotechnologies for nefarious use.

Partially in response to media frenzy surrounding the Congressional resolution, on 18 October, 2002, the NAS outlined its recommendations for addressing the issue in its "Background Paper on Science and Security in an Age of Terrorism." In this paper, the NAS provided a series of action items for the life science research community and the federal government, citing the success of recent collaborations between the government and scientists:

> The nation must balance two needs for achieving a safe and secure society: 1) the need to restrict access to certain information, and 2) the need for a strong research enterprise that improves both our general welfare and our security. Clearly, policy-makers must seek mechanisms by which both interests can be served.
>
> To this end, we call for a renewed dialogue among scientists, engineers, health researchers, and policy-makers. To stimulate such a dialogue, we present two "action points": one focused on scientists, engineers, and health researchers and the other focused on policy-makers.
>
> <u>Action Point 1:</u> The scientific…community should work closely with the federal government to determine which research may be related to possible new security threats and to develop principles for researchers in each field.

---

[42] James Petro, Ted Plasse, and Jack McNulty, "Biotechnology: Impact on Biological Warfare and Biodefense," *Biosecurity and Bioterrorism* 1, no. 3 (2003): 161-68.

- Today, the chemical, biological, and even social science communities bear new responsibilities to identify materials and areas of research that should – or should not be – classified, and to provide assessments on the impact of classification on scientific, engineering, and health research.

- The science, engineering, and health community can also clarify the distinction between the basic research that yields fundamental new understanding and the technological developments that are required for weapons development.

Action Point 2: The federal government should affirm and maintain the general principle of National Security Decision Directive 189, issued in 1985.

- A successful balance…demands clarity in the distinctions between classified and unclassified research.

- We believe it to be essential that these distinctions not include poorly defined categories of "sensitive but unclassified" information that does not provide guidance on what kind of information should be restricted from public access.

- Even classified research, within its much smaller universe, must be confirmed through the participation of a community of outstanding science, engineering, and health researchers.[43]

Immediately following release of the NAS background paper, scientists issued their support for the highlighted principles, including their distaste for the concept of creating a category for "sensitive but unclassified" research. Ron Atlas, the president of ASM, testified before the House Science Committee that the government needs to clarify what constitutes a threat before it can implement protective guidelines, such as screening foreign graduate students for entry to U.S. laboratories.[44] Moreover, scientists argued that clear distinctions need to be made between classified and unclassified research since

[43] The National Academies of Science, *Background Paper on Science and Security in an Age of Terrorism* (Washington, DC: National Academy Press, 2003).

[44] David Malakoff, "Security and Science. Researchers See Progress in Finding the Right Balance," *Science* 298, 5593 (18 Oct 2002): 529.

"poorly defined third categories of sensitive but unclassified research that do not provide precise guidance on what information should be restricted from public access…generate deep uncertainties among both scientists and the officials responsible for enforcing regulations."[45]

This discussion raised concern that many scientists would either deal with the issue of classification by determining that it should be rejected from university laboratories as unsuitable (as was the case at the Massachusetts Institute of Technology) or deem the "sensitive" label as prone to too many interpretations to be accommodated in an academic setting.[46] Despite this, however, the NAS demonstrated its willingness to withhold certain information from general release to those who lack a demonstrated "need to know." This option came into play when the Academies agreed to remove an entire chapter of the 2002 NAS study on agricultural bioterrorism that the authors and the Department of Agriculture agreed would be of high dual use value to individuals with nefarious intentions.[47] Also, with some scientists, the concern over research classification was secondary to the potential consequences of misuse of their research. As one such researcher wrote, "scientists need to be aware of the regulatory and ethical implications of bioweapon proliferation."[48]

---

[45] B. Alberts, and R. M. May, "Scientist Support for Biological Weapons Controls," *Science* 298, no. 5596 (8 Nov 2002): 1135.

[46] D. S. Greenberg, "Homeland Security is Good and Bad News for US Scientists," *Lancet* 360, no. 9350 (28 Dec 2002): 2056.

[47] M. Enserink, "Science and Security. Entering the Twilight Zone of what material to Censor," *Science* 298, no. 5598 (22 Nov 2002): 1548.

[48] J. A. Singh, and P. A. Singer, "Isolationism is not the Answer to Bioterrorism," *Nature* 420, 6916 (12 Dec 2002): 605.

In addition to lobbying Congress and federal agencies regarding their concerns, biologists began to independently discuss new voluntary guidelines on publishing potentially dangerous information, in part to head off possible government rules.[49] On 9-10 January, 2003 the NAS and Center for Strategic and International Studies (CSIS) hosted a workshop for life science researchers and national security experts to discuss the issue of assessing and mitigating potential threats presented by biological research. Although many of the 200 senior scientists and researchers argued that scientists should be free to publish all unclassified work, some academicians acknowledged that the scientific community needs to reassure the public and the government that it is acting responsibly.[50]

Moreover, statements by senior policymakers appeared designed to reassure scientists, but challenged them to take the initiative. According to Dr. Parney Albright, then Associate Director of Homeland Security for the President's Office of Homeland Security, "it is the policy of this Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted" and that as per NSDD 189, "no restrictions will be placed upon the conduct or reporting of federally-funded fundamental research that has not received national security classification."[51] However, Dr. Albright did not give the research community a free pass, making it clear that "the science community ought to come up with a process before the public demands the government

---

[49] David Malakoff, "Security and Science. Researchers See Progress in Finding the Right Balance," *Science* 298, no. 5593 (18 Oct 2002): 529.

[50] Erika Check, "US Officials Urge Biologists to Vet Publications for Bioterror Risk," *Nature* 421, 6920 (16 Jan 2003): 197.

[51] B. Vastag, "Openness in Biomedical Research Collides with Heightened Security Concerns," *Journal of the American Medical Association* 289, no. 6 (12 Feb 2003): 686, 689-90.

do it for them…that will be driven by the rate at which controversial papers hit the street."[52]

Ultimately, scientists at the NAS/CSIS meeting agreed that there may be some research that should not be published, although clear guidelines would be helpful in identifying future papers of concern. To help craft a better definition of taboo science, the academies and CSIS announced their plan to convene future meetings of top science and security leaders. Gerald Epstein, a security expert with the Institute for Defense Analysis, proposed a simple question to aid scientists in deciding whether a paper should be more closely reviewed: "Would you like it to be found in a cave in Afghanistan with sections highlighted in yellow?"[53]

During the second day of the workshop, a group of editors from leading scientific journals crafted a consensus statement regarding the publication of research with potential for aiding bioterrorism.[54] An editorial that ran alongside the statement in *Science* highlighted the need for researchers, editors, and national security professionals to reach a consensus regarding guidelines for scientific information that should not be published. The editorial statement did not represent a radical departure from standing policy; rather it concisely stated the opinions of the editors present with regard to publishing information that might aid terrorists. The statement made four general points:

- First, the scientific information published in peer-reviewed journals carries special status, and confers unique responsibilities on editors and authors.

[52] Erika Check, "US Officials Urge Biologists to Vet Publications for Bioterror Risk," *Nature* 421, no. 6920 (16 Jan 2003): 197.

[53] David Malakoff, "Science and Security. Researchers Urged to Self-Censor Sensitive Data," *Science* 299, no. 5605 (17 Jan 2003): 321.

[54] Ronald Atlas, and others, "Statement on Scientific Publication and Security," *Science* 299, no. 5610 (21 Feb 2003): 1149.

- Second, the editors recognize that the prospect of bioterrorism has raised legitimate concerns about the potential misuse of published information, but also recognize that research in the very same fields will be critical to society in meeting the challenges of defense.

- Third, scientists and their journals should consider the appropriate level and design of processes to accomplish effective review of papers that raise such security issues.

- Fourth, on occasion an editor may conclude that the potential harm of publication outweighs the potential societal benefits.[55]

Despite the intentions of the editors to contribute a meaningful document, the joint statement received a mixed response from researchers and security experts.[56] Some researchers complained that they were not consulted on the publisher's statement.[57] For example, Steven Block, a biophysicist at Stanford University, was quoted as saying the statement is "more equivocal and less definitive" than he would like to see.[58] Others believe that scientists should go much further to address security concerns about life science research. David Heyman, a science and security expert at CSIS, says that the statement is "only a step" and that scientists should make changes earlier in the research process to reduce the risk of biological research being misused.[59]

By far the sharpest public critic of the statement, respected microbiologist Stanley Falkow has taken issue with the fact that the authors failed to elicit more extensive discussion on the statement before its publication. Falkow faults the authors for failing

[55] Ron Atlas, and others, "Statement on Scientific Publication and Security."

[56] Erika Check, "Journals Tighten up on Biosecurity," *Nature* 421, no. 6925 (20 Feb 2003): 774.

[57] Erika Check, "Biodefense Plans Earn Lukewarm Response from US Academics," *Nature* 422, no. 6929 (20 Mar 2003): 245-6.

[58] Check, "Journals Tighten up on Biosecurity."

[59] Check, "Journals Tighten up on Biosecurity."

"to provide guidelines regarding who exactly would make these decisions about publication and what constitutes a potential contribution to the activities of bioterrorists."[60] Falkow's statement suggests that he supports the formation of a committee designed to provide insight and oversight regarding research of concern. However, it is his opinion that the issue should be "earnestly discussed by the broad community of scientists, together with those whose mission it is to guard national security."[61]

In a further effort to characterize the challenges posed by misuse of biotechnology, the NAS created the Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology which was charged with considering ways to minimize threats from BW and bioterrorism without hindering the progress of biotechnology. The committee's report, *Biotechnology Research in an Age of Terrorism* (commonly referred to as the Fink report), released in October 2003, proposed a new system for mitigating the potential for life science knowledge to be misused by establishing "a number of stages at which experiments and eventually their results would be reviewed to provide reassurance that advances in biotechnology with potential applications for BW or bioterrorism receive responsible oversight."[62] The Fink report outlined seven specific recommendations for the scientific community to mitigate the

[60] Stanley Falkow, "Science Publishing and Security Concerns," *Science* 300, no. 5620 (20 May 2003): 737-9.

[61] Check, "Journals Tighten up on Biosecurity."

[62] Gerald Fink, and others, *Biotechnology Research in an Age of Terrorism* (Washington, D.C.: The National Academies Press, 2004), 3.

potential for misuse of dual use knowledge and seven general guidelines for identifying "research of concern."[63]

In the Fink report, the NAS committee members clearly identified the absence of an "established culture of working with the national security community among life scientists as currently exists in the fields of nuclear physics and cryptography"[64] as a challenge to achieving consensus regarding the identification of dual use information and mitigation of its potential misuse. As one of its seven overall recommendations, the committee called for a role for the life sciences in efforts to prevent bioterrorism and biowarfare, recommending that "the national security and law enforcement communities develop new channels of sustained communication with the life sciences community about how to mitigate the risks of bioterrorism."[65] The Fink report clearly suggested that leading scientists believe some guidance from intelligence professionals would assist the scientific community as it seeks to identify information that may be of use to terrorists and support comparative assessments regarding the cost-benefit ratio of limiting the availability of such information.

In response to the recommendations of the NAS Fink report, the Department of Health and Human Services recently announced the creation of a National Scientific Advisory Board for Biosecurity (NSABB).[66] According to the DHHS press statement, the NSABB will "advise the Secretary of HHS, the director of the NIH, and the heads of

[63] Fink, 111-26.

[64] Fink, 85.

[65] Fink, 123.

[66] DHHS Press release available at URL: <http: //www.biosecurityboard.gov/NSABB_press_release.pdf>.

all federal departments and agencies that conduct or support life sciences research" by "recommending specific strategies for the efficient and effective oversight of federally conducted or supported potential dual-use biological research taking into consideration both national security concerns and the needs of the research community."[67] According to the NSABB website, the group will be charged specifically with guiding the development of guidelines for the identification and conduct of research that may require special attention and security surveillance.[68] Although a general list of participants on the NSABB website identifies a role for representation from the intelligence community, how that role will be filled appears to remain undetermined.

NEED FOR INTELLIGENCE SUPPORT TO THE SCIENTIFIC COMMUNITY

The life science research community could benefit from insights of the intelligence community (IC) and other national security professionals if it is to progress beyond the current state of discussion and develop a coordinated strategy for assessing and mitigating threats enabled by research of concern. Engagement of the scientific community should be of paramount importance to biological warfare and CBRN terrorism analysts in the IC due to the impending potential for life science discoveries to impact the capabilities of nefarious actors.

In addition to obvious areas of contribution, such as providing key insight and methodologies for deriving threat assessments and offering national security insights

[67] DHHS, 1.

[68] NSABB website: URL: <http: //www.biosecurityboard.gov>.

while sitting on life science expert panels, there are many less obvious opportunities for IC input. For example, the IC is well positioned to help educate life science experts about the exploitation activities of terrorist groups and foreign states to support their BW efforts. Also, IC personnel possess access to a wealth of information on the physical properties and characteristics of biothreat agents. Much of this information – at least that which is unclassified or for official use only (FOUO) – would be useful to researchers struggling with the development of novel countermeasures and systems for civilian biodefense.

Developing a deeper relationship between the IC and life science community also holds potential to benefit the IC. Because the life science community possesses a wealth of world-class expertise regarding cutting-edge knowledge, closer partnerships with key life science researchers could yield significant dividends to the IC, which has long struggled to maintain an internal core of bioscience expertise. In addition, shaping a positive view among life science professionals of the IC may increase the number of top graduate students and young life science researchers who seek employment opportunities within intelligence or national security agencies. Furthermore, closer and continuing contact with life science investigators might yield occasional insight regarding suspicious attempts by unknown researchers to acquire information, reagents, or technology of high dual use value from legitimate scientists. Such insights could enable further targeting of IC resources. There is high potential for synergy between the two communities; however, the intelligence and national security communities will need to take the first step in engaging life scientists. Ultimately, none of the potential benefits will be realized until long after IC professionals have sown seeds of goodwill within the life science research community and engaged influential scientists as partners on BW counterproliferation initiatives.

CHAPTER 2

BIOTECHNOLOGY: IMPACT UPON BIOLOGICAL WARFARE AND BIODEFENSE

INTRODUCTION

Advances in biological research likely will permit development of a new class of advanced biological warfare (ABW) agents engineered to elicit novel effects. In addition, biotechnology will have applications supporting ABW weaponization, dissemination, and delivery. Such new agents and delivery systems would provide a variety of new use options, expanding the BW paradigm. Although ABW agents will not replace threats posed by traditional biological agents such as *Bacillus anthracis* (anthrax) and *Variola* (smallpox) in the near term, they will necessitate novel approaches to counterproliferation, detection, medical countermeasures and attribution.

The concept of employing disease as a weapon has existed for centuries. The low cost, minimal barriers to acquisition, and potential impact of biological agents as weapons have influenced a number of countries to pursue biological warfare (BW) throughout the 20th century.[69] International agreements, such as the Biological Weapons and Toxins Convention (BWC), have arguably done little to deter foreign BW programs; ironically, information regarding the former Soviet Union[70] suggests that such programs

[69] Thomas Mangold and Jeff Goldberg, *Plague Wars: The Terrifying Reality of Biological Warfare* (New York, New York: St. Martin's Press, 1999), 335-51.

[70] Alibek, *Biohazard*.

reached new heights of sophistication following ratification of the Convention. This is due in part to the ease with which BW programs can be concealed within legitimate research. Thus, it is logical to expect states that seek to acquire weapons of mass destruction will continue to pursue BW.

The threat that BW proliferation poses to civilian and military populations is compounded by the possibility that terrorist organizations may either acquire these weapons, indirectly or serendipitously, from national programs or develop their own intrinsic BW capability. This bioterror threat represents a significant challenge to organizations and agencies responsible for directing biodefense efforts. To date, most discussions regarding the creation of a national biodefense strategy have focused largely on addressing existing threats posed by a select group of naturally occurring pathogens and toxins. Although agents traditionally associated with BW likely will remain the predominant threat over the next 10 years, implications of current and emerging biotechnologies upon development of novel BW agents should also be considered and factored into any long-term biodefense strategy.

Biotechnology has the potential to revolutionize concepts underlying development, weaponization, and limitations of biological agents. It is now possible to build upon previous reports devoted to communicating biological threats posed by molecular biology[71] by identifying key technologies that could support efforts to engineer

[71] Gigi Kwik, and others, "Biosecurity: Responsible Stewardship of Bioscience in an Age of Catastrophic Terrorism," *Biosecurity and Bioterrorism* 1, no. 1 (2003): 27-35; George Poste, "Facing Reality in Preparing for Biological Warfare: a Conversation with George Poste. Interview by Jeff Goldsmith," *Health Affairs* (Millwood); Supp Web Exclusives (2002): W219-28; Claire Fraser and Malcolm Dando, "Genomics and Future Biological Weapons: the Need for Preventive Action by the Biomedical Community," *Nature Genetics* 29, no. 3 (2001): 253-6; Steven Block, "Living Nightmares: Biological Threats Enabled by Molecular Biology," in S. Drell, and others, eds, *The New Terror* (Stanford, CA: Hoover Institute Press, 1999), 39-75.

novel BW agents. Such estimations will require close cooperation among leading intelligence and security professionals and highly respected scientists from the life science research community, and preclude extensive technical discussions here. Rather, this chapter will focus on how biotechnology, when applied to BW, holds promise to challenge biodefense efforts targeted to counter threats presented by traditional agents, including counterproliferation, detection, and development of medical countermeasures. Ultimately, in order to be well situated to meet future challenges, some resources in all areas of biodefense will need to be diverted toward development of next-generation approaches sufficient to counter emerging threats. The intelligence and security professional will play an important role in guiding the civilian scientific and biodefense communities regarding the nature and scope of such threats.

TRADITIONAL AND GENETICALLY MODIFIED BW AGENTS

Historically, BW agents of concern have included a relatively select group of pathogens and toxins, referred to as traditional BW agents. Traditional BW agents are all naturally occurring organisms or their toxic products. From the perspective of a BW scientist, traditional BW agents have serendipitously evolved a select group of traits: toxicity, stability, and ease of production. However, until recent decades, the serendipity that aided researchers in choosing select organisms also limited BW applications to the characteristics of available agents. For example, environmental stability, infectious dose, time to effect, clinical progression, and lethality are all properties intrinsic to candidate traditional agents that may limit their utility for BW. Although researchers have identified general processes for the selection of subpopulations of microorganisms that may develop enhanced traits through naturally occurring mutations, the ability of such strategies to evoke radical alterations in organism function remains limited.

With the advent of recombinant DNA technology, researchers have developed standard methodologies for altering an organism's genetic makeup. Application of this technology to enhance traditional BW agents has led to the classification of genetically modified BW agents as a separate category of BW agents. Examples of potential modifications include antibiotic resistance, increased aerosol stability, or heightened pathogenesis. Importantly, genetic modifications may alter epitopes or sequences used for detection and diagnostics, necessitating that multiple points of reference be incorporated into these systems and highlighting the need for security regarding biodetection strategies. However, genetically modified BW agents will remain closely related to the parent agent at the genetic level and should be generally identifiable using traditional diagnostics. Ultimately, these modifications serve to increase effectiveness of a traditional BW agent or counteract known aspects of the target population's biomedical defense strategy without significantly manipulating the parental organism in a manner that might compromise natural properties suitable for BW use.

ADVANCED BW (ABW) AGENTS

Technologies developed across multiple disciplines in the biological sciences will have a profound global impact and concurrently have the potential to revolutionize BW by facilitating an entirely new class of fully engineered agents referred to as advanced

BW (ABW) agents. Emerging biotechnologies likely will lead to a paradigm shift in BW agent development; future biological agents could be intelligently engineered to target specific human biological systems at the molecular level. This is a departure from the traditional model of BW agent development, which is focused on the naturally occurring agent, not the target organism. Biological science trends hold promise to change this, allowing BW agent developers to identify biochemical pathways critical for physiological processes and engineer specific ABW agents to exploit vulnerabilities. These future developments do not mitigate threats from traditional BW agents; as described earlier, advances in biology already hold promise to improve traditional agents.

Applying discoveries made by emerging biotechnologies to BW likely will parallel the biological sciences by creating a biological systems-based approach to agent development. Systems-based models derived from integration of data obtained through genomic and proteomic observations will be critical components of this approach.[72] Advanced BW agents will be able to target specific biological systems, such as the cardiovascular, immunological, neurological, and gastrointestinal systems. Using an ever-increasing information base, BW designers of the future will have the capability to engineer agents that target biological processes, producing a wide range of effects including death, incapacitation, or neurological impairment. Not only will advances in biotechnology facilitate novel agents engineered to attack human systems, they will increasingly permit modification of existing agricultural pathogens and development of new anti-agricultural and anti-material BW agents. The effect that biotechnology may

[72] Leroy Hood, "Systems Biology: Integrating Technology, Biology and Computation," *Mechanical Ageing Development* 124, no. 1 (2003): 9-16.

have upon BW threats facing both military and civilian populations is graphically represented in Figure 1.

The threat presented by traditional agents has been increasing since the early 20th century but eventually will level off due to two major factors: 1) development of targeted medical countermeasures will reduce threats posed by current BW agents and 2) the number of natural pathogens and toxins that contain properties suitable for BW is finite.

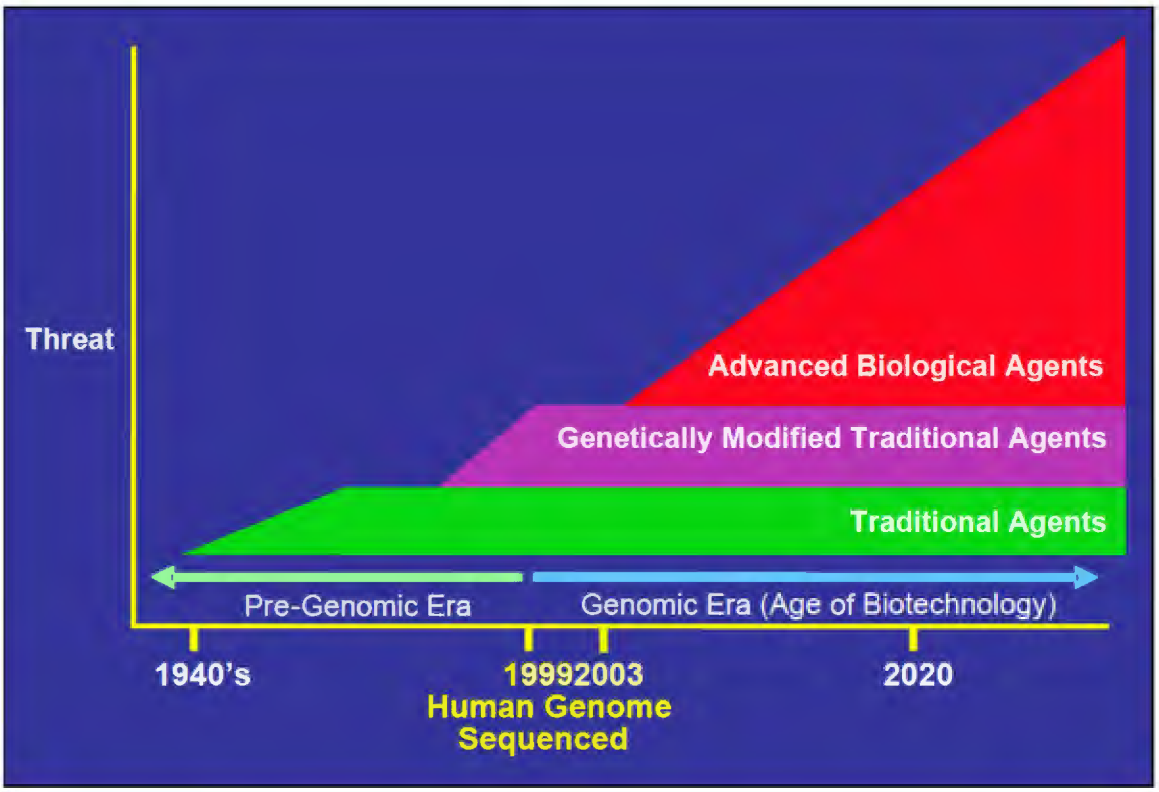

Figure 1. Timeline Describing Impact of Biotechnology on Biological Warfare Threat.

This timeline depicts the relative threat level presented by traditional (e.g., naturally occurring bacterial, viral agents), genetically modified traditional (e.g., antibiotic-resistant bacteria) and advanced biological agents (rationally-engineered BW agents artificially created using biotechnological applications).

Like traditional agents, the threat posed by genetically modified traditional agents eventually will plateau partly because ultimately, only a finite number of properties and genetic modifications can be used to enhance a traditional agent without altering it beyond the point that it could be recognized as the parental strain or serotype. Importantly, the large, yet finite, number of potential genetic modifications may well represent a multiplicative threat compared with that posed by the traditional agents, thus the width of the threat bars are not fully to scale. Unlike threats posed by traditional and genetically modified traditional agents, the capability-based threat posed by ABW agents will continue to expand indefinitely in parallel with advances in biotechnology.

IMPLICATIONS FOR DOWNSTREAM BW PROCESSES

Production

Biotechnological advances already have revolutionized many processes associated with bacterial and viral production as well as purification of proteins from bioprocess systems. Many of these newer approaches are specifically designed to decrease the technical expertise necessary to produce quantities of biological agents that would be sufficient for a group with nefarious intentions. Application of these technologies toward production of BW agents may lead to increased yield of high-quality product from decreased resources, greater consistency among product batches and marginal requirements for "cutting-edge" expertise. Importantly, this shift also may radically alter signatures that intelligence analysts and law enforcement professionals use to identify proscribed activity. However, biotechnological advances have not been limited to enhancement of industrial mechanisms for agent production.

The ability to introduce foreign genes into animal and plant DNA in a manner that permits the targeted organism to produce new proteins not previously encoded in its genetic material may have future applications for BW. Transgenic systems have proved to be a relatively inexpensive way to produce large quantities of medically useful proteins. Recent examples of such animals include goats that secrete insulin or spider silk in their milk. Future applications of transgenics technology will be targeted toward development of transgenic plants and insects that produce a desired protein.[73] Much of this technology easily could be diverted toward nefarious ends.

Transgenic plants could be engineered to produce large quantities of bioregulatory or toxic proteins. The bioregulator/toxin proteins could either be purified from plant cells or used directly as a BW agent. Thus in the future, transgenic plants might serve as bioproduction reactors, eliminating the need for standard mechanical equipment normally associated with this process. This method would primarily be limited to the production of protein-based BW agents, such as toxins or bioregulators; however, it would provide a covert mechanism to produce large quantities of such agents as a field of transgenic plants might be indistinguishable from non-transgenic crops.

Transgenic insects, such as bees, wasps, or mosquitoes, could be developed to produce and deliver protein-based BW agents. By employing future discoveries related to insect ontogeny and genetic manipulation, a mosquito potentially could be genetically altered to produce and secrete a highly potent bioregulator or toxin protein in its saliva. The insect would then intoxicate people with the protein by inoculation during its feeding

[73] E. James and J. M. Lee, "The Production of Foreign Proteins from Genetically Modified Plant Cells," *Advances in Biochemical Engineering and Biotechnology* 72 (2001): 127-56; J. M. Crampton, and others, "Model Systems to Evaluate the Use of Transgenic Haematophagous Insects to Deliver Protective Vaccines" *Parassitologia* 41, nos. 1-3 (1999): 473-77.

process. Because many bioregulators and toxins are thought to be effective at exceedingly low doses, an individual may succumb to infection after having been bitten by a few transgenic mosquitoes. Development and employment of genetically engineered insects for this purpose could have ecological implications that may favor offensive use against targets in a foreign country and not as a defense against invading military forces in a domestic theater of operations.

Weaponization

Research related to the use of nanoparticles in the storage and delivery of pharmaceuticals and vaccines will yield findings with direct application for improved weaponzation and storage of BW agents. Currently, microencapsulation technology is focused on development of processes to encapsulate biologically active organisms, proteins, and even DNA within a coating nanoparticle substance. Encapsulated products would be protected from environmental hazards, increasing their capacity for storage and survival. In addition, some research on microencapsulation technology is designed to increase the ability of bioproducts to be disseminated as an aerosol.[74] All of these features are indirectly applicable to BW agent weaponization, storage, and dissemination.

In addition to microencapsulation of bioproducts using microscopic particles, extensive research is being performed to dissect genetic and molecular mechanisms that regulate biofilm formation.[75] Biofilms are colonies of bacteria encased in secreted

[74] T. Kissel, and others, "Microencapsulation of Antigens Using Biodegradable Polyesters: Facts and Phantasies," *Behring Institute Mittation* 98 (1997): 172-83; T. E. Greenway, and others, "Induction of Protective Immune Responses against Venezuelan Equine Encephalitis (VEE) Virus Aerosol Challenge with Microencapsulated VEE Virus Vaccine," *Vaccine* 16, no. 13 (1998): 1314-23.

[75] C. Stephens, "Microbiology: Breaking Down Biofilms," *Current Biology* 12, no. 4 (19 Feb 2002): R132-34; M. E. Shirtliff, J. T. Mader, and A. K. Camper, "Molecular Interactions in Biofilms," *Chemistry Biology* 9, no. 8 (2002): 859-71.

exopolysachharides (complex sugars) that adhere to each other and a solid surface. Complex sugars produced by bacteria not only contribute to biofilm generation, but also protect the colony from environmental hazards and may even play a role in aiding bacteria to avoid the host immune system. Discoveries in this field might one day be diverted toward enhanced storage and delivery of bacterial BW agents.

Delivery

A systems approach to the creation of novel BW agents likely will occur concurrently with development of more advanced methods for agent delivery. Because ABW agents will be targeted against specific biochemical pathways, the effective dose likely will be reduced compared with that of traditional BW agents, which is already very low. Thus, vectors (organisms or mechanisms to transmit a biological compound) that previously could not be utilized for BW now would become potential delivery vehicles due to the reduced amount of ABW agent required to elicit a desired effect. Use of a vector, particularly viral vectors, to carry and express foreign genes could permit targeted delivery of nucleic acid-based BW agents. Engineered viral vectors hold potential to ensure successful delivery of genetic material with exquisite specificity to a targeted cell type.[76] In addition, development of alternate strategies for agent delivery including lipid-based[77] and other non-colloidal vectors[78] also has potential for delivery of foreign genes,

[76] W. S. Hu, and V. K. Pathak, "Design of Retroviral Vectors and Helper Cells for Gene Therapy," *Pharmacology Reviews* 52, no. 4 (2000): 493-511.

[77] N. M. Wassef, C. R. Alving, and R.L. Richards, "Liposomes as Carriers for Vaccines," *Immunomethods* 4, no. 3 (1994): 217-22.

[78] C. Uherek, and W. Wels, "DNA-carrier Proteins for Targeted Gene Delivery," *Advances in Drug Delivery Reviews* 44, nos. 2-3 (15 Nov 2000): 153-66.

albeit with a significant reduction in specificity. The ultimate expression of this technology would be development of a vector that encapsulates, protects, penetrates, and releases DNA-based BW agents into target cells but is not recognized by the immune system. Such a "stealth" agent would significantly challenge current medical countermeasure strategies.[79]

NEW BW USE OPTIONS

The wide range of effects that can be designed into ABW agents will expand options for employment significantly and ultimately may decrease the current threshold for use of BW. Among these new use options, for example, would be the opportunity to covertly target a civilian population for strategic effect with minimal risk of attribution. Other properties favoring development of ABW agents may include:

- Customizable aspects of advanced agent development allows for predictable, desired results following agent release.
- Unusual clinical presentation could allow a BW attack to be mischaracterized as a natural outbreak and remain unattributed or undetected as an unnatural event.
- Development of novel agents previously unknown to the medical community would yield BW agents that are difficult to diagnose and treat.
- Advanced agents could circumvent vaccines or treatments designed to counter traditional agents.
- Agents could be tailored to target a specific population based upon cultural or genetic traits. For example, cultural activities or behaviors associated with a specific target population could be exploited for greatest efficiency of agent delivery. Alternately, as polymorphic differences in genetic material among varying populations of individuals are discerned, it may become possible to

[79] Block, 39-75.

engineer a microorganism to specifically target a subpopulation based upon the presence or absence of a specific genetic marker.

- Creation of sterilizing, oncogenic (cancer causing), or debilitating agents for use as a strategic weapon against a target population for long-term effects.

When coupled with traditional motivations for pursuing BW as an asymmetric weapon (low cost-to-effect ratio, few technical barriers, force multiplier, etc.), these new use options likely will make BW more attractive. Thus, advances in biotechnology research may lead to a coming revolution in BW development for technologically proficient rogue nations and possibly sophisticated terrorist organizations.

CHALLENGES FOR BIODEFENSE

By supporting development of ABW agents, emerging biotechnologies will present novel challenges to biodefense strategies. Currently, concepts pertaining to biodefense are largely rooted in proven medical treatments and prophylactics. Although these strategies are critical to addressing immediate bio-threats, they will be inadequate against ABW agents. Thus, new initiatives designed to deal with broader threats that may result from misuse of technology need to be pursued in parallel with existing and planned programs. These initiatives must be tailored within each component of the national biodefense infrastructure.

Nonproliferation

Historically, nonproliferation efforts have been focused largely on monitoring foreign acquisition of weapons systems, “dual-use” biological production equipment, and a handful of biological agents. This approach appears to satisfactorily address primary concerns related to nations acquiring BW technology; however, information from defectors, such as the Iraqi WMD Chief Husayn Kamel,[80] reveal that states with even marginal technological proficiency are not deterred from pursuing traditional BW programs. Advances made possible through applied biotechnology, which portends a change in the information, equipment, expertise, and access to agents that can underlie BW programs in the future, will compound this problem. Thus, intelligence and domestic security professionals must supplement their current approach with novel relationships, collection methodologies, and analytic strategies that will be discussed in greater detail in Chapter IV.

Development of advanced BW agents and genetically modified traditional agents will be facilitated largely by availability of technical information from the Western scientific community. Foreign malefactors already have a variety of options for addressing their technological needs: openly published literature, freely accessible knowledge databases, interactions with unsuspecting researchers at symposia, and opportunities to have students trained on cutting-edge technologies in Western laboratories; these options will increase in the future. Unfortunately, the potential threat presented by proliferation of biotechnology information cannot be contained as easily as that presented by research in certain applications of nuclear fission; unlike much of the fission research, particularly that which is related to the development of nuclear weapons,

[80] John M. Deutch, Worldwide Threat Assessment Brief to the Senate Select Committee on Intelligence by the Director of Central Intelligence, John M. Deutch. 1996. Full text available at: URL: <http: //www.fas.org/irp/congress/1996_hr/s960222p.htm>; Raymond Zilinskas, "Iraq's Biological Weapons. The Past as Future?" *Journal of the American Medical Association* 278, no. 5 (6 Aug 1997): 418-24.

all biotechnology research builds upon previous findings across a variety of disciplines. Thus, restricting the spread of discoveries in the biological sciences may well impede progress in development of new therapeutics and vaccines, including those that will be essential to biodefense.

Intelligence and domestic security communities will need to engage the published literature head-on by establishing closer continuing relations with basic and applied bioscience research communities and developing systems to monitor access to questionable combinations of research findings. Also, where possible, the national security community will need to become more engaged in educating academic and industrial researchers regarding foreign exploitation efforts and developing and implementing approved mechanisms for communicating suspicious activity. Because the application of biotechnology toward development of novel agents will require detailed information that may provide a specific signature, identifying potential malefactors based on their information requirements might be possible. Additional nonproliferation efforts could then be targeted against individuals of concern.

In the future, biotechnology likely will impact the equipment and expertise that supports BW. Novel equipment and production strategies probably would alter signatures associated with BW activity, blending them with background signatures of legitimate research. Furthermore, decreasing technical barriers to engineering ABW agents through development of technical kits and detailed protocols for advanced laboratory techniques will reduce the need for highly trained scientists. Nonproliferation professionals will need to remain cognizant of equipment and techniques associated with cutting-edge biotechnologies with high dual-use potential and more carefully monitor foreign acquisition of those underlying technologies and capabilities. This will become increasingly difficult to do amidst a rapidly growing background of legitimate biotech research and manufacturing activities in many areas of the developing world. In addition, the national security community will need to factor in the effects of emerging technologies upon standard signatures associated with BW activities and adjust its strategies accordingly.

Most important, biotechnology will significantly impact global proliferation of agents of concern in a manner that will be difficult to regulate or monitor. Modern DNA sequencing technology permits absolute characterization of any organism's genetic material. To date, genomes of many organisms, including humans, fruit flies, nematodes, bacteria, and many viruses have been determined. All this information is stored in digital data files that are commonly accessible via a currently non-attributable manner over the Internet. Coupled with advances in DNA synthesis technology, it is becoming increasingly possible to reconstruct viruses from genomic digital data files, a process becoming increasingly recognized as "digital proliferation." The recent production of infectious poliovirus from synthetic DNA[81] is merely the tip of the iceberg when it comes to potential implications of this technology toward proliferation of agents of concern or, for that matter, gene sequences that can be assembled to create ABW agents. As the number of commercial DNA synthesis enterprises and prevalence of this technology in

[81] J. Cello, A. V. Paul, and E. Wimmer, "Chemical Synthesis of Poliovirus cDNA: Generation of Infectious Virus in the Absence of Natural Template," *Science* 297, no. 5583 (9 Aug 2002): 1016-18.

smaller laboratories increases, standard approaches to monitoring the spread and acquisition of organisms on the CDC select agent list will become less effective.

Environmental Detection

Currently, biodefense is challenged by the absence of real-time environmental detectors for biological agents of concern. Detection systems currently under development focus largely on detecting hazardous bioaerosols by size, antigen recognition, or nucleic acid sequence. Although a number of technical considerations must be addressed regarding sensitivity, selectivity, false positive rates, and methodology for use of these systems, they are based upon fundamental approaches that ultimately will permit detection of a select group of traditional BW threat agents. Unfortunately, the nature by which ABW agents are engineered automatically will permit them to circumvent systems currently under development to address threats posed by traditional agents. Thus, allocating a limited amount of resources toward development of more general detection strategies would be prudent.[82]

Systems are needed that profile a variety of physical characteristics likely to be incorporated into ABW agents, including gene sequences from humans and a variety of microorganisms not previously identified as high-threat agents. This will ensure detection of a wide range of pathogens, including both traditional and ABW agents. Ideally, these systems would integrate readouts of a variety of properties including particle size and nucleic acid profile. Because these detectors will need to recognize components from traditional and non-traditional threat organisms as well as some human

[82] Petro, 164.

gene sequences, elaborate pattern recognition software will be critical to distinguish the presence of threat agents from a large background of environmental contaminants and minimize false positives. Fortunately, bioscience discovery almost certainly will enable creation of such next-generation environmental detectors in the future. Once appropriate generalized detectors are available, their doctrine for use should be the same regardless the agent detected.

Medical Countermeasures

Advanced BW agents will pose the greatest challenge to development of appropriate medical countermeasures. Current strategies for medical diagnostics, prophylaxis, and therapeutics for BW agents may be inadequate to address emerging ABW threats. This is largely due to standard paradigms in basic and applied research that focus efforts to address individual agents based upon distinct physical attributes. Although this process yields countermeasures that protect against the intended organism, sometimes with exquisite specificity, the wheel must constantly be reinvented to apply underlying principles towards novel threat agents. In the coming environment where ABW agents can be engineered to circumvent standard medical countermeasures, there will be increasing need for research into novel strategies for protecting military and civilian populations from agents of unknown properties and origin.

Employment of ABW agents most likely would result in targeted individuals presenting with symptoms not normally associated with known traditional BW agents. Thus, it will be necessary to rapidly diagnose and identify underlying principles of the disease-causing agent. A number of potential approaches profile specific biochemical and molecular responses to infection with different organisms. For example, recent studies monitoring profiles of gene expression in immune system cells following exposure to a variety of microorganisms suggest that it may be possible to specifically identify an infectious agent based upon early stages of the immune response.[83] Also, the reemergence of mass spectrometry as a powerful tool for profiling a complete array of proteins and peptides in clinical samples[84] may hold promise for identifying components of infectious agents and potentially could serve to reveal whether an ABW is altering expression levels of bioregulatory genes. These strategies are still at the conceptual stage and would require additional resources to be adapted as diagnostic systems for biodefense. Ultimately, development of a generalized diagnostic system based upon searching for characteristic host responses among individuals potentially exposed to traditional or ABW agents would be a major step forward for biodefense.

The process for developing prophylaxis against traditional BW agents has yielded many effective vaccines; however, the current strategy of developing individual vaccines against distinct pathogens will not be capable of protecting against ABW agents. Thus, research into vaccines that confer a general increase in immune system activation should be pursued. Preliminary findings in a number of immunological laboratories suggest that classes of immune system cells are capable of responding with the potency of the adaptive immune system to a variety of pathogens recognized by the innate immune system based upon structural moieties (features of proteins) conserved among wide

[83] A. R. Whitney, and others, "Individuality and Variation in Gene Expression Patterns in Human Blood," *Proceedings of the National Academies of Sciences U S A* 100, no. 4 (18 Feb 2003): 1896-1901; C. A. Cummings and D. A. Relman, "Genomics and Microbiology. Microbial Forensics – 'Cross-Examining Pathogens'," *Science* 296, no. 5575 (14 Jun 2002): 1976-79.

[84] R. Aebersold, and M. Mann, "Mass Spectrometry-Based Proteomics," *Nature* 422, no. 6928 (13 Mar 2003): 198-207.

classes of pathogens.[85] Possibly, vaccines that stimulate these cells could be created, providing a more rapid immune response to a wide variety of bacterial and viral pathogens. In addition to developing standard vaccines, resources need to be directed toward study of these generalized vaccination strategies as well as the potential for immunomodulatory compounds that could boost immune responses following an attack with traditional or ABW agents. Naturally, studies into the potential negative effects of generalized immunomodulation, such as autoimmunity or hypersensitivity, will also need to be conducted.

Developing therapeutics to mitigate the effects of ABW agents will be a unique challenge. Currently, therapeutics are either engineered against specific molecular pathways or interactions critical for agent pathogenesis or identified through high-throughput screening of libraries of compounds until one with an inhibitory effect upon the targeted agent is identified and validated for further study. These approaches may remain viable for developing novel compounds to respond after a BW or bioterror attack has occurred. However, the major question regarding therapeutic development raised by the potential for ABW agents to integrate human bioregulatory genes or otherwise affect gene expression is "how does one treat an attack on the genome?" Preliminary studies designed to dissect the cellular pathways for RNA interference (RNAi)[86] and development of short hairpin RNA (shRNA) molecules[87] hold potential to address this

---

[85] R. Boismenu, W. L. Havran, "An Innate View of Gamma Delta T Cells," *Current Opinions in Immunology* 9, no. 1 (1997): 57-63; R. M. Crawford, and others, "Macrophage Activation: a Riddle of Immunological Resistance," *Immunology Seminars* 60 (1996): 29-46; M. C. Carroll, and A. P. Prodeus, "Linkages of Innate and Adaptive Immunity," *Current Opinions in Immunology* 10, no. 1 (1998): 36-40.

[86] G. L. Hannon, "RNA Interference," *Nature* 418, no. 6894 (11 Jul 2002): 244-51.

[87] P. J. Paddison, and others, "Short Hairpin RNAs Induce Sequence-Specific Silencing in Mammalian Cells," *Genes and Development* 16, no. 8 (15 Apr 2002): 948-58.

question as they could lead to therapeutic strategies designed to mitigate effects of some ABW agents. In addition, gene therapy research may provide insight regarding viable delivery vectors for therapeutic shRNA sequences. However, these preliminary studies are a far cry from a deployable therapeutic vector; resources need to be allocated to support aspects of this and other research devoted specifically to biodefense.

Attribution

Some current attitudes regarding attribution are focused upon developing a post-incident ability to identify an agent's source by comparing genetic polymorphisms against a database of different strains and isolates from the environment and laboratories around the world.[88] Advanced BW agents would make attribution via this route nearly impossible. Moreover, genomic approaches represent only one aspect of the various strategies that could be employed to support attribution of a BW or bioterror attack. For example, the potential for attribution could be increased by incorporating software into DNA synthesizers that "tags" products with signature sequences. Although concerns regarding the effects of incorporating "genetically silent" DNA tags into synthetic DNA sequences will need to be addressed, such markers would provide some measure for attributing agents based upon synthetic DNA. Also, many of the materials involved in production and refinement of organisms and toxins into BW agents are commercially available. Introducing trace amounts of inert, identifiable material that ultimately would become part of the agent into culture media and components used in refinement and

[88] Paul Keim, and others, *Microbial Forensics: A Scientific Assessment* (Washington, DC, American Academy of Microbiology, 2003), 5-6.

weaponization may provide insight regarding the source of materials used for agent engineering and production, providing an additional avenue to pursue attribution. Such long-term approaches would require interaction with corporations on an international level, would likely require a minimal investment, and could potentially help attribute an attack to its source.

NEED FOR "NEXT-GENERATION" APPROACHES TO BIODEFENSE

A variety of steps should be taken to ensure that our biodefense capabilities provide sufficient protection from emerging threats. First, resources should be allocated to permit evaluation of emerging biotechnologies that may foster ABW agent development and prioritize threats presented by those agents. Unclassified recommendations from intelligence professionals regarding both traditional and ABW agents should be considered when determining research priorities. Importantly, these assessments should be based primarily upon foreign technological capabilities. Depending on intelligence agencies to provide a justification for exploring novel countermeasures based upon foreign BW intentions could hinder biodefense efforts by forcing the research community to continuously remain behind the curve on emerging threats.

Second, a federally funded venue for experimentally validating biotechnology threat assessments needs to be established. Appropriate allocation of biodefense resources will require some research that has limited implications for the general bioscience community but significant application for nefarious scientists. This research should be consolidated and conducted at a single federal facility for a few key reasons: 1) consolidation of research of concern would minimize some of the challenges associated with building national and international confidence that such work was not in violation of the BWC; 2) aggregation of a good deal of leading talent in research upon highly hazardous microorganisms could facilitate higher quality research and could more efficiently promote outreach to leading scientists in developing areas that may be in need of evaluation. Research findings at such a facility could also be factored into prioritizing funding allocations for general research. In the interest of national security, many of the findings of threat assessment research probably should not be published openly;[89] however, public confidence in this effort could be maintained by establishing an independent panel of bioscience experts responsible for approving and reviewing research at the facility. Moreover, steps will need to be taken to assure allies and other international observers that such biodefense threat assessment research is not being withheld from general publication to cover up treaty violations.

Third, some federal bioscience research funds should be allocated to promote development of next-generation systems for environmental detection, medical diagnostics, prophylactics, and therapeutics. Such systems will need to provide broader analysis and identification of agents of concern. Researchers investigating the fundamental properties underlying development of these next-generation systems should be focused on identifying agents based upon the presence of a panel of indicators, keeping in mind that such agents probably would contain genetic material from a variety

[89] Gerald Epstein, "Controlling Biological Warfare Threats: Resolving Potential Tensions among the Research Community, Industry, and the National Security Community," *Critical Reviews in Microbiology* 27, no. 4 (2001): 321-54.

of organisms, including humans, bacteria, and viruses. Importantly, the bioscience research community and national security communities should be engaged to ensure transparency regarding technological breakthroughs with significant applications to biodefense.

Successful implementation of a national biosecurity strategy will require integration of a variety of independent efforts across the federal, bioscience research, and medical/public health communities. Many of these resources will be devoted to protecting populations against bioterror attacks employing traditional BW agents. This is appropriate, as these agents are and will remain the primary threat for the next few years. However, all players within the biodefense community need to be cognizant of the potential for biotechnology to impact BW in a manner that exponentially amplifies the threat both to civilian and military populations. Timely engagement of life science-enabled challenges will ensure the biodefense community is adequately prepared to address new threats before they become reality.

CHAPTER 3

PRESERVING SCIENTIFIC OPENNESS AND NATIONAL SECURITY

INTRODUCTION

This chapter provides a declassified case study describing terrorist exploitation of life science findings as an example of one kind of support that intelligence and security professionals will need to provide to the civilian scientific community to help mitigate life science enabled threats. Many in the scientific community question the nature and level of threat presented by open communication of all research findings. National security professionals have a responsibility to educate researchers regarding real world threats and ensure that they are sufficiently armed with knowledge necessary to initiate appropriate safeguards. Importantly, intelligence and security professionals must approach life scientists with a positive, open-minded attitude that reassures the research community of their primacy in addressing current issues without concerns that the national security community may call for federal implementation of restrictive measures; additional discussion following the case study serves as an example to the intelligence professional regarding the appropriate tone and language that should be used when engaging life scientists.

CASE STUDY: AL-QAIDA'S EXPLOITATION OF THE OPEN SCIENTIFIC COMMUNITY

Historically, public interest regarding the proliferation of materials and technology that could support biological warfare (BW) has been driven by information about foreign State-sponsored offensive programs and the potential for terrorist organizations to acquire weapons from rogue states. More recently, concerns that well-organized terrorist groups may seek to develop an intrinsic BW capability has reinitiated debate within both the scientific and national security communities related to the availability of "dual use" methodologies via literature and scientific exchanges. While State programs have likely used open source information to foster their BW programs, they have historically also possessed the infrastructure and funds needed to perform underlying basic and applied research into BW agents themselves. In contrast, terrorist organizations may be much more dependent upon opportunities to exploit the fruits of legitimate researchers to streamline their establishment of a BW program. This may be dangerous as it could reduce the time and technical barriers for terrorists and other extremist groups to fashion biological weapons of mass destruction.

It is no secret that the al-Qaida terrorist organization has been seeking a biological warfare capability.[90] Indeed, al-Qaida's leader Usama bin Ladin has stated that the acquisition and use of weapons of mass destruction, including biological weapons, are 'the right and religious duty' of his organization's sympathizers.[91] International press

[90] "Worldwide Threat – Converging Dangers in a Post 9/11 World," Testimony of Director of Central Intelligence George J. Tenet Before the Senate Select Committee on Intelligence (as prepared for delivery) February 6, 2002.

[91] Stefan Leader, "Osama Bin Ladin and the Terrorist Search for WMD," *Jane's Intelligence Review*, 1 Jun 1999; "Bin Laden Sought Nuclear Matter," *Boston Daily Globe*, 16 Sep 2001.

reports assert that bin Ladin's group may have acquired pathogenic agent cultures from rogue states.[92] Material recovered from Afghanistan suggests that al-Qaida was successful in obtaining some laboratory equipment and a great deal of scientific information that could be diverted toward production of BW agents.[93] Furthermore, the March 2002 discovery of an al-Qaida BW laboratory in Afghanistan is a testament to the organization's commitment to develop an intrinsic BW capability.[94] These indicators of a concerted BW effort do not reveal whether al-Qaida has yet succeeded in engineering a viable bioweapon; however, they provide insight regarding the mechanism by which the group sought to acquire their capability.

EXPLOITATION OF OPEN SOURCES A KEY COMPONENT OF AL-QAIDA'S BW PROGRAM

The documents recovered from an al-Qaida training camp in Afghanistan[95] have shed new light on the procedures and methodologies employed by al-Qaida in its efforts to establish a biological warfare program. Collectively, they reveal that individuals involved in this effort framed their program through apparent reliance upon scientific

[92] "Bin-Ladin Front Reportedly Bought CBW from E Europe, FSU," *London Al-Hayah* (in Arabic), 20 Apr 1999, 1; "Islamic Front Said Ready to use CBW Against US, Israel," *London Al-Hayah* (in Arabic), 19 Apr 1999, 1; "Preparations for BC Attack Viewed," *The Jerusalem Report* (in English), 29 Mar 1999, 20-22; "Bin-Ladin Men Reportedly Possess Biological Weapons," *London Al-Sharq al-Awsat* (Internet version-in Arabic), 6 Mar 1999.

[93] Michael R Gordon, "U.S. Says It Found Qaeda Lab Being Built to Produce Anthrax," *New York Times*, 23 Mar 2002.

[94] Tim Russert, "Interview with Gen. Tommy Franks," *NBC News' Meet the Press*, 24 Mar 2002.

[95] Research papers, clinical studies, and excerpts from academic texts related to Bacillus anthracis, Clostridium species, and Yersinia pestis, and other bacterial and viral pathogens. A list of these materials and a sample FOIA request for full documents are available at URL: <www.sciencemag.org/cgi/content/full/302/5652/1891/dc1>.

research and information obtained collegially from public and private sources (Figure 1). Handwritten letters and custom-made BW primers derived from collocated source material also suggest that al-Qaida's BW initiative was significantly advanced by the recruitment of individual(s) with PhD-level expertise who were able to support planning and acquisition efforts via their familiarity with the scientific community.

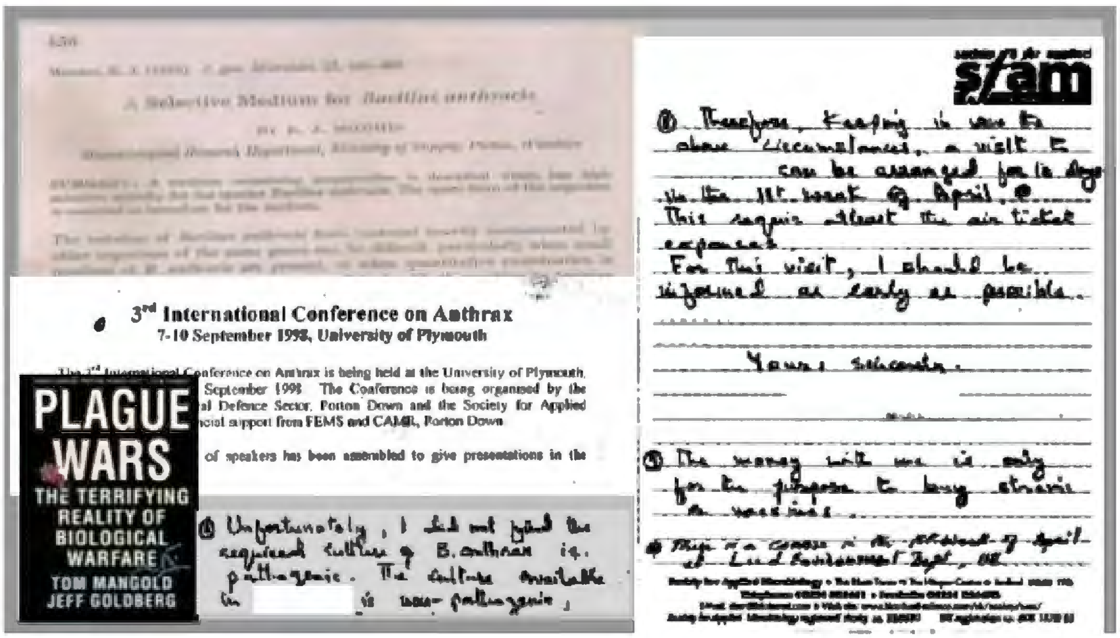

Figure 2. Collage of Selected Documents Captured at an al-Qaida Training Facility.

These are examples of documents al-Qaida obtained or drafted during its efforts to establish a BW program. The popular non-fiction book demonstrates the kind of information al-Qaida used to obtain overall guidelines for its BW program. The research article and advertisement are representative of a more extensive cache of documents and symposia proceedings that al-Qaida exploited to obtain information on isolating and growing cultures of pathogenic bacteria. The letter is but one of a series of communications among individuals involved in this activity discussing plans to acquire bacterial strains, vaccines, production equipment, training, and expertise from unsuspecting researchers. (Note that the logo of the stationary upon which the letter was written is from a respected professional society). Importantly, the excerpt in the bottom of the figure clearly outlines the need for the involved individuals to obtain a pathogenic strain of B. anthracis, confirming the author's nefarious motivation. Although certain names and locations have been removed from these examples to protect national security interests, they collectively suggest that this activity was not simply an academic exercise or pure review of relevant literature.

In defining the scope and infrastructure of its program, al-Qaida employed commonly available texts that describe foreign BW activities and outline the history of biological warfare. These books likely provided the framework for al-Qaida's intended program, as they apparently focused their efforts to model well-documented BW programs previously established by other organizations with similar financial and scientific capabilities. Diagrams (including Figure 3) and hand-written primers among the captured documents confirm al-Qaida's intention to employ this in a BW program.

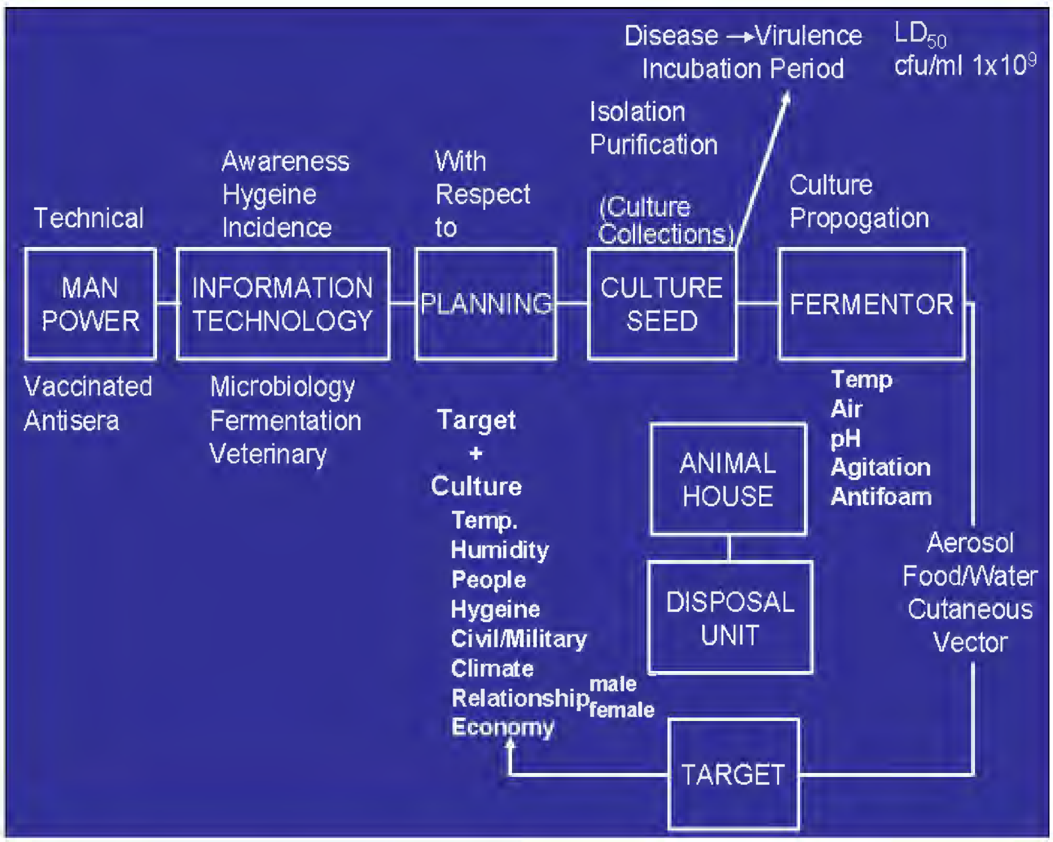

Figure 3. Cartoon Representation of al-Qaida BW Program Blueprints.

The original document was hand drawn in English and represents the conceptual framework al-Qaida apparently used to frame its BW program. Associated open source reference material contained all aspects of information compiled in this document. This blueprint outlines many factors inherent to developing bacteriological agents for BW; however, it lacks specific information discussing plans for weaponizing and delivering BW agents. The figure has been recreated from the hand-drawn original, including spelling errors.

Having laid the foundation, al-Qaida next endeavored to surmount the technical barriers presented by its limited hands-on experience producing biological agents. Lacking the capability to perform extensive research and development, al-Qaida relied heavily on reprints of vintage research articles and scientific publications from U.K. journals of the 1950's and 60's to provide a tailored methodology for the isolation, culture, identification, and production of distinct bacteriological agents, specifically *Bacillus anthracis* and *Clostridium botulinum*. When specific information was not available in print, al-Qaida scientists took advantage of selected recent symposia and other scientific meetings where they could obtain the necessary tips and techniques directly from unsuspecting researchers.

The identification of a recently-constructed laboratory within a few kilometers of the site where the BW-related documents were found and the recovery of related medical equipment and supplies that could be used to produce biological agents strongly suggests that Al-Qaida's BW effort proceeded beyond a simple review of "dual use" literature.[96] However, there is no indication that Al-Qaida was successful in obtaining a starter culture or producing any BW agents.[97] Moreover, the documents do not reveal whether al-Qaida was pursuing the acquisition of information and technology that would permit the refinement of a bacteriological culture into a BW weapon with capabilities for producing mass casualties.

---

[96] Michael R Gordon, "U.S. Says It Found Qaeda Lab Being Built to Produce Anthrax," *New York Times*, 23 Mar 2002.

[97] "Al Qaeda-Anthrax Link?" *CBS News.com,* 23 Mar 2002.

Along with Aum Shinrikyo, which developed a science-based BW program,[98] the al-Qaida BW effort may represent a trend among well-organized terrorist organizations with BW aspirations towards the establishment of a small-scale intrinsic BW production capability under the guidance of trained scientists. This represents a dangerous departure from BW-related activities of other terrorist organizations, which have historically sought to either acquire completed weapons or employ rudimentary methods to produce crude preparations of toxins and other BW agents for small scale terrorist activities, such as assassination.[99] Should terrorist organizations continue to pursue a comparatively sophisticated BW program in the future, these efforts are likely to be extremely reliant upon dual use information.

KEY OBSERVATIONS AND THEIR IMPLICATIONS FOR ADDRESSING THE PROBLEM

The al-Qaida case raises some interesting issues that must be factored into any discussions regarding the impact of scientific research upon national security:

First, al-Qaida exploited scientific resources from multiple nations, suggesting that any solution to this problem will require the active participation of the international scientific community. In the age of the Internet, the exchange of scientific ideas and

[98] Thomas Mangold and Jeff Goldberg, *Plague Wars: The Terrifying Reality of Biological Warfare* (New York, New York: St. Martin's Press, 1999), 335-51.

[99] W. S. Carus, *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents since 1900* (Washington D.C: Center for Counterproliferation Research, February 2001), 7-16.

technical information ignores national borders. Obtaining international consensus on policies to limit the spread of dual use information certainly will not be a simple task; however, it is by no means insurmountable. The threat of bioterrorism and distaste for biological weapons research are motivating factors that apply to nearly all nations. At the same time, the bulk of research funding, activity, and mechanisms for publishing and archiving published findings are consolidated within the hands of a few nations. At a minimum, U.S. scientific organizations seeking to address the dual use threat should include leading colleagues from counterpart organizations both at home and abroad. Although this may not guarantee international consensus, it is a critical first step towards resolving this issue.

Second, most of the literature al-Qaida acquired to support agent cultivation and production was published nearly 50 years ago, suggesting that a certain amount of dual-use methodology is beyond containment. It is likely that some basic information pertaining to certain human pathogens has been so widely disseminated that any effort to conceal it would be fruitless. With this information alone, a marginally-skilled terrorist could produce a crude agent for use in a limited bioterror attack. However, production of a similar quantity of agent highly refined to a “weapons grade” would significantly escalate the efficiency of dissemination, and consequently, the lethal effects of any bioterror incident. Fortunately, unclassified research that could be diverted towards such agent enhancements has only begun to appear in the open literature within the last decade and may not have been as widely disseminated. Likewise, the implications of emerging and widely disseminated biotechnologies for the enhancement or engineering of novel biological warfare agents cannot be overstated. Thus, the inability to secure a large and ever-expanding body of published research that could in theory support limited bioterrorist activities in no way absolves the scientific community of our responsibility to address these problems. It is all too easy to throw up our hands and conclude on the basis of theoretical and practical considerations that they are insurmountable.

HOW CAN THE SCIENTIFIC COMMUNITY BEST ADDRESS THE OPEN SOURCE ISSUE?

First and foremost, it must preserve free and open scientific discourse; to do otherwise would be to declare victory for our enemies the terrorists, as well as deter efforts to enhance our defenses against naturally-occurring and deliberate biological threats. However, as scientists we also accept as a moral imperative the need to ensure that our efforts result in public benefit. This goes beyond our daily research activities; while investigating technologies and fundamental properties that will lead to better medical defenses against potential biological threats we should not forego our professional obligation to mitigate against the possible misuse of our findings. At a minimum, consensus should be reached regarding research explicitly designed to enhance the utility of select organisms as weapons. For example, everyone should be able to agree that the tradeoff between benefit and risk from research aimed at improving the aerosol properties of select agents favors placement of some limitations on its otherwise broad dissemination.

The media have sensitized the general public to the potential for some published research to enhance bioterrorist efforts. Unaddressed public concerns could prompt legislative action. The scientific community could best avoid overly restrictive measures either by crafting our own set of guidelines or leading collaborative efforts on the national and international levels to develop reasonable controls.[100] Indeed, the January 9, 2003 workshop on "Scientific Openness and National Security" hosted by the U.S. National Academies of Science and the recent commitment of a number of leading scientific journals to take steps to minimize their publication of research that could directly aid bioterrorists[101] are first steps toward dealing with this problem. More recent activities, such as the NAS Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology and its report, *Biotechnology Research in an Age of Terrorism* (commonly referred to as the Fink report), released in October 2003, have made some general recommendations regarding steps the scientific community can take to mitigate the potential for nefarious use and have even identified some basic guidelines regarding specific research activities that could reasonably be anticipated to raise public concern and which should probably be subject to review and approval at an institutional level.[102]

In response to the recommendations of the NAS Fink report, the Department of Health and Human Services recently announced the creation of a National Scientific Advisory Board for Biosecurity (NSABB).[103] According to the DHHS press statement,

---

[100] Gerald Epstein, "Controlling Biological Warfare Threats: Resolving Potential Tensions among the Research Community, Industry, and the National Security Community," *Critical Reviews in Microbiology* 27, no. 4 (2001): 321-54.

[101] Ronald Atlas, and others, "Statement on Scientific Publication and Security," *Science* 299, no. 5610 (21 Feb 2003): 1149; J. B. Verrengia, "Science Journals to Join Fight against Terrorists," *Washington Post*, 16 Feb 2003, A9.

[102] Gerald Fink, and others, *Biotechnology Research in an Age of Terrorism* (Washington, D.C.: The National Academies Press, 2004), 3.

[103] DHHS Press release.

the NSABB will "advise the Secretary of HHS, the director of the NIH, and the heads of all federal departments and agencies that conduct or support life sciences research" by "recommending specific strategies for the efficient and effective oversight of federally conducted or supported potential dual-use biological research taking into consideration both national security concerns and the needs of the research community."[104] According to the NSABB website, the group will be charged specifically with guiding the development of guidelines for the identification and conduct of research that may require special attention and security surveillance.[105]

Although specific NSABB members have not yet been publicly identified, the board will consist of voting and ex-officio members from the national security and intelligence communities as well as an abundance of leading life scientists. Thus, the NSABB may serve as one vehicle for consistent and productive interaction between the intelligence and life science communities. Maximum benefit of this relationship could best be realized by ensuring that intelligence and national security professionals given the opportunity to support NSABB efforts possess a strong background in the life sciences; it will do little good for intelligence professionals who do not adequately understand the underlying principles to engage life scientists in discussions on the potential security implications of highly technical research findings.

[104] DHHS, 1.

[105] NSABB website, URL: <http: //www.biosecurityboard.gov>.

ULTIMATELY, BIOSECURITY WILL REMAIN AN ISSUE OF PERSONAL RESPONSIBILITY

The findings of a recent workshop organized by The Defense Threat Reduction Agency and The Center for Nonproliferation Studies, and public debates on how best to secure dual use information suggest that the proliferation of research techniques and methodologies applicable to biological warfare are of significant concern to the U.S. scientific community.[106] Revelations regarding the ability of al-Qaida operatives to exploit the collegiality of the scientific community in order to pursue a covert biological warfare program underscore the important role that we can play in securing all homelands across the globe. However, biosecurity will always remain an issue of personal responsibility. Ultimately, while exercising our right and responsibility to communicate novel and relevant discoveries, researchers must continue to be mindful of the potential negative implications associated with misuse of our findings. We should remain alert for indicators that others may be attempting to exploit such information for nefarious purposes, but in so doing, avoid paranoia and excessive suspicion, and promote the dramatic, beneficial impact of creative and open science.

[106] Raymond A. Zilinskas, and Jonathan B. Tucker, "Limiting the Contribution of the Open Scientific Literature to the Biological Weapons Threat." Homeland Security website, URL: <http: //www.homelandsecurity.org/journal/Articles/tucker.html>, accessed 21 Dec 2002.

CHAPTER 4

THREAT ASSESSMENT RESEARCH: A CRITICAL COMPONENT OF NATIONAL BIODEFENSE

INTRODUCTION

The principal objective of biological warfare (BW) threat assessments is to identify and prioritize BW threats to civilian and military populations. In an ideal world, BW threat assessments provide policymakers with clear and compelling guidance to prioritize biodefense research, development, testing, evaluation (R, D, T, & E) and acquisition in a manner that utilizes finite resources yet achieves parity with the offensive BW threat. Unfortunately, the biodefense community does not yet live in an ideal world. National security professionals responsible for crafting BW threat assessments are often challenged by both intrinsic and external factors that limit either the clarity or timeliness of their assessments; these factors may necessitate analytic strategies that yield broader judgments and complicate threat prioritization. Some of the challenges underlying prioritization of BW threats could be mitigated if a greater volume of technical assessments based upon empirical data were available. In this regard, creation of a national program for threat assessment research for the technical validation of threat agents would be a valuable addition to the nation's overall biodefense strategy. This article will outline the fundamental justification for a coordinated national threat assessment research effort, discuss some of the principal challenges associated with such research, and suggest a few options for their resolution.

BW Threat Assessments: Models, Options, and Limitations

Traditionally, analysts charged with assessing biological weapons threats to the U.S. have focused on identifying the capabilities and intentions of foreign states and non-state actors. For most intelligence professionals, Threat = Capabilities + Intent. Some analysts responsible for assessing the risk posed by BW threats to U.S. infrastructure have assessed the threat in the context of a potential target's perceived vulnerability. For these individuals, Risk = Vulnerability + Threat, which can also be written as: Risk = Vulnerability + Capability + Intent. The specific responsibilities of the analyst notwithstanding, a strong understanding of both the capabilities and intentions of potential bioweaponeers are critical components of a balanced, informative BW threat assessment.

In general, the term "capability" refers to the fundamental ability of a state or non-state actor to access assets required for production and employment of biological weapons. These assets can be tangible or intangible. Tangible assets include: knowledgeable personnel, seed stocks, materials and equipment necessary for agent culture, production, harvesting, refinement, weaponization, and delivery, and facilities with appropriate sources of water, power, and when desired, biocontainment for hazardous materials and/or disposal of hazardous waste. Intangible assets can include expertise and information germane to the production and deployment of BW agents.

In theory, acquisition of assets that can be applied towards an adversary's capability to develop a bioweapon are associated with an identifiable signature. Once identified, an analyst familiar with BW issues can categorize and evaluate the data obtained from such signatures and, through synthesis, arrive at a general assessment regarding a specific organization's capability to employ BW. However, most of the materials and knowledge applicable to bioweapons development are principally associated with legitimate endeavors; thus, analysts require further information to determine whether a foreign entity's capability actually represents a threat.

International condemnation of bioweapons development through agreements such as the Biological Weapons and Toxins Convention presumably motivates foreign entities to conceal illicit programs (often within legitimate activities), compounding challenges associated with distinguishing BW activity from the background of legitimate medical research and pharmaceutical industry. Thus, information that provides insight regarding the intentions of an adversary to employ available assets towards BW is of greatest value. Unlike information that provides insight into foreign capabilities, which is targeted toward the identification and characterization of personnel, equipment, and materials and can be collected from a variety of sources, insight regarding foreign intentions can only be obtained from people - individuals actively engaged in utilizing foreign personnel, equipment, and materials for BW. Thus, BW analysts generally rely upon the willing cooperation of individuals associated with foreign bioweapons programs for intelligence that provides insight regarding the intentions of their organization's program; such individuals are rare and the insights they provide are often incomplete, contradictory, or lack sufficient detail for analysts to reach definitive judgments.

In the traditional model for crafting BW threat assessments, information gathered from a variety of sources is evaluated for its validity and then integrated to craft as clear an assessment as possible regarding the capabilities and intentions of an adversary's program. Much of the information related to this activity is subjective and lacks technical detail; thus, the quality and analytic rigor applied to individual program assessments can vary somewhat based upon the relative technical expertise and perspective of individual analysts. This challenge to establishing a consistent analytic threshold is compounded by the fact that the intelligence community's collection capabilities are finite, diffused among a wide range of priorities, and ultimately unable to provide sufficient information to characterize foreign BW activities beyond a reasonable doubt. Thus analysts vary not only in their intrinsic abilities to perform analysis, but have different amounts of information of varying and subjective quality that can at best yield a partial picture of a foreign entity's BW activities. Together, these intrinsic and external variables pose a significant challenge to intelligence professionals tasked with prioritizing BW threats in a manner that appropriately helps target biodefense resources.

Biodefense Prioritization Models: Threat or Capabilities based?

One defining principle of a successful biodefense strategy is that it achieves parity with the BW threat. In this regard, the traditional model of prioritizing biodefense initiatives based upon BW threat assessments is problematic for biodefense policymakers because it ensures that the defense lags behind the offense. This naturally stems from the requirement for scarce information that provides key insight to foreign intentions regarding BW. By the time such a threat assessment is available to biodefense decision makers, the foreign entity often has achieved significant progress toward acquisition of a BW capability. Thus, biodefense efforts to protect civilian or military personnel from BW threats largely follow development of the threats themselves. Since development of countermeasures approved for human use requires more time and money than development of an offensive capability, a BW threat may persist for years before an adequate defense is available. This problem is compounded by the potential for relatively inexpensive and ubiquitous methods for genetic modification of existing threat agents to defeat countermeasures. Thus, it is reasonable to assume that a biodefense effort that justifies R, D, T, &, E of specific countermeasures based solely on threat assessments will continue to remain behind the "threat curve."

An alternate option for biodefense to establish parity with the offense would be to move from a "threat assessment"-based justification of countermeasures development towards a "capabilities-based" approach. Such a strategy would roughly parallel Secretary of Defense Donald Rumsfeld's plan for incorporating the capabilities-based methodology into his transformation of the Department of Defense.[107] Under this plan, development of weapons systems and acquisition of military countermeasures would no longer be principally tied to specific threat-based assessments; instead, such systems would be developed in a manner that provides DOD the capability to surmount any potential threat an adversary could present. Applied broadly to biodefense, a capabilities-based approach would entail the creation of environmental detectors, diagnostics, prophylactics, therapeutics, and attribution methodologies that could ensure a rapid and efficacious response to any BW attack, regardless of the agent used. Importantly, the development of these systems would not be tied to the presence of specific threat assessments, permitting biodefense to not only establish parity with the offensive threat, but to exceed it.

---

[107] United States Department of Defense, *Quadrennial Defense Review Report* (Washington, DC: Office of the Secretary of Defense, 2001), iv.

Although the capabilities-based model appears to circumvent the major limitations of a threat assessment-based strategy, there are a number of challenges presented by a purely capabilities-based approach to biodefense:

- First, current limitations regarding underlying technologies necessary for creation of generalized countermeasures will continue to necessitate agent-specific defenses for at least the next few years.

- Second, the pursuit of high-technology approaches to biodefense holds promise for immense benefits; however, disproportionate allocation of resources toward their development would leave civilian and military populations vulnerable to near term threats.

- Third, biotechnology holds promise to enable the rational engineering of novel threat agents in vast excess of what finite biodefense funding allocations could address. Thus, even in the absence of intelligence-based threat assessments, a mechanism for the prioritization of BW threats to civilian and military populations will be required to ensure a basic level of near and long term security.

These challenges suggest that a purely capabilities-based approach to biodefense might not be possible in the near term, or cost-effective in the long term.

Quite likely, the most feasible and cost effective approach for targeting and prioritizing biodefense R, D, T, & E activities would integrate the strengths of both threat assessment-based and capabilities-based strategies. Although threat assessments that provide specific insight regarding the intent of nefarious actors should always be considered in this process, biodefense initiatives would be more responsive if they were not wholly dependent upon such assessments. At least in the near term, biodefense activities will remain tied to the development of specific countermeasures and would benefit from BW threat assessments that focus on the specific capabilities of foreign entities whose strategic interests are likely to conflict with those of the US. In addition, generalized biodefense initiatives that hold promise to yield a strategic advantage to the defense also should be pursued. Such an approach will quite likely increase the quantity of potential BW threat scenarios that are incorporated into existing assessments; thus, a methodology for evaluating and prioritizing these threats would be required to increase the likelihood that biodefense expenditures are addressing threats that pose the greatest risk to the US.

Threat Assessment Research: Empirical Validation of BW Threat Agents

A critical, yet often overlooked component underlying BW threat assessment pertains to the relatively limited breadth and depth of integrable information that is available on the physical properties and characteristics of microorganisms with potential as BW agents or their toxic products. Empirical data can provide critical insight regarding the threat many of these agents actually present to naïve and protected populations. Traditionally, BW agents have been selected from naturally occurring microorganisms that possess an ideal combination of toxicity, stability in the environment, and ease of production. Many of the organisms traditionally associated with BW were first identified as human or agricultural pathogens; varying amounts of data relevant to epidemiology, prophylaxis, diagnosis, and therapy as well as some basic insight regarding the mechanism(s) of pathogenesis are available on these agents. Throughout the twentieth century, technically advanced state-sponsored bioweapons programs recognized the operational benefits associated with optimization of microbiological weapons through laboratory studies; these programs have generated some additional data regarding the physical properties of agents that are highly germane to assessing their potential as bioweapons and would not normally be generated through medical research or basic science targeted toward development of countermeasures. Such information is and will continue to be extremely valuable to those individuals responsible for assessing bioweapons threats.

Historically, US intelligence efforts have arguably been hampered somewhat by varying levels of information regarding the basic properties of suspected biological agents. Despite the presence of some research reports generated by the former US BW program, which was discontinued in 1969, the body of technical literature related to prospective biological threat agents available to BW analysts arguably has not kept pace with the identification of organisms potentially being developed in foreign bioweapons programs or the emergence of infectious diseases with epidemiological properties that suggest potential for their misuse as BW agents. Even the data that was generated in the 1950-60's does not reflect the level of granularity and insight that could be gained if modern laboratory approaches were used to study relevant properties of biological threat agents. Moreover, with few exceptions, little research regarding the implications of genetic modification of existing pathogens has been performed, hampering our understanding of how such activities might truly impact the BW threat. In the absence of empirical data, analysts with varying levels of scientific expertise have been forced to make estimates and judgments when trying to evaluate and portray the threat posed by newly emerging organisms or genetically modified BW agents. Efforts to direct finite biodefense resources in a manner that best addresses threats would benefit if threat assessments incorporated more empirical observation and less intellectual inference.

A national strategy targeted to support threat assessment research could be immensely beneficial both to BW threat analysts and the prioritization of biodefense R, D, T, & E activities. Such research could be directed to explore a variety of areas. Studies designed to thoroughly characterize the physical properties of biological agents on the CDC select agent list germane to bioweapons development, including their environmental stability, aerosol properties, and human lethality (LD_{50}[108]) values extrapolated from studies on validated animal models would fill essential gaps on traditional agents. Research into the effects of simple genetic modifications upon existing countermeasures to known BW threat agents could help answer questions regarding the actual risks posed by such activities. Focused investigation of the feasibility for emerging technologies to enable rational engineering of novel threat agents or to fundamentally alter the technologies and processes traditionally associated with bioweapons development would permit informed and educated discussions regarding options to mitigate the proliferation of technologies with greatest potential for misuse. Data obtained from these studies would be useful for prioritizing threat agents for development of countermeasures; in addition, the findings of threat assessment researchers could feed back to the intelligence community and enhance existing threat assessments.

Creation of a national strategy for threat assessment research would require input from a number of entities within the federal government, private industry, public health, and life science research communities. Within the federal government, the Department of Homeland Security (DHS) likely will have a major role in formulating and implementing policies for threat assessment research; this activity would most likely occur in the context of the National Biodefense Analysis and Countermeasures Center (NBACC). Additionally, members of the national security organizations, particularly

[108] A dose which is lethal for 50% of the recipient population.

those in the intelligence community, stand to benefit from threat assessment research coordinated by DHS and should be engaged in providing insight and guidance to research efforts. The Departments of Agriculture, Defense, Energy, and Health and Human Services also should be engaged in crafting, supporting, and benefiting from the findings of threat assessment research as such findings could help better target allocations of biodefense funding to appropriate research projects. Outside of the federal government and its assorted biodefense contractors and subcontractors, private biodefense organizations, public health professionals, and life scientists would likely seek to benefit from research activities and findings, but also would be likely to pursue opportunities to obtain research funding, advise on topics requiring expertise that resides outside of the government, and provide independent oversight to threat assessment research activities.

Since threat assessment research activities hold potential to impact such large and disparate groups within the biodefense community, it would seem logical to include input from these groups into any national strategy to pursue such research. At a minimum, discussions need to occur among members from the relevant parties to identify key issues and obtain consensus regarding their resolution. Initially, these interactions will likely be ad hoc. Ultimately, formal partnerships between concerned communities and federal representatives committed to initiating, executing, and sustaining DHS programs for threat integration, analysis, and assessments from a technical perspective will be needed. Implementation of an efficacious research program will require coordination of a variety of organizations; overall cooperation could be enhanced if each participant is aware that they hold a stake in the outcome.

CRITICAL ROLE FOR INTERACTIONS WITH THE LIFE SCIENCE COMMUNITY

Any national activity related to threat assessment research is likely to benefit significantly from the full engagement of the life science research community. Scientists from academia and industry as well as those within the government have unique insights and expertise that would permit them to contribute in relevant and meaningful ways to research efforts targeted to aid BW threat assessment. As a community, life science researchers possess significant knowledge in the biological sciences that, as a whole, overshadows the relatively limited expertise currently retained within the government. Their involvement could augment federal capabilities in this area, enhancing research activities and assessments and ensuring a broad perspective regarding threat assessment research activities. In addition, those scientists within the government whose efforts have historically focused on studying BW threat agents and developing countermeasures possess insights that would be helpful to those seeking to experimentally validate BW threats. Thus, representative life scientists from academia, industry, and the federal government should be included in discussions regarding a national strategy for threat assessment research.

Currently, discussions within the life science community regarding the potential for open communication of a subset of discoveries to support the activities of bioterrorists or bioweaponeers have led a number of leading researchers to consider the potential impact associated with misuse of their research findings.[109] These discussions, along with ongoing debates regarding what, if anything should be done to mitigate open-source

[109] David Malakoff, "Science and Security. Researchers Urged to Self-Censor Sensitive Data," *Science* 299, no. 5605 (17 Jan 2003): 321.

enabled threats hold potential to invigorate a number of researchers to reconsider fundamental questions regarding the biological weapons threats facing the US. This renewed interest among life scientists in issues pertinent to BW could increase willingness among leading researchers to partner with the federal government on research projects and working groups intended to explore the technical aspects of BW threats. Such partnerships will play a critical role in establishing legitimacy, building confidence, and ensuring quality control of threat assessment research activities. Clearly, the onus will be on representatives of the federal government to harness the goodwill of the scientific community and incorporate life science researchers in unique and effective ways.

Some life scientists are already engaged in fundamental research targeted to elucidate potential threats presented by biotechnologies. The 2001 revelation that incorporation of an immmunoregulatory gene, IL-4, into ectromelia resulted in a virus capable of high lethality among vaccinated mice[110] raised concern that similar modification of Variola (smallpox) could yield a virus capable of evading the smallpox vaccine.[111] However, there are a number of fundamental questions that must first be answered regarding the underlying mechanism of lethality in mice and the

[110] R. Jackson, and others, "Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox," *Journal of Virology* 75, no. 3 (2001): 1205-10.

[111] E. Finkel, "Australia. Engineered Mouse Virus Spurs Bioweapon Fears," *Science* 291, 5504 (26 Jan 2001): 585.

immunoregulatory role of IL-4 in different species.[112] Some scientists are currently researching these issues;[113] depending upon their findings, some may claim that further studies into the threat posed by incorporation of immunomodulators into viruses capable of infecting non-human primates would be justified. In addition, the Department of Defense has funded research targeted to address specific concerns, including the recreation and evaluation of a genetically modified strain of *Bacillus anthracis* that foreign researchers had reported capable of evading a human anthrax vaccine.[114] These examples underscore the importance of federal involvement in coordinating and regulating threat assessment research; a centralized effort will minimize redundancy and has the greatest potential to facilitate transparency regarding justification of research activities with participating scientists and safeguarding against foreign misperceptions and allegations of illegitimate research activities.

Ensuring ideal interactions between biodefense professionals performing technical threat assessment research and the appropriate life scientists will be challenging. Federal biodefense professionals will possess sufficient expertise in a few key areas; however, they may not possess the extensive network of contacts needed to ensure that leading experts in niche areas of research from outside the government are

---

[112] M. N. Norazmi, "Possible Mechanism for the Enhanced Lethality of an Interleukin-4-Expressing Mousepox Virus." *Journal of Medical Microbiology* 50, no. 10 (2001): 936.

[113] T. R. Johnson, and others, "Construction and Characterization of Recombinant Vaccinia Viruses Co-expressing a Respiratory Syncytial Virus Protein and a Cytokine," *Journal of General Virology* 82, no. 9 (2001): 2107-16; M. S. Rolph and I. A. Ramshaw, "Interleukin-4-Mediated Downregulation of Cytotoxic T Lymphocyte Activity is Associated with Reduced Proliferation of Antigen-Specific CD8+ T Cells," *Microbes and Infection* 5, no. 11 (2003): 923-32; D. MacKenzie, "US Develops Lethal New Viruses," *New Scientist* 29 Oct 2003.

[114] Victoria Clarke, "DoD News Briefing," briefing presented at the Pentagon, Washington, DC, 4 Sep 2001.

provided the opportunity to participate. Likewise, knowledgeable scientists committed to supporting federal initiatives may be unable to identify and engage the appropriate federal entities. Clearly, both communities could benefit from the intercession of a third party as an emissary to facilitate necessary interactions. In this regard, the National Academies, particularly the National Academy of Sciences (NAS), has an established track record of providing the federal government with advice and scientific advisors related to a range of national security topics.[115] The NAS is well placed to interact with federal representatives, determine the substantive requirements of the government, and identify, contact and host workshops consisting of the appropriate experts from academia, government, and industry. Inviting the NAS to help guide creation of a standing committee of scientists with the expertise to advise and provide oversight of both classified and unclassified federal threat assessment research initiatives would ensure the involvement of a sufficiently broad and eclectic cross-section of the life science research community. Such scientific support and oversight of threat assessment research programs would lend itself to confidence building and ensuring quality control of research activities. However, because the NAS is primarily a facilitator of advisory efforts and typically employs a process that can be slow and is unresponsive to rapidly changing requirements, it ultimately cannot be considered a responsible entity for decision making and would need to be directed by a federal entity.

[115] Information about the NAS available at URL: <http: //www.nationalacademies.org/about/>.

CHAPTER 5

PRINCIPAL CHALLENGES ASSOCIATED WITH THREAT ASSESSMENT RESEARCH

INTRODUCTION

In crafting and implementing a national strategy for empirical validation of biological weapons threats, the biodefense community will need to carefully evaluate how to address the variety of issues that such research will raise both nationally and globally. Not only will all threat assessment research need to comply with the precepts outlined in the Biological Weapons and Toxins Convention (BWC), but the federal government will also need to take steps to build national and international confidence that such research is not intended to establish an offensive capability. Furthermore, internal mechanisms for proposing and executing individual studies will need to be developed; such mechanisms would benefit from independent external reviews to ensure scientific rigor. Finally, individuals responsible for the research programs will need to define guidelines for distinguishing findings that can be openly reported from those that should probably be retained for national security purposes and only disseminated to key individuals in participating communities with a defined “need to know.” Although resolution of these issues may enable a more productive program for threat assessment research, less obvious challenges are also likely to arise in the future.

COMPLIANCE WITH THE BIOLOGICAL WEAPONS AND TOXINS CONVENTION

Following President Nixon's decision for the U.S. to discontinue and dismantle its BW program in 1969, a number of nations called for the creation of a comprehensive international agreement banning the use or development of biological weapons. Discussions along these lines occurred throughout 1970 in the Conference for the Committee on Disarmament, which in late 1971 unanimously approved a draft resolution prohibiting biological weapons programs. This resolution, commonly referred to as the Biological Weapons and Toxins Convention (BWC), was signed by the U.S. on April 10, 1972 and ratified on March 26, 1975.[116] According to Articles I and IV of the BWC, each of the participating State Parties:

> Undertakes never in any circumstances to develop, produce, stockpile, or otherwise acquire or retain:
>
> (1) Microbial or other biological agents, or toxins whatever their origin or method of production, of types and in quantities that have no justification for prophylactic, protective or other peaceful purposes;
>
> (2) Weapons, equipment or means of delivery designed to use such agents or toxins for hostile purposes or in armed conflict.[117]
>
> Each state party to this Convention shall, in accordance with its constitutional processes, take any necessary measures to prohibit and prevent the development, production, stockpiling, acquisition, or retention of the agents, toxins, weapons, equipment and means of delivery specified in article I of the Convention, within the territory of such State, under its jurisdiction or under its control anywhere.[118]

[116] M. Leitenberg, "Biological Weapons in the Twentieth Century: A Review and Analysis," *Critical Reviews in Microbiology* 27, no. 4 (2001): 267-320.

[117] Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction. 10 Apr 1972. Article I.

[118] Convention, Article IV.

Thus, under the BWC, research activities that are consistent with the development of microbiological organisms or their toxic products for BW are strictly prohibited and signatory states assume responsibility for ensuring that they do not directly engage in or otherwise facilitate such proscribed research.

Despite outlawing offensive BW activities, the BWC does make a provision for research targeted toward the development of defensive measures or for other peaceful purposes. However, the text pertaining to these provisions is vague and open to legal interpretation. These defensive provisions present a situation that can challenge international confidence in signatory parties. For example, under BWC provisions, signatory states are permitted to maintain small quantities of pathogenic microbes and toxins consistent with legitimate research. Arguably, small quantities of microbes that could be used for defensive research could also be employed by an aggressor as seed stocks for rapid expansion and production of biological weapons in response to a perceived need. Thus, the dual use nature of defensive research activities naturally invites international suspicion of facilities and researchers engaged in such studies. These suspicions are likely compounded by the well documented BWC violations of the Former Soviet Union and Iraq throughout the 1970's-1990's.[119,120] Unfortunately, the BWC does not provide clear insight as to the mechanism by which participants can distinguish the legitimate endeavors of others from proscribed research under the cover of

---

[119] Alibek, *Biohazard.*

[120] Raymond A. Zilinskas, "Iraq's Biological Weapons. The Past as Future?" *Journal of the American Medical Association* 278, no. 5 (6 Aug 1997): 418-24.

a legitimate activity. Instead, the Convention prohibitions focus largely on the intent underlying research initiatives, which as discussed above, is difficult to gauge.[121]

As a signatory of the BWC, the U.S. has a moral imperative to make certain that all federal research activities in the biological sciences are consistent with the Convention's language and intention. Generally, the vast majority of life science research that either occurs in or is funded by the U.S. is of such an obviously beneficial nature that it poses little potential for conflict with the BWC. However, many research initiatives pertaining to the empirical assessment of biological weapons threats are likely to raise concerns regarding U.S. compliance with the BWC. Thus, any federal strategy that focuses on threat assessment research will require strict administrative guidelines and procedures to verify that all activities are legally compliant. There is a small precedent set by research performed within the Department of Defense (DOD), which historically has engaged in the bulk of activities designed to defend against foreign BW threats. In September 2001, the DOD revealed that it had approved a research project to genetically engineer a strain of *Bacillus anthracis* that reportedly was capable of circumventing a human anthrax vaccine.[122] Prior to its approval, the proposed study reportedly was subject to many levels of review throughout the DOD, including an internal assessment regarding its compliance with the BWC.[123] This study likely represents one of the most extreme examples of such research: the genetic modification of a highly hazardous human pathogen. A review of DOD's validation process for this research may be

[121] M. Leitenberg, "Distinguishing Offensive from Defensive Biological Weapons Research," *Critical Reviews in Microbiology* 29, no. 3 (2003): 223-257.

[122] Clarke, 2001.

[123] Clarke, 2001.

insightful for those charged with ensuring threat assessment research is compliant with the BWC.

Ultimately, however, as intent is the driver for compliance with the BWC, not necessarily the actual action; the intention of the U.S. to not engage in the development of offensive BW program will automatically ensure that all activities are legally compliant; however, a variety of actions will be required to express that intent to domestic and international entities. Therefore, in addition to standard mechanisms for legal and administrative review of research proposals, there may be a set of general principles that researchers could follow to safeguard against misperceptions that their studies violate the BWC. Some of these principles could be related to the subtle nuances one would expect to see in offensive BW research programs as opposed to those efforts exclusively associated with the defense. For example, although studies regarding the basic physical properties of many organisms associated with BW are equally useful to weapons development and modeling for defensive purposes, downstream research regarding the optimization of agent delivery systems would be important for weapons development but not definitive for defensive purposes. Having guidelines that permit some basic research with high potential for concern but draw the line short of applications needed for weapons development may help minimize concerns related to BWC compliance.

The scale of the research activity also can provide some insights as to its legitimacy. In the case of threat assessment research, most studies into the optimization of scale-up production are not particularly relevant to understanding the threat presented by an agent, but would conceivably be of interest to an offensive program. Maintaining studies with traditional BW agents at a small scale could further reduce concerns; however, genetically engineered agents may present a hazard that exceeds that of traditional agents regardless the scale of production, requiring additional guidelines. In respect to such "artificial" agents, BWC compliance could be maintained by ensuring that whenever possible, such studies are performed with microorganisms that are not infectious for humans or organisms of agricultural concern. In this regard, the threat presented by an underlying technology or principle could be gauged in a manner that does not *a priori* entail the creation of a new organism with potential for misuse.

Finally, the focus and documentation of research activities might be able to provide insight regarding BWC compliance. In theory, an offensive BW research effort would be primarily concerned with the identification and refinement of an agent for use as a weapon. Assuming such an effort were carefully documented, external review of those documents might reveal the progression of the offensive effort over time entailed a number of dead ends leading to successes that undergo increasing levels of refinement and optimization. Legitimate threat assessment research should be focused on specific questions and have a finite scope that does not include sequential rounds of optimization. Tightly regulated documentation of all activities and resources expended upon threat assessment research could permit external reviews that support the defensive nature of the research. Incorporation of these and other nuances associated with defensive and not offensive programs could help ensure that threat assessment research activities remain fully compliant with the BWC.

BUILDING NATIONAL AND INTERNATIONAL CONFIDENCE THAT RESEARCH IS NOT OFFENSIVE

U.S. threat assessment research programs will be challenged to build confidence both domestically and within the international community that laboratory studies are not intended to support an offensive BW program. Although measures to ensure compliance with the BWC will be essential, the fact that confidence in the Convention has been undermined somewhat by covert BW programs of signatory states will require the U.S. to pursue avenues above and beyond what the BWC requires to obtain domestic and international support. A satisfactory level of domestic support could possibly be achieved through the creation of both federal and independent oversight mechanisms responsible for monitoring and reviewing threat assessment research activities. Garnering international support will present more challenges, but could benefit from activities specifically designed to build confidence in the defensive nature of the programs.

Oversight of threat assessment research activities would be simplified if they were consolidated within or coordinated by a single federal entity, as may be the case under NBACC. Assuming a centralized organization, federal oversight could be maintained through Congress and the Department of Homeland Security. Congressional oversight would provide a mechanism for ensuring research is properly coordinated with relevant organizations throughout the Departments of Homeland Security, Defense, Agriculture, Energy, and Health and Human Services. In addition, the Office of Management and Budget (OMB) could provide oversight regarding expenditures and documentation associated with research activities, inspiring confidence that funds are being spent accordingly. Since a small proportion of threat assessment research will be classified, oversight mechanisms would need to be capable of monitoring all projects accordingly.

In addition to federal oversight, public confidence in the legitimacy of research activities could be enhanced by additional oversight from non-governmental sources. Some of the toughest critics of federal threat assessment initiatives are likely to come from within the life science research community itself. Thus, confidence in federal threat assessment research could be built among this community if a panel of leading life scientists was established to validate, review, and oversee research activities. Such a panel would need to contain respected researchers not affiliated with the federal government but knowledgeable about fundamental technologies pertinent to biodefense. Either the NAS or the Department of Health and Human Services could be well placed to identify such researchers and manage the administrative challenges associated with initially organizing and convening such an oversight committee (OC). OC members would ideally consist of respected leading researchers with the expertise and ability to inspire confidence in the international scientific community and a handful of key government scientists and national security experts with a strong background in the biological sciences. These individuals should be critical thinkers who recognize the need for threat assessment research but are capable of evaluating individual research proposals on their own technical merits. The OC would be responsible for reviewing and approving threat assessment research proposals based upon technical merit, appropriateness of research, and anticipated value of research findings to national biodefense. Importantly, the OC would need full access to all research proposals, activities, and findings to provide the stringent oversight needed to inspire external confidence. Thus, the federal government would need to reserve high level security clearances for all standing OC members. Furthermore, the OC would benefit from intelligence community insights regarding foreign bioweapons threats.

Securing international confidence regarding threat assessment projects will require a variety of initiatives that roughly parallel traditional non-proliferation confidence building activities. Chief among these are efforts to ensure confidence among our closest allies. International exchanges between leading defense and security researchers will provide opportunities for transparency regarding research initiatives and findings. Naturally, the level of transparency will vary depending upon the classification of the research; however, interactions among threat assessment researchers and their appropriate counterparts could foster some confidence in U.S. activities. Naturally, similar exchanges with representatives from friendly governments may hold potential to mitigate suspicions.

International confidence could also be enhanced by hosting foreign researchers and representatives at sites associated with threat assessment research. There will be challenges inherent to having such visits at sites where classified research is occurring; however, there is the potential for immense benefit to permitting such interactions. Visits to U.S. research facilities may dissolve foreign misconceptions regarding the materials and activities present at those sites. According to Ken Alibek, a former program manager in the Soviet bioweapons program, his participation in confidence-building site visits played a large role in convincing him that the U.S. was not engaged in offensive BW.[124] Visits of a similar nature would provide skeptical governments an opportunity to interact

---

[124] Alibek, *Biohazard*.

with working researchers and verify the information provided during information exchanges. Openness with the international community in areas of unclassified work would further support U.S. diplomatic assurances regarding the defensive nature of threat assessment research.

Participation by threat assessment researchers in international scientific meetings and symposia would provide an additional confidence-building measure. Having researchers present aspects of their research and findings that do not directly relate to issues sensitive to national security could provide opportunities for threat assessment researchers to network with leading international scientists in areas of mutual interest. Such informal associations can lead to increased confidence in the personnel engaged in validating bioweapons threats and provide some margin of support to the legitimacy of their efforts. Despite all of the above options, there will likely be a subset of nations that will remain skeptical and suspicious of U.S. threat assessment research activities regardless of the efforts taken to build their confidence. Thus, decision makers and diplomats will need to determine how much international support is necessary or sufficient to merit independent U.S. threat assessment research and target confidence-building measures to achieve that level of international consensus.

DEFINING THRESHOLDS FOR INITIATING RESEARCH PROJECTS

In addition to addressing external challenges, such as ensuring BWC compliance and promoting confidence that threat assessment research is not supporting offensive developments, homeland security professionals will need to develop internal procedures that set the threshold for identifying and initiating specific research projects. Arguably, there are many gaps in U.S. technical knowledge regarding both traditional and technology-enabled BW threats; the potential avenues of investigation could possibly exceed available federal funds. Thus, efficient prioritization of research topics will be a critical determinant of how effectively the federal program is able to empirically assess BW threats. In addition, certain topics of investigation are likely to raise greater concerns than others regarding the benefit of research findings compared with the potential risk the study might pose to the general population. For example, concerted studies intended to ascertain the UV sensitivity(ies) of various strains of *Bacillus anthracis* (anthrax) would likely raise fewer eyebrows than would efforts to explore whether targeted genetic modifications to the Ebola virus impact the efficacy of vaccines currently in development. Although both studies address issues highly relevant to understanding potential BW threats, they highlight the need for a defined mechanism to identify and pursue maximally beneficial research initiatives.

One option would be for the federal government to require that any research be fully justified by intelligence that indicates a specific threat. For example, let's assume an intelligence agency were to learn that a terrorist group had developed a method to isolate a highly potent toxin from coffee grounds and were planning to use the toxin extract in an attack. In this situation, threat assessment researchers would review the relevant scientific literature and initiate a research study to assess the efficacy of the extraction methodology, perform toxicity studies in animal models, extrapolate the estimated human LD_{50} of the "coffee toxin," and provide a technical assessment regarding its utility in the indicated attack. The intelligence-based approach has the benefit of linking each research project to validated intelligence, providing a defensible, albeit classified, justification for its execution. Such justification can serve to mitigate foreign concerns regarding studies undertaken to support an offensive program. Furthermore, having threat assessment research closely tied to specific intelligence keeps it on a short leash; projects have specific goals and can be focused in a finite manner. An intelligence-based program can also ensure that federal expenditures are targeted to address national security issues, validating investments in the associated laboratories and investigators.

However, despite the benefits associated with linking the threshold for initiating threat assessment research to specific intelligence reporting, this option also presents a number of potential limitations. In order for research to be shielded from suspicion by its association with an intelligence report, the research must closely parallel the threat as outlined. This links the depth and quality of research to that of the supporting intelligence. Unfortunately, intelligence rarely provides a clear picture regarding highly technical details and can even contain some information that is inaccurate or open to misinterpretation. If linked tightly to partial or flawed intelligence, research proposals will be only partially effective at providing technical assessments of the threat. For example, imagine in our earlier scenario of the "coffee toxin" that the extraction procedures indicated by intelligence were inaccurate or represented an initial methodology that the terrorists had later refined, but one the IC had been unable to identify. Laboratory exploration of the reported extraction methodology could inadvertently result in an inaccurate assessment that the activity represents a low threat based upon the poor methodology employed. Although the researchers may hypothesize that a refined methodology could yield an ample quantity of the deadly coffee toxin, they would be unable to perform the necessary experiments because they lie outside of the threat indicated directly by the intelligence. Thus, strict adherence to an intelligence-based justification may hamper creativity and scientific rigor, preventing an optimal balance between the breadth and depth of research.

Another option for regulating threat assessment research is to make it purely science-based and hypothesis driven. Under this methodology, research proposals are validated solely upon their technical scientific merit and potential to address hypotheses with implications for our biodefense capabilities. For example, a threat assessment researcher reads a scientific paper that leads her to hypothesize that a simple genetic manipulation of a human virus could make it resistant to all known antiviral drugs. Based upon this hypothesis, the researcher develops a thorough, well controlled research strategy to engineer the virus, test its ability to resist the antiviral drugs, issues an appropriate technical threat assessment based on the data, and suggests strategies for the creation of novel therapeutics. The science-based method provides the researcher greater intellectual flexibility and permits a thorough assessment of threat enabling technologies based upon a rationally-designed research strategy. Moreover, the hypothesis-driven approach engenders greater confidence in the technical merits of the final assessment due to the rigorous process underlying the scientific methodology. Furthermore, under this approach, research projects are permitted to develop in a manner that has sufficient breadth and depth to facilitate deep technical understanding of the underlying threat.

Similar to the intelligence-based approach, the science-based approach potentially has significant limitations. In the absence of guidance from intelligence regarding current threats, research that is purely hypothesis driven may tend to reflect the personal preferences and interests of the researcher. For example, in examining the previous case of the researcher who genetically modified a virus to be resistant to known antiviral drugs, it may be enlightening to learn that the virus she studied, although a human pathogen, has never been suspected or associated with any BW programs. Although the research would have been well-executed technically and led to novel discoveries, it ultimately would be of marginal benefit to national biodefense. Taken to an extreme, threat assessment projects that are approved based solely on scientific criteria may hold long-term potential for researchers to become entrenched in niches and could ultimately decrease the ability of our biodefense programs to rapidly respond to emerging or evolving threats. Thus, strict adherence to a science-based justification for research could ultimately lead to a program that is more academic and less relevant to real world threats.

There remains a third option: if research justifications determined solely by intelligence or scientific hypotheses are each insufficient to address national requirements in the area of threat assessment research, then an ideal process may require integration of the first two options. A threshold that is determined by scientific rigor and guided by intelligence reporting may permit threat assessment researchers to benefit from the strengths of both methods while minimizing the potential for limitations to impede their work. This strategy would require threat assessment researchers to interact closely with intelligence professionals trained in the biological sciences. Researchers could incorporate concepts from BW threat assessments into their project proposals and permit the threat to frame their hypotheses; however, they would not be constrained to adhere to archaic or flawed methodologies simply because they are the only processes outlined in intelligence reporting. Rather, the intelligence component of the threshold could possibly be tied to "worst case" assessments based in part upon the biotechnology capabilities of foreign states or organizations of concern. In this context, the onus is on the threat assessment researcher to propose relevant studies that will provide insight regarding the technical aspects of the threat. Ultimately, the threshold for research, although probably not quantitative, should incorporate intellectual creativity and flexibility of experimental design while reflecting the key concerns of intelligence professionals.

ENSURING THE QUALITY OF RESEARCH

Threat assessment research programs will not only encounter close scrutiny from individuals suspicious of offensive developments, but the level of scientific quality of such research may be questioned as well. Many leading life science researchers may be skeptical of the analytic rigor and experimental methodologies applied by scientists that choose to investigate those aspects of biology that could be misused to enable traditional or advanced biological weapons threats. This skepticism may be compounded by the fact that some research will likely be classified, occur at a few facilities across the country, and be largely performed by scientists that are either employed by the federal government directly or through contracts. These factors could leave the threat assessment research community open to the misperception by the general life science community that it represents a compartmented discipline not directly related to general research. Nearly all life scientists embrace the principles of openness and transparency regarding all research activities; mischaracterization of threat assessment research as completely antithetical to such openness might hinder relationships among its researchers with the larger life science community. In order to challenge skeptical opinion, threat assessment research programs will need to incorporate mechanisms to ensure quality control and engage life scientists in academia and industry. Fortunately, the confidence-building mechanisms to ensure BWC compliance will also present opportunities to directly benefit the quality of the science.

The creation of the external oversight committee (OC) would provide a mechanism for quality control of scientific activities. Not only can the OC provide oversight of individual research initiatives for security, but it could also present critical insight regarding the technical merits of research proposals. As highly respected researchers from academia and industry, OC members would possess the necessary background and expertise to perform peer review of research proposals. As a body with responsibility for oversight, the OC would be empowered to ensure that research activities meet an appropriate level of scientific rigor and could provide external support by endorsing the quality and reliability of federal threat assessment programs before the general life science community at meetings and symposia. Ultimately, OC involvement could provide federal threat assessment research with a legitimacy that should appease all but the staunchest life science skeptics.

In addition to external oversight, the federal government will need to ensure that it recruits and retains talented researchers to manage and execute threat assessment studies. The government will have a small pool of talented researchers with germane experience that are immediately available from the Departments of Energy, Agriculture, Defense, and Health and Human services. However, because bioresearch expertise within the government is relatively thin, recruitment of experts from external sources will also be critical. Initially, contract research support could fill some of the gaps; however, creation of a sustained, high-quality, long term research capability would benefit from a core of expertise that resides within the government. To keep the core from stagnating, it should be immersed in a permeable work environment that provides opportunities for close interaction with a wide range of experts. Thus, those responsible for creating and managing research programs will likely need to pursue a variety of options for recruiting and retaining top scientists in a manner that permits the flexibility and inclusion of new technologies that are associated with “cutting edge” research facilities.

Naturally, standard employment issues such as compensation, benefits, work environment, and conditions will be factors that impact the quality of core researchers. Existing options for recruiting young talent to federal laboratories, such as the National Academies’ Research Associateship Programs,[125] should also be considered. Importantly, opportunities for research should not be limited to adaptation of policies that are already standard for federal laboratories; rather, innovative approaches should also be embraced. One such option for ensuring revitalization of expertise would be the creation of temporary positions intended for visiting researchers who can impart a new technology or capability. In another option, threat assessment facilities could have funds available to contract specific studies out to established academic researchers with critical expertise or capability. Although these options may provide some opportunities to encourage direct participation of researchers whose knowledge and expertise could be a significant contribution, other options towards the same end likely exist and should probably be

[125] Information available at URL: <http: //www4.nas.edu/pga/rap.nsf/WebDocuments/ Home+Page>.

considered as well. Creation of recruiting and retention policies competitive with opportunities in academia and industry will be necessary to ensure the high-caliber workforce that is an essential cornerstone of any high-quality scientific enterprise.

COMMUNICATION OF RESEARCH FINDINGS

The vast majority of threat assessment research likely will be directed toward the physical characterization of microorganisms traditionally associated with BW. Examples of this research could include the sensitivity of microorganisms to ultraviolet radiation or their survival under a variety of environmental conditions. In addition, basic studies related to production methodologies and characterization/extrapolation of the infectious (ID_{50}) and lethal doses (LD_{50}) of specific microorganisms to assess their potential to present a BW threat will likely be performed to address the needs of the national security and biodefense communities. In this manner, threat assessment research will support intelligence assessments and enhance the accuracy of simulations used in response and crisis management scenarios. Threat assessment research studies may also have significant benefits to life scientists developing medical countermeasures. Communication of research findings among threats assessment researchers, modelers, and intelligence analysts is unlikely to be impeded or restricted based upon security concerns. However, the scientific community generally has less access to secured or sensitive information than do intelligence or modeling professionals. Thus, in the interest of national biodefense, most threat assessment research activities and findings should be communicated openly.

Advances in the life sciences have historically been fostered by the open communication of research activities and findings. However, some research targeted to provide technical insight regarding BW threats may have potential to support nefarious activities to a level that exceeds its benefit to the general life science community. Thus, it is likely that a small fraction of threat assessment research projects will need to be secured from those who would seek to use the findings to do harm. The federal government has a mechanism for protecting sensitive information through classification, which may be an appropriate method for securing highly sensitive threat assessment studies. However, the issue of classification as it pertains to threat assessment research raises a number of questions regarding which research activities should be subject to classification, the threshold for classifying research, who is responsible for deciding which research should be classified, and whether classification of some research can be consistent with the openness and transparency required to build confidence regarding the lack of offensive intent underlying its genesis. How these questions are addressed will significantly impact the public's perception of federal threat assessment research initiatives and will likely affect the program's overall security and success.

Identifying specific research activities that should be classified will likely be the most important, and most controversial, issue that federal representatives managing threat assessment projects will encounter. However, ongoing discussions within the life science community regarding how an appropriate balance between open communication and national security can be achieved may provide some precedents. For example, the NAS Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology has provided specific recommendations regarding microbiology research activities of a sensitive nature that may require an external security review prior to approval or publication.[126] In addition, the seven recommendations by NAS' Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology for identifying research of concern[127] can further shape guidelines regarding classification. These suggestions could serve as initial guidelines that would need to be expanded as expert initiatives, such as the NAS' current Committee on Advances in Technology and the Prevention of Their Application to Next Generation Biowarfare Threats, consider the potential contributions of other technologies. Investigation of the threat presented by a variety of activities will likely be a goal of threat assessment researchers; as such, guidelines for classifying research projects will need to be even broader than those provided thus far by NAS. Ideally, classification would be reserved for those activities that:

1) Provide BW enabling information to nefarious actors that is not otherwise available from the general scientific community

2) Alert potential adversaries to gaps in or opportunities to circumvent current US countermeasures

3) Compromise the sources or methods of US intelligence agencies.

The threshold for classifying information and research activities will also be a critical factor that will need to be addressed. There are many aspects to a research project including the rationale, research methodologies and materials, data and findings, and conclusions. Depending on the underlying reasons for determining that a specific

[126] Recommendations at URL: <http: //books.nap.edu/html/biotechnology_research/0309089778.pdf >.

[127] Gerald Fink, and others, *Biotechnology Research in an Age of Terrorism* (Washington, DC: The National Academies Press, 2004), 114-15.

research initiative falls within the guidelines for classification, classification of each of the components of that research should be considered independently. For example, if a research project regarding the genetic manipulation of a microorganism falls within the guidelines for classification because it may support the efforts of BW researchers, it may be sufficient to classify only the materials and methods used to engineer the organism. Thus, the existence, rationale, and conclusions of the project can remain unclassified while the information of greatest concern is secured. In a system that appropriately addresses the underlying issue of threshold, identification of classified research projects can be generalized without completely inhibiting the communication of some information pertinent to their activities.

Ultimately, the decision to classify a specific research initiative, either totally or in part, will likely reside with the federal representatives responsible for administrating threat assessment programs. Ideally, this group will possess sufficient familiarity with national security issues and processes to permit classification decisions based upon a rational assessment of the benefits and risks posed by open communication of each study. Decisions regarding classification might further benefit from the insights of leading life science researchers. As an advisory panel of cleared scientists, the OC could assess the potential value of a specific research proposal to the general life sciences community; OC assessments could then be considered along with the other factors relevant to the security assessment. Furthermore, when a research project is initiated in response to a specific intelligence report, intelligence professionals would be best suited to providing classification recommendations sufficient to protect the underlying sources or methods. Together, these options would enhance the ability of federal representatives to make informed decisions regarding research classification. Such an approach would be more flexible and facilitate greater transparency than would a system based simply upon the bureaucratic application of generalized regulations for determining classification.

As discussed earlier, federal threat assessment research activities will require a significant level of transparency to assure both life scientists and international parties that the US is not developing an offensive BW capability. The potential for classification of some research could be viewed as a barrier to transparency and confidence-building. However, provided appropriate groups have had input to the classification process, projects have been evaluated against a series of detailed criteria, and individual components of the projects have been independently classified according to relevant security concerns, the proportion of material that is classified should be exceedingly small. Ideally, an outside observer would be able to access general information regarding virtually all of the research projects under a threat assessment program, if not the specific details, findings, or recommendations of the projects themselves. Nonetheless, regardless the level of detail and variety of options used to minimize the volume of threat assessment research that is classified, there will likely remain a group of life scientists who argue that classification is completely inconsistent with the transparency required to engender confidence in the defensive nature of federal programs. Therefore, it stands to reason that federal policymakers will need to determine the level of transparency that establishes an appropriate equilibrium between confidence-building and national security.

Threat assessment research will be performed to address the specific requirements of the intelligence community and provide basic data on BW threat organisms that can be employed in the discovery and development of countermeasures. Thus, it will be important for researchers to communicate their findings, regardless of classification. Communication of classified findings will likely occur via standard channels of communication currently employed by various organizations of the federal government that traffic in classified material; this process will not benefit from further discussion here. However, the methods by which threat assessment researchers communicate their unclassified findings could potentially impact the transparency and confidence inspired among outside parties. Open communication of unclassified research activities and findings to the general scientific community via its standard mechanisms for interaction would have the greatest potential for positive impact. Thus, threat assessment researchers should be encouraged to publish the bulk of their work in peer-reviewed journals and present their findings at both national and international conferences. In addition, general release of information to the public or press should be encouraged, so long as it follows established procedures that mirror those in other federal agencies. Overall, open dissemination of information pertinent to unclassified research could provide significant credibility to threat assessment research programs.

CONCLUSIONS

The threat presented by misapplication of the life sciences towards employment of micobiological organisms or their toxic products as weapons hold potential to negatively impact the security of humans and our agricultural resources on a scale that ranges from personal to global. As threats of increasing sophistication from state BW programs that seek to incorporate cutting edge biotechnology discoveries are compounded by an expanding base of non-state actors that employ cruder methodologies towards rudimentary but effective BW attacks, intelligence analysts are likely to identify a growing number of diverse threats that will each need to be addressed. In the face of the increasing volume of requirements that may result from such expanding threat lists, the biodefense community will be challenged to optimally allocate its finite resources to achieve parity with the threat. Thus, a mechanism for prioritizing BW threats to U.S. interests is needed. Such a mechanism could benefit significantly from empirical data regarding the organisms, production methodologies, and dissemination strategies associated with BW; however, despite a handful of decentralized projects, the U.S. has not initiated a concerted program for experimental validation of BW threats. Such a program would provide critical support to further analytic biothreat assessments and biodefense R, D, T, & E activities.

Those charged with the creation of a national biothreat assessment research program will face many challenges that could limit its scope and effectiveness. Not only will such a program need to comply with the regulations laid out by the BWC, but its executors will have to take additional steps to build confidence that research activities are not being directed toward development of an offensive capability. In addition, threat assessment research will require defined guidelines and standards for ensuring projects are responsive to intelligence threat estimates yet remain flexible enough to anticipate those threats that are on the horizon. Also, principles and practices that ensure the highest quality of scientific and analytic rigor in threat assessment research, such as external review of project proposals and efforts to recruit and retain high-quality scientists with cutting-edge expertise, will need to be considered. Furthermore, those that direct research programs will need to develop a strategy for identifying and securing research that should be classified, while at the same time, encouraging openness and transparency regarding research activities. Resolution of these issues will require efforts that could exceed the individual capabilities and expertise of the federal entities responsible for crafting and implementing the national strategy for threat assessment research.

In order to surmount the potential obstacles to implementation of a successful federal threat assessment research program, officials should consider seeking out and incorporating the views of a variety of communities, including those of national security professionals, biodefense experts, life science researchers, science policy experts, and BWC legal experts, among others. Each community will have varying levels of input regarding the mechanics and methodologies of the research program. National security professionals will be able to provide insight to direct or support research efforts; they will also benefit from the findings of threat assessment researchers. Biodefense professionals will likely seek to incorporate research conclusions into their prioritization efforts and may provide a source of external support and insight to research activities. Life science researchers will be a prime source of expertise to provide oversight and evaluate the quality and technical merit of research activities. Science policy experts can help craft policy regarding the activities of threat assessment programs and incorporation of their findings into federal biodefense efforts. BWC legal experts can provide guidance regarding the legality of individual research projects and help craft strategies for building confidence regarding the defensive nature of these activities.

Ultimately, a coordinated federal program for experimental validation of BW threats will require the harmonization of inputs from numerous disparate communities, creation of novel research strategies, and achieve partial resolution of ongoing debates regarding thresholds for communicating or restricting the flow of information of concern. These are daunting tasks that will not be resolved overnight. However, successful implementation of a centralized biothreat assessment program will support both the national security and biodefense communities and will also enhance other efforts by the federal government to craft and implement a national "end-to-end" biodefense strategy.

BIBLIOGRAPHY

Aebersold, R., and M. Mann. Mass Spectrometry-Based Proteomics. *Nature* 422, no. 6928 (13 March 2003): 198-207.

Alberts, B., and R. M. May. "Scientist Support for Biological Weapons Controls." *Science* 298, no. 5596 (8 November 2002): 1135.

Alibek, Kenneth. *Biohazard: The Chilling True Story of the Largest Biological Weapons Program in the World.* New York: Random House, Inc., 1999.

"Al Qaeda-Anthrax Link?" *CBS News.com*, 23 March 2002. URL: <http://www.cbsnews.com/stories/2002/03/23/attack/printable504460.shtml>. Accessed 12 June 2002.

Atlas R. M., and others. "Statement on Scientific Publication and Security." *Science* 299, no. 5610 (21 February 2003): 1149.

________. "Public Health. National Security and the Biological Research Community." *Science* 298, no. 5594 (25 October 2002): 753-754.

Basile, G. "Health Science and National Security." *Science* 295, no. 5562 (15 March 2002): 257.

"Bin-Ladin Front Reportedly Bought CBW from E Europe, FSU." *London Al-Hayah* (in Arabic), 20 April 1999.

"Bin-Ladin Men Reportedly Possess Biological Weapons." *London Al-Sharq al-Awsat* (Internet version-in Arabic), 6 March 1999.

"Bin Laden Sought Nuclear Matter." *Boston Daily Globe*, September 16, 2001. URL: <http://www.boston.com/dailyglobe2/259/nation/Bin_Laden_sought_nuclear_matter+.shtml>. Accessed 14 June 2002.

Block S. M. "Living Nightmares: Biological Threats Enabled by Molecular Biology." In *The New Terror*, S. Drell, and others, eds. Stanford, CA: Hoover Institute Press, 1999, 39-75.

Boismenu, R., and W. L. Havran. "An Innate View of Gamma Delta T Cells. *Current Opinions in Immunology* 9, no. 1 (1997): 57-63.

Boyce, Nell. "Speak No Evil: Should Biologists Publish Work that could be Misused?" *US News and World Report*, 24 June 2002.

Brumfiel, G. "Mission Impossible?" *Nature* 419, no. 6902 (2002): 10-11.

Carroll, M. C., and A. P. Prodeus. "Linkages of Innate and Adaptive Immunity." *Current Opinions in Immunology* 10, no. 1 (1998): 36-40.

Carus, W. S. *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents Since 1900*. Washington D.C: Center for Counterproliferation Research, February 2001.

Cello, J., and others. Chemical Synthesis of Poliovirus cDNA: Generation of Infectious Virus in the Absence of Natural Template. *Science* 297, no. 5583 (9 August 2002): 1016-1018.

Check, E. "Biodefense Plans Earn Lukewarm Response from US Academics." *Nature* 422, no. 6929 (20 March 2003): 245-246.

________. "Biologists Apprehensive over US Moves to Censor Information Flow." *Nature* 415, no. 6874 (21 February 2002): 821.

________. "Journals Tighten Up on Biosecurity." *Nature* 421, no. 6925 (20 February 2003): 774.

________. "US Officials Urge Biologists to Vet Publications for Bioterror Risk." *Nature* 421, no. 6920 (16 Jan 2003): 197.

________. "US Prepares Ground for Security Clampdown." *Nature* 418, no. 6901 (2002): 906.

Clarke, Victoria. "DoD News Briefing." Briefing presented at the Pentagon. Washington, DC, 4 September 2001. URL: <http://www.defenselink.mil/ news/ Sep2001/t09052001_t0904asd.html>. Accessed 16 June 2004.

Cochrane, Rexmond C. *The National Academies of Sciences: The First Hundred Years, 1863-1963*. Washington, D.C.: National Academy of Sciences, 1978.

Colton, R. J., and J. N. Russell, Jr. "Counterterrorism: Making the World a Safer Place." *Science* 299, no. 5611 (28 February 2003): 457.

Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction. 10 April 1972. URL: <http://www.opbw.org/convention/documents/btwctext.pdf>. Accessed 15 June 2004.

Couzin, J. "Bioterrorism. A Call for Restraint on Biological Data." *Science* 297, 5582 (2 August 2002): 749-751.

Crampton, J. M., and others. Model Systems to Evaluate the Use of Transgenic Haematophagous Insects to Deliver Protective Vaccines. *Parassitologia* 41, nos. 1-3 (1999): 473-477.

Crawford, R. M., and others. "Macrophage Activation: a Riddle of Immunological Resistance." *Immunology Seminars* 60 (1996): 29-46.

Cummings, C. A., and D. A. Relman. "Genomics and Microbiology. Microbial Forensics – 'Cross-Examining Pathogens'." *Science* 296, no. 5575 (14 June 2002): 1976-1979.

Director of Central Intelligence. Worldwide Threat Assessment Briefing to the Senate Select Committee on Intelligence by the Director of Central Intelligence, John M. Deutch. 1996. URL: <http://www.fas.org/irp/congress/1996_hr/s960222p.htm>. Accessed 18 June 2002.

Enserink, M. "Science and Security. Entering the Twilight Zone of what material to Censor." *Science* 298, no. 5598 (22 November 2002): 1548.

Epstein, G. L. "Controlling Biological Warfare Threats: Resolving Potential Tensions among the Research Community, Industry, and the National Security Community." *Critical Reviews in Microbiology* 27, no. 4 (2001): 321-354.

________. "Bioresponsibility: Engaging the Scientific Community in Reducing the Biological Weapons Threat." *BioScience* 52, no. 5 (May 2002).

Falkow, S. "Science Publishing and Security Concerns." *Science* 300, no. 5620 (20 May 2003): 737-739.

Finkel, E. "Australia. Engineered Mouse Virus Spurs Bioweapon Fears." *Science* 291, 5504 (26 January 2001): 585.

Floweree, C. C. "The Biological Weapons Convention and the Researcher." *Annals of the New York Academy of Sciences* (31 December 1992): 666.

Fraser, C. M., and M. R. Dando. "Genomics and Future Biological Weapons: The Need for Preventive Action by the Biomedical Community. *Nature Genetics* 29, no. 3 (2001): 253-256.

Fredrickson, D. S. *The Recombinant DNA Controversy, A Memoir: Science, Politics, and the Public Interest, 1974-1984*. Washington, D.C.: ASM Press, 2001).

________. "Asilomar and Recombinant DNA: The End of the Beginning." In *Biomedical Politics*. Washington, DC: National Academy Press, 1991, 258-298.

Gordon, Michael R. "U.S. Says It Found Qaeda Lab Being Built to Produce Anthrax." *New York Times*, 23 March 2002.

Gouvras, G. "The Far Reaching Impact of Bioterrorism: What the European Union is Doing Regarding Deliberate Releases of Biological/Chemical Agents Based upon the Events in the United States." *IEEE Engineering Medical Biology Magazine* 21, no. 5 (September-October 2002): 321-329.

Greenberg, D. S. "Homeland Security is Good and Bad News for US Scientists." *Lancet* 360, no. 9350 (28 December 2002): 2056.

Greenway, T. E., and others. "Induction of Protective Immune Responses against Venezuelan Equine Encephalitis (VEE) Virus Aerosol Challenge with Microencapsulated VEE Virus Vaccine." *Vaccine* 16, no. 13 (1998): 1314-1323.

Hannon, G. J. "RNA Interference." *Nature* 418, no. 6894 (11 July 2002): 244-251.

Hood, L. "Systems Biology: Integrating Technology, Biology and Computation." *Mechanical Ageing Development* 124, no. 1 (2003): 9-16.

Hu, W. S., and V. K. Pathak. "Design of Retroviral Vectors and Helper Cells for Gene Therapy." *Pharmacology Reviews* 52, no. 4 (2000): 493-511.

"Islamic Front Said Ready to use CBW against US, Israel." *London Al-Hayah* (in Arabic), 19 April 1999.

Jackson, R. J., and others. "Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox." *Journal of Virology* 75 (2001): 1205-1210.

James, E., and J. M. Lee. "The Production of Foreign Proteins from Genetically Modified Plant Cells." *Advances in Biochemical Engineering and Biotechnology* 72, (2001): 127-156.

Johnson T. R., J. E. Fischer, and B. S. Graham. "Construction and Characterization of Recombinant Vaccinia Viruses Co-expressing a Respiratory Syncytial Virus Protein and a Cytokine." *Journal of General Virology* 82, no. 9 (2001): 2107-2116.

Kaushansky, K. "Access to the Biomedical Literature: A Stand against Coercion." *Blood* 97, no. 8 (15 April 2001): 18-26.

Keim, P., and others. *Microbial Forensics: A Scientific Assessment.* Washington, DC: American Academy of Microbiology, 2003).

Kennedy, D. "Balancing Terror and Freedom." *Science* 298, no. 5601 (December 2002): 214.

________. "Happy New Year." *Science* 299, no. 5603 (3 January 2003): 329.

________. "Two Cultures." *Science* 299, no. 5610 (21 February 2003): 428.

Kissel, T., and others. "Microencapsulation of Antigens Using Biodegradable Polyesters: Facts and Phantasies." *Behring Institute Mittation* 98 (1997): 172-183.

Kobinger, G. P., and others. "Filovirus-Pseudotyped Lentiviral Vector can Efficiently and Stably Transduce Airway Epithelia in Vivo." *Nature Biotechnology* 19, no. 3 (March 2001): 225-230.

Kun, L. G. "Homeland Security: The Possible, Probable, and Perils of Information Technology. Information Technology is a Key Component in both Defending against and Aiding Terrorism Threats." *IEEE Engineering Medical Biology Magazine* 21, no. 5 (2002): 1121-6.

Kwik, G., and others. "Biosecurity: Responsible Stewardship of Bioscience in an Age of Catastrophic Terrorism." *Biosecurity and Bioterrorism* 1, no. 1 (2003): 27-35.

Leader, Stefan. "Osama Bin Ladin and the Terrorist Search for WMD." *Jane's Intelligence Review*, 1 June 1999.

Leitenberg, M. "Distinguishing Offensive from Defensive Biological Weapons Research." *Critical Reviews in Microbiology* 29, no. 3 (2003): 223-257.

_______. "Biological Weapons in the Twentieth Century: A Review and Analysis." *Critical Reviews in Microbiology* 27, no. 4 (2001): 267-320.

Lichtblau, E. "Response to Terror; Rising Fears that What We Do Know Can Hurt Us." *Los Angeles Times*, 18 November 2001.

MacKenzie, D. "US Develops Lethal New Viruses." *New Scientist*, 29 October 2003.

Malakoff, D. "Bioterrorism. Congress Adopts Tough Rules for Labs." *Science* 296, no. 5573 (31 May 2002): 1585-1587.

________. "Confronting Terrorism. One Year after: Tighter Security Reshapes Research." *Science* 297, no. 5587 (6 September 2002): 265-8.

________. "Counterterrorism. Academics Weigh in on Homeland Defense." *Science* 296, no. 5577 (28 June 2002): 209-11.

________. "Homeland Security. New Agency Contains Strong Science Arm." *Science* 298, no. 5598 (22 November 2002): 321.

________. "National Security. Pentagon Proposal Worries Researchers." *Science* 296, no. 5569 (3 May 2002): 826.

________. "Science and Security. Researchers Urged to Self-Censor Sensitive Data." *Science* 299, no. 5605 (17 January 2003): 321.

________. "Security and Science. Researchers See Progress in Finding the Right Balance." *Science* 298, 5593 (18 October 2002): 529.

Mangold, T., and J. Goldberg. *Plague Wars: The Terrifying Reality of Biological Warfare*. New York, New York: St. Martin's Press, 1999.

Marshall, E. "Counterterrorism. US Enlists Researchers as Fight Widens against Bioterrorism." *Science* 294, no. 5545 (9 November 2001):194.

McCarthy, M., and S. Ramsay. "Fears that Security Rules will Impede US and UK Science." *Lancet* 359, no. 9307 (23 February 2002): 679.

Miller, J. D. "The Attitudes of Religious, Environmental, and Science Policy Leaders toward Biotechnology." *Recombinant DNA Technical Bulletin* 8, no. 4 (1985): 426.

National Academies of Science. *Background Paper on Science and Security in an Age of Terrorism*. Washington, DC: National Academy Press, 2003.

________. "Panel on Scientific Communication and National Security." In *Scientific Communication and National Security*. Washington, DC: National Academy Press, 1982.

Norazmi, M. N. "Possible Mechanism for the Enhanced Lethality of an Interleukin-4-Expressing Mousepox Virus." *Journal of Medical Microbiology* 50, no. 10 (2001): 936.

Paddison, P. J., and others. "Short Hairpin RNAs (shRNAs) Induced Sequence-Specific Silencing in Mammalian Cells." *Genes and Development* 16, no. 8 (15 April 2002): 948-958.

Panofsky, W. K. H. "National Security and Scientific Communication." *Proceedings of the National Academies of Science USA* 97, no. 10 (2002): 1934-1936.

Petro, J., T. Plasse, and J. McNulty. "Biotechnology: Impact on Biological Warfare and Biodefense." *Biosecurity and Bioterrorism* 1, no. 3 (2003): 161-168.

Pines, D. "Science Based Security under Threat." *Nature* 407, no. 6803 (28 September 2000): 326.

Poste, G. "Facing Reality in Preparing for Biological Warfare: a Conversation with George Poste. Interview by Jeff Goldsmith." *Health Affairs* (Millwood); Supp Web Exclusives (2002): W219-28. URL: <http://www.healthaffairs.org/WebExclusives/Goldsmith_Web_Excl_060502.htm>. Accessed 14 April 2003.

"Preparations for BC Attack Viewed." *The Jerusalem Report* (in English), 29 March 1999.

Press, F. *Scientific Communication and National Security*. Washington, DC: National Academy Press, 1982.

Relyea, H. *Silencing Science: National Security Controls and Scientific Communication*. Norwood, NJ: Ablex Publishing Corporation, 1994.

Rindskopf-Parker, E., and L. Gielow-Jacobs "Government Control of Information and Scientific Inquiry." *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 1, no. 2 (2003): 16-24

Rolph M. S., and I. A. Ramshaw. "Interleukin-4-mediated Downregulation of Cytotoxic T Lymphocyte Activity is Associated with Reduced Proliferation of Antigen-specific CD8+ T Cells." *Microbes and Infection* 5, no. 11 (2003): 923-932.

Rosengard, A., and others. "Variola Virus Immune Evasion Design: Expression of a Highly Efficient Inhibitor of Human Complement." *Proceedings of the National Academies of Sciences of the United States of America* 99 (25 June 2002): 8808-8813.

Rumsfeld, Donald. *Quadrennial Defense Review Report. 2001*. Washington, DC: Office of the Secretary of Defense, 2001. URL: <http://www.defenselink.mil/pubs/qdr2001.pdf>. Accessed 14 June 2004.

Russert, Tim. "Interview with Gen. Tommy Franks." *NBC News: Meet the Press*, 24 March 2002. URL: <http://www.centcom.mil/news/transcripts/tim_russert_interview_with_gen.html>. Accessed 15 June 2002.

Shirtliff, M. E., and others. "Molecular Interactions in Biofilms." *Chemistry Biology* 9, no. 8 (2002): 859-871.

Singh, J. A., and P. A. Singer. "Isolationism is not the Answer to Bioterrorism." *Nature* 420, no. 6916 (12 December 2002): 605.

Smithson, A. E. "International Mechanisms for Threat Reduction of Chemical and Biological Weapons." *IEEE Engineering Medical Biology Magazine* 21, no. 5 (2002): 418.

Stephens, C. "Microbiology: Breaking Down Biofilms." *Current Biology* 12, no. 4 (19 February 2002): R132-134.

Stephenson, J. "Biowarfare Warning." *Journal of the American Medical Association* 285, no. 6 (2001): 725.

"Surfing for a Satan Bug. Why Are We Making Life so Easy for Would-Be Terrorists?" *New Scientist* (20 July 2002): 5.

Tenet, G. "Worldwide Threat – Converging Dangers in a Post 9/11 World." Testimony of Director of Central Intelligence George J. Tenet Before the Senate Select Committee on Intelligence (as prepared for delivery) February 6, 2002. URL: <http://www.cia.gov/cia/public_affairs/speeches/dci_speech_02062002.html>. Accessed 12 June 2002.

Toth, C. L. "Keep Tabs on Who Sees What." *Medical Economics* 9, no. 79 (9 December 2002): 213.

Uherek, C., and W. Wels. "DNA-carrier Proteins for Targeted Gene Delivery." *Advances in Drug Delivery Reviews* 44, nos. 2-3 (15 November 2000): 153-166.

Vastag, B. "Openness in Biomedical Research Collides with Heightened Security Concerns." *Journal of the American Medical Association* 289 (12 February 2003): 686, 689-90.

Verrengia J. B. "Science Journals to Join Fight against Terrorists." *Washington Post*, 16 February 2003, A9.

Volchkov, V. E., and others. "Recovery of Infectious Ebola Virus from Complementary DNA: RNA Editing of the GP Gene and Viral Cytotoxicity." *Science* 291, no. 5510 (9 March 2001): 1965-1969.

Wallerstein, Mitchell B. "Science in an Age of Terrorism." *Science* 297, no. 5590 (27 September 2002): 2169.

Wassef, N. M., C. R. Alving, and R. L. Richards. "Liposomes as Carriers for Vaccines." *Immunomethods* 4, no. 3 (1994): 217-222.

Weiss, R. "Polio-Causing Virus Created in N.Y. Lab: Made-from-Scratch Pathogen Prompts Concerns about Bioethics." *The Washington Post*, 12 July 2002.

Westphal, S. P. "Ebola Virus Could be Synthesized." *New Scientist*, 17 July 2002.

Westwick, Peter J. "In the Beginning: The Origin of Nuclear Secrecy." *Bulletin of the Atomic Scientists* 56 (November, December 2000): 43-49.

Whitney, A. R., and others. "Individuality and Variation in Gene Expression Patterns in Human Blood." *Proceedings of the National Academies of Sciences USA* 100, no. 4 (18 February 2003): 1896-1901.

Zilinskas, R. "Iraq's Biological Weapons. The Past as Future?" *Journal of the American Medical Association* 278, no. 5 (6 August 1997): 418-424.

Zilinskas, Raymond A., and Jonathan B. Tucker. "Limiting the Contribution of the Open Scientific Literature to the Biological Weapons Threat." Homeland Security website, URL: <http://www.homelandsecurity.org/journal/Articles/tucker.html>. Accessed 21 December 2002.

Zilinskas, Raymond A., and T. Wilson. "The Microbiologist and Biological Defense Research. Ethics, Politics, and International Security. Introduction." *Annals of the NY Academy of Sciences* 666 (31 December 1992): xi-xvii.