International Journal of Intelligence and CounterIntelligence

ISSN: 0885-0607 (Print) 1521-0561 (Online) Journal homepage: http://www.tandfonline.com/loi/ujic20

Managing Emerging Health Security Threats Since 9/11: The Role of Intelligence

Patrick F. Walsh

To cite this article: Patrick F. Walsh (2016) Managing Emerging Health Security Threats Since 9/11: The Role of Intelligence, International Journal of Intelligence and CounterIntelligence, 29:2, 341-367

To link to this article: http://dx.doi.org/10.1080/08850607.2016.1121048

Published online: 28 Jan 2016.

International Journal of Intelligence and CounterIntelligence, 29: 341–367, 2016

ISSN: 0885-0607 print/1521-0561 online
DOI: 10.1080/08850607.2016.1121048

Routledge
Taylor & Francis Group

PATRICK F. WALSH

Managing Emerging Health Security Threats Since 9/11: The Role of Intelligence

The health and broader biosecurity environment has evolved dramatically since 11 September 2001 (9/11). Less clear is the role intelligence should play in understanding emerging bio-threats. Understanding the role and limitations of intelligence in interpreting a complex set of potential "bio-threats" is essential as advances in synthetic biology and biotechnology grow exponentially. Questions remain, however, as to how well intelligence can function in managing this environment in ways that can reduce both the uncertainty and impact of health/biosecurity related risks and threats for policymakers, first responders, security managers, and public health officers.

Dr. Patrick F. Walsh, a former intelligence analyst, has worked in Australia's national security and law enforcement intelligence environments. He is now an Associate Professor on Intelligence and Security Studies at the Australian Graduate School of Policing and Security, Charles Sturt University, Australia. He is course coordinator for its post-graduate intelligence analysis program and has taught widely across Australia and internationally. Dr. Walsh is also a consultant to government agencies on intelligence reform and capability issues. His book, Intelligence and Intelligence Analysis *(Abingdon, UK: Routledge, 2011), examines a range of intelligence reform issues post-9/11 across Australia, Canada, New Zealand, the United States, and the United Kingdom.*

CONCEPTUALIZING THE HEALTH AND BIOSECURITY AGENDA

Health Security

A brief exploration of some key terminology, namely ''health security'' and ''biosecurity,'' is warranted. Debates are ongoing among academics, policymakers, and scientists about what constitutes ''biosecurity'' as opposed to ''health security.'' Though such debates may seem trivial, they matter because they determine what is considered a ''bio-threat and risk'' and whether a biological agent represents a security and/or a public health issue. While the intentional or unintentional release of a dangerous pathogen like anthrax may involve health and law enforcement officials, the mixture of resources required from security/law enforcement or public health agencies will vary if the threat is not a criminally intentional act. Defining health security/biosecurity, therefore, depends also on the extent to which biological agents become ''securitized'' and by whom.

William Aldis has provided a useful discussion on the lack of agreement and understanding, particularly between developed and developing countries, on the concept of health security. He stated that the term ''health security,'' like ''biosecurity,'' ''sits at the intersection of several disciplines which do not share a common methodology (e.g., practitioners from security studies, foreign policy, IR [international relations], development theory and practice of UN agencies).''[1] As in biosecurity, inconsistencies arise in how health security is defined. Kenneth Bernard has referred to a ''tribalism'' between the public health and security sectors which has prevented both from understanding each other and perceiving common priorities.[2] While some ''tribalism'' may exist between public health and security sectors, a greater connectivity and understanding has developed more recently between each ''tribe.'' For example, by the 1990s and onwards, global infectious diseases such as HIV/AIDS, SARs, Avian Flu, and the most recent Ebola outbreak in Western Africa have ''acquired a greater security salience in world politics.''[3] In addition, other perspectives, not from the traditional International Relations and Strategic Studies worlds, such as medical sociology, also remind those working in the intelligence, national security, and law enforcements worlds that, while health may have become securitized, so too has security to some extent become '''medicalized.'' As Stefan Elbe correctly points out, ''the task of securing populations cannot rely solely on the traditional institutions of security such as the police, intelligence services and armed forces.''[4] The health security literature makes clear that the concept of security is in a flux and continues to mean different things to different discipline audiences.[5] Arguably, ''global (public) health security,'' ''national security,'' ''human security,'' and ''biosecurity,'' while contested terms in themselves, are all components of a broader ''super discipline'' of health

security. While defining ''biosecurity'' and ''biosecurity threats'' remains problematic, the health security literature shows that it is inextricably linked to the broader global health literature as much as it connects with the ''traditional'' national security and law enforcement contexts.[6] Perhaps biosecurity can then be seen as the link between those who focus on the *criminal exploitation of health* and those who focus on other aspects of the public health security discipline, such as, but not limited to, pandemic security. In summary, health security remains poorly defined—as does ''biosecurity.'' Nonetheless, the activities, policy, and research associated with both are by necessity linked. The focus here is on defining biosecurity and restricting discussion to the role of intelligence in managing biosecurity threats since 9/11.

BIOSECURITY

Gregory Koblentz has summarized the difficulties associated with defining biosecurity, arguing that it has ''specific'' meanings within different disciplines. He sees four competing definitions of the word.[7] The first consists of threats to animal, and plant health, and bio-diversity, that may have an indirect effect on human health.[8] The second definition arose in the 1990s ''in response to the threat of biological terrorism.''[9] The third relates to monitoring dual use biological research, meaning research that has a legitimate scientific purpose (for example, vaccine research), but may be misused and therefore present a bio-threat to public health and national security. The fourth definition listed by Koblentz was developed by the U.S. National Academies of Science (NAS) and is an amalgamation of the other three. The NAS defines biosecurity as ''security against the inadvertent, inappropriate, or intentional malicious or malevolent use of potentially dangerous biological agents or biotechnology, including the development, production, stockpiling, or use of biological weapons as well as outbreaks of newly emergent and epidemic disease.''[10]

The National Academies' definition reflects in part the human security agenda that emerged in the mid-1990s, which argued for a broadening of what constitutes ''national security'' beyond merely the prevention or prosecution of wars between states to also include the security of individuals within and between states.[11] Adherents of the human security agenda view the term ''national security'' as including the protection of people within states from political violence (terrorism, civil war, state collapse), economic vulnerabilities, and even disease and natural disasters.[12]

But the broader all-inclusive definitions have their disadvantages. One is that they are so broad that individual disciplines return back to their own meanings of the word ''biosecurity'' when working with threats in their contexts. For example, animal health specialists will continue to have a different

understanding of what constitutes a biosecurity threat in their working environment than their counterparts in a national security intelligence agency.[13] The "biosecurity label" is, therefore, really a classifier for what is a broad church of related disciplines, among them botanists, microbiologists, virologists, veterinarians, physicians, laboratory bio-safety officers, and national security analysts/investigators. This cross-disciplinary focus is both a strength and weakness to understanding biosecurity threats. It is a weakness in that the presence of multiple players in the biosecurity field can result in a more fragmented understanding and operational response to various biosecurity threats. But it is also a strength in that, if intelligence systems are optimal, a multi-disciplinary approach allows a combination of expertise to assess and manage the bio-threat or risk. This is because bio-threats—whether they are intentional or unintentional in origin—can cross multiple dimensions (plant, animal, and human health), which in turn requires both a multi-disciplinary interpretation of the "threat" and treatment of any ensuing risks. This examination of the multiple dimensions of biosecurity across the health spectrum (plant, animal, and human health) has been described in policy circles as the "one health approach."[14]

In summary, no optimal definitions of biosecurity are agreeable to all disciplines working in this field. Here the word biosecurity will be used when referring to threats that include those that are intentional (from "weaponizing" dangerous biological material—bacteria, viruses, and toxins), the deliberate misuse of dual-use bio-technologies, and other threats that are unintentional, arising from a diverse range of pathogens that threaten the food supply and the environment.[15] While naturally occurring or emerging infectious diseases are a critical part of the bio-threat and health security spectrum, the focus here is exclusively on those bio-threats resulting from the intentional or unintentional (such as bio-safety violations) use by individuals or groups of biological agents.

THE POST-9/11 BIOSECURITY THREAT ENVIRONMENT

Understanding today's biosecurity threat environment requires a brief contextual understanding of how threats have evolved since 1945. Starting a survey of bio-threats at 1945 may seem a bit arbitrary given that historians and scientists contend that diseases, whether naturally occurring or used as "weapons," have for centuries had a major impact on the political and cultural history of humans.[16] But the year 1945 parallels the development of modern microbiology, and the ability of states to use technology to "industrialize" various biological agents as weapons. At the end of World War II, developments in industrial microbiology and advances in the aerolization of biological agents made weaponizing them a more accurate and lethal option for states that chose to develop them.

State-based biological weapons programs, particularly those developed by the major Cold War protagonists, the former Soviet Union and the United States—from 1945 until the 1970s for the U.S., and up to the 1990s for the Soviet Union—dominated policymakers' understanding and framing of the bio-threat environment. These large, industrial programs produced vast quantities of such dangerous pathogens as highly virulent anthrax, plague, and tularemia.[17] According to Ken Alibek's account of his time as the chief scientist of the Soviet biological weapons, just one of its six biological weapons production facilities at Stepnogorsk, in Kazakhstan, contained ten 20,000-liter fermenters capable of producing 1000 tons of anthrax per year.[18] But concern was also raised from 1945 and throughout the Cold War that other less stable or rogue states (among them Iraq, Iran, Syria, and North Korea) were seeking to develop biological weapons.[19]

By 1990, Iraq's Saddam Hussein regime had tested and weaponized anthrax and botulinum toxin, using 400-kilogram aerial bombs and al-Hussein warheads. By the end of the first Gulf War in 1991, as United Nations (UN) weapons teams moved into Iraq, the Iraqi regime destroyed its bulk supply of biological agents and munitions.[20]

During the mid-1990s, policymakers started to shift their focus from historical and traditional notions of bio-threats (state-sponsored conventional biological weapons programs) to the use of biological agents by non-state actors, primarily terrorists. Gregory Koblentz provides a useful explanation of how ''bio-terrorism'' became the policy priority during this period. In summary, three events, spanning the 1990s and up to 2001, helped recast policymakers' understanding of the bio-threat from non-state actors.[21]

The first occurred in 1995 when the Japanese doomsday cult Aum Shinrikyo released sarin nerve gas into the Tokyo subway system, killing 12 people and injuring 5000 more. Although the cult is most remembered for its development of a crude chemical weapon, it was also attempting to weaponize anthrax.[22] The second event was the discovery by U.S. soldiers after the 2001 invasion of Afghanistan of technical documents and equipment in a biological weapons laboratory under construction near Kandahar. Since 1998, Osama bin Laden had made statements that the ''acquisition of WMD was a 'religious duty.'''[23] In his memoirs, former Director of Central Intelligence George J. Tenet provided further details on two individuals, Rauf Ahmad and Yazid Sufaat, who were recruited by al-Qaeda's then second-in-charge Ayman al-Zawahiri to develop this capability.[24] Both events also showed that the groups involved lacked, particularly in the Aum Shinrikyo case, the full complement of ''scientific and technological skills that would have helped ensure their success.''[25]

In contrast to al-Qaeda's general lack of advanced knowledge and skills in pursuing biological weapons, the third bio-terror event involved the 2001

release of anthrax spores in the U.S. mail system. It showed the lethality of biological agents when developed by individuals or groups who do possess the expertise to produce and weaponize dangerous pathogens. In September and October 2001, seven envelopes containing a dried powder form of anthrax spores were posted to several media outlets and to the U.S. Senate offices of Senators Thomas Daschle (D-South Dakota) and Patrick Leahy (D-Vermont). The letters resulted in 22 cases of anthrax, five leading to a fatal inhalation. The anthrax letters also resulted in the contamination and closure of several major U.S. post offices.

In contrast to attempts made by Aum Shinrikyo and al-Qaeda to use anthrax as biological weapons, the Federal Bureau of Investigation (FBI) investigation revealed that the anthrax used in this attack was a highly concentrated, aerolizable ''weapons grade'' form of this bacteria. The subsequent seven-year investigation was complex and protracted, and resulted in the U.S. Department of Justice determining that a single spore batch created by anthrax specialist Dr. Bruce E. Ivins at the U.S. Army Medical Research Institute of Infectious Diseases (USAMRID) was the parent material for the letter spores. In July 2008, Ivins committed suicide before being indicted.[26]

The Ivins case was significant on a number of fronts. It underlined the tremendous skill required to produce biological agents in sufficient pure and aerolized quantities. Ivins had been an anthrax expert for over two decades, yet the FBI's case against him documents that, despite his extensive knowledge and the optimal laboratory conditions, he was confronted with challenges in producing the anthrax thought responsible for the attack. This fact helped recalibrate policymakers' understanding of the relative difficulty for a terrorist to produce a ''biological bomb.'' This may have been comforting to some policymakers, though it did raise another bio-threat scenario—namely that the terrorists may not be outsiders, but rather insiders—even more concerning than a scientist capable of developing a biological weapon.

The fact that the ''attacker'' had been a scientist with access to highly-controlled dangerous biological agents focused intelligence agencies on the threats and risks associated with dual-use research and technology.

Other biosecurity issues that have shaped the post 9/11 threat environment have included a litany of ''bio-crimes.'' Bio-crimes denotes a diverse bundle of issues which have in common the use of biological agents by non-state actors as weapons for extortion, murder, or profit rather than for the politically-motivated reasons seen in bioterrorism. A 2001 study by Seth Carus attempted to delineate between the motives of bio-terrorists and those of bio-criminals by surveying major cases of each dating back to 1900. He concluded that, in contrast to bio-terrorism, bio-criminal attacks

tend to be aimed at individuals or small groups using crude means of dissemination (for example, food contamination, murder of spouses using ricin, or illegal injection of pathogens [HIV] to a victim).[27]

In reality, a ''lack of professional consensus'' persists on the differences between these two threat classes, and ''perceptions of the threat'' continue to evolve. For example, Tim Inglis and colleagues tend to lump together a number of bio-threats across the bio-criminal and bio-terrorism space.[28]

The bio-criminal threat landscape has shifted, however, since the 2011 Carus study that focused primarily on small, individually motivated bio-attacks by criminals. Global food quality, environmental pressures, and companies seeking to ''cut corners'' currently present another layer of more complex bio-criminal threats with potentially greater economic and public health impacts beyond individuals—to groups and nations.[29] Similarly, in countries with large primary industry sectors, such as Australia and New Zealand, the organized, criminal manipulation of regulations concerning export/import markets, and the criminal introduction of a controlled plant or animal species, represent serious biosecurity threats to these economies.

EMERGING BIOSECURITY THREATS AND INTELLIGENCE

The list of potential threats seems endless. Analyzing them thematically is easier within two broad thematic bio-threat areas. The first, ''stolen biological agents,'' includes material stolen from a supplier, a university, research laboratory, hospital, or animal health facility. The second is ''dual-use research and synthetic biology.''

The events of 9/11 and the anthrax letter attack of that period resulted in numerous changes of policy, legislation, and codes of ethics aimed at enhancing the control and access to dangerous biological agents and toxins in the U.S., Australia, Canada, UK, and the EU.[30] The enactment of the USA Patriot Act of 2001 and the Public Health Security and Bio-Terrorism Preparedness and Response Act of 2002 were influential in requiring the registration of persons allowed to work with potentially dangerous biological agents.

Further initiatives such as Biological Surety, the National Academies Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, chaired by Gerald Fink in 2004, also played a role in identifying internal risks posed by those working in secure laboratories.[31] These initiatives collectively provided guidance on how to improve internal oversight, including background checks on scientists, as well as other safety protocols that appropriately risk-managed the access to, and production and transfer of, dangerous pathogens.

Stolen Biological Agents

Leaving aside the investigation into microbiologist Bruce Ivins and the anthrax postal incident of 2001 discussed earlier, the ''insider threat'' of a scientist stealing or conspiring to steal a controlled biological agent appears to date to be both rare and extremely difficult to detect.[32] The increased policy and biosafety regulatory environments for the operation of BSL-3 and BSL-4 laboratories now make it more difficult than in 2001 for both unintentional accidents in the workplace and the theft of pathogens. BSL-3 and BSL-4 laboratories are the two most secure bio-safety lab designations. These labs have in place strict guidelines prescribing the physical layout, safety equipment, and the training of scientific staff who work in them, though arguably no safety guidelines can avoid all unintentional incidents. For example, in 2014, several safety breaches involving potential bioterrorism agents occurred, including the accidental exposure of scientists to anthrax, bird flu virus, and the discovery of previously forgotten unsecured smallpox samples.[33] Such safety breaches, though not reflecting any intentional ''insider'' threat behavior, underscore vulnerabilities in procedures that could be exploited by adversaries with malevolent intentions. Despite the new bio-safety measures that have been put in place, predicting and detecting if someone has the intent and capability to steal a biological agent from a secure lab site for profit, political motivation, or due to a mental health issue, remains difficult.[34]

Background checks on scientists may assist in flagging staff who present security risks prior to their appointment, though this process cannot completely screen out individuals whose intentions change later in their careers in ways that present challenges to security. The motivation for individuals to criminally use biological agents from secure labs will likely differ individually.[35]

From a bio-criminal perspective, where profit rather than ideology is the motive, the intent to commit the theft depends on the nature of the agent potentially available to the criminal conspirators, and how quickly the act can be turned into a ''profit.''[36] In most Western countries such as Australia, Canada, New Zealand, the UK, and the U.S., stealing a controlled biological agent such as anthrax from a BSL-3 or -4 private or government lab, while not impossible, presents several security challenges, in terms of physical security barriers and exposure risks, for a criminal gang interested in such an enterprise.[37]

The 2001 Ivins case also revealed the genetic sequence analysis of the Ames strain of anthrax used in that attack, thus making possible the tracing of some of these substances back to their source, and enabling investigators to identify which laboratories they came from and ultimately who was

working with them. The theft of controlled biological agents from secure labs thus becomes a high risk venture for the individual or any organized crime group involved. The motivation of most crime groups is to make ''a quick buck'' through traditional revenue pathways such as drugs, fraud, and money laundering where the risks of detection are comparatively less. An easier proposition for a sophisticated criminal or syndicate may be the theft of new scientific breakthroughs (or research intellectual property), either directly from a laboratory computer or by hacking into a secure database. These illicit activities may carry less risk, be more attractive financially, and logistically easier to commit then the theft of a controlled biological substance from a high-containment lab. Similarly, while making threats to ''use'' biological agents as weapons may create the psychological terror sought by terrorists, exacting harm on innocent targets can still be more efficiently and cheaply achieved using simple homemade devices, such as the kitchen pressure cookers used by the Tsarnaev brothers in the 2013 Boston bombings.[38] Certainly, physical security, biosafety procedures, and vetting lab personnel may help mitigate many threats. Additional analysis of previous individuals or groups involving biological substances or scientific institutions, required to better understand how similar threats may evolve, can proceed, as Ryan Burnette has described, along three development phases: intent, ability, and opportunity. With this knowledge, better threat assessment tools can be developed to help security and law enforcement agencies interrupt the development of a threat at each of the three stages.[39]

The theft of biological agents may be most vulnerable to criminal exploitation in the laboratories of developing countries if physical security is not optimal, or if scientists perceive that they are not adequately remunerated for the research they do. In addition to difficulties assessing intent/motivation, measuring the consequence of a theft of a Category A pathogen from a BSL-4 lab is also very difficult. Part of this difficulty goes back to motivation. Is the objective of the theft to merely pose a threat to a community or to extort funds from a government without the intention of actually using the substance? Or is the intention that the pathogen be weaponized and disseminated at ports, truck stops, or airports? Leaving aside issues such as atmospheric temperature, sunlight, and choice of dissemination vehicle, other variables which impact on the overall pathogenicity and ''contagion dynamics'' of dangerous pathogens into a locality are also at play. While a research agenda into epidemiological modelling is active, predicting ''the likelihood of a global pandemic, and to mitigate its consequences,'' remains difficult.[40] A reminder of how difficult is accurately predicting the outbreak or modelling of an epidemic became evident with the 2014 Ebola outbreak in Africa.

Dual Use Research and Synthetic Biology

Though the theft of well-known and controlled pathogens such as anthrax from a BSL-4 laboratory now seems less likely, debates continue about how dual use research and synthetic biology might create a number of potential emerging threats, risks, and vulnerabilities. Such threats may arise from two sources. First are the concerns that highly skilled and trained individuals could use their knowledge to create biological agents under the guise of legitimate research for illegitimate ends. The second source consists of interested ''outsiders'' exploiting legitimate advances in conventional biological research, synthetic biological sciences, and bio-technology for illegitimate purposes. Both pathways to potentially new bio-threats underline concerns about dual use technology. Each pathway also defines the key dimensions of ''dual use research,'' but in reality this term has been defined in many ways in science, policy, and security circles.[41] Herein, ''dual use research'' is defined as that which is largely focused on the research of dangerous biological agents that might be weaponized, and the publication of that research, which theoretically could be disseminated to bio-criminals or terrorists for their own nefarious objectives.

In recent years, the published results of dual use research have captured the attention of the biosecurity policy community and the media—perhaps even more than the experiments themselves. Catriona McLeish and Paul Nightingale have argued that starting in the early 2000s the publication of three papers: ''one on the synthesis of polio virus cDNA without a natural template by Cello et al., (2002), the second on how the variola virus (smallpox) can invade the immune system by Rosengard et al., (2002), and a third on overcoming resistance to mouse-pox by Jackson et al., (2001), were widely interpreted as publishing blueprints for terrorists and led to public calls for changes to research and publication procedures.''[42]

Subsequent publications, have raised security concerns about dual use research.[43] Later, two separate items, an article one in 2012 and a letter in August 2013, raised security concerns about whether the published outcomes of research could be used for such illegitimate reasons as bio-terrorism.[44] The 2012 article showed how scientists were able to identify the genetic changes needed for the avian influenza H5N1 to be efficiently transmitted between ferrets—acting as surrogates for human-to-human transmission.

In this research, the U.S. National Science Advisory Board for Biosecurity (NSABB) had to determine whether the benefits of such research outweighed the risk of the accidental or intentional release of a lethal new virus. In November 2011, the NSABB recommended that the two articles arising from this research be redacted, though they were later published.[45] The

publication ordeal regarding the H5N1 research article showed the ongoing challenges in both identifying and overseeing dual use research. Questions about what experiments may be too risky to perform and the publication of the results and how governments effectively manage this risk remain unclear. The debate over gain-of-function experiments on the avian influenza virus H7N9 continues between government regulators and scientists.[46] In October 2014, the White House Office of Science and Technology announced a funding moratorium on new gain-of-function studies pending a further review and the development of a national gain-of-function policy, with its report due in 2015.[47] Within the scientific community, two groups have developed—the Cambridge Working Group (concerned about gain-of-function experiments) and Science for Scientists (pro gain-of-function experiments). Both are likely to seek to influence the outcome of the new policy.

These examples of ''sensitive'' dual use research illustrate the potential threats and risks associated with synthetic biology and the manipulation of microbial genetics. The manipulation of naturally occurring viruses like H5N1 to allow them to mutate more easily into hyper-virulent variants that are more easily passed from animals to humans, or humans to humans—and the creation of dangerous pathogens using chemically synthesized genomes—indicate that this kind of knowledge can be put on the radar of interested bio-criminals and terrorists. The rapid advances in biotechnology, or what some describe as the ''industrialization of biology,'' can result in faster, cheaper, and more effective scientific breakthroughs for health, chemical manufacturing, bio-fuels, and mining, but they also highlight several other newer threat scenarios for criminal or terrorist exploitation.[48]

Concern exists among biosecurity regulators and national security intelligence agencies that not only knowledge is on offer, but also that some of the equipment and technology (used chiefly in the past by scientists working on government-funded research projects in BSL-3 and -4 labs), is becoming more available to the wider public. The increased growth of biotechnology and the growing accessibility of automated biological techniques and relatively inexpensive equipment (such as that used in DNA sequencing and synthesis) make scientific experimentation accessible in ways it wasn't even a decade ago to ''citizen scientists'' or people interested in DIY (''do it yourself'') Bio.[49] To illustrate this point, the entire human genome was sequenced in 2003. A team of scientists required 13 years and nearly a half-billion dollars to identify the approximately 20,500 genes in humans. In contrast, today's companies such as Life Technologies claim that they can decode a human genome sequence in a day for only $1000 using smaller equipment (such as a benchtop Ion Proton Sequencer) that can be ordered from them.[50] Other

DNA sequences from deadly pathogens can also be bought online. For example, in 2006 a journalist from the *Guardian* was able to purchase online a short sequence of the smallpox DNA.[51]

A 2006 U.S. National Research Council report, *Globalization, Biosecurity and the Future of the Life Sciences*, provided a detailed summary of both the global drivers and trajectories of advanced life science technologies that raise biosecurity concerns.[52] In fact, the list of potential biotechnological threat scenarios may be endless due to the overlapping skills and technologies involved with synthetic biology. The evolving nature of some biotechnology also prevents a full threat and risk assessment of the security issues that may arise out of such technology.

Additionally, part of the difficulty in trying to assess the boundaries of biotechnological threat scenarios is that, in many cases, insufficient discussion and analysis has taken place between scientists and their national security counterparts as to the rationale for assessing an issue as a threat or risk. To provide some context of what threats may be possible, Marc Goodman and Andrew Hessel surveyed a number of scenarios, including what they referred to as bad bio-technologists, biological spam, phishing for DNA, identity theft, piracy, and spear phishing. Discussion here will be restricted to three—bad bio-technologists, identity theft, and piracy—to illustrate how they assess this evolving threat environment.[53]

Regarding ''bad bio-technologists,'' Goodman and Hessel argued that, over the past decade, given the increasing number of biotech companies and people working in this field, statistics alone suggest the likelihood of a few ''lunatics'' with intentions to cause harm. Their analysis has been supported by other biosecurity specialists, who consider that experts with an intent to cause harm, or ''bio-Unabombers,'' as of more concern than amateurish bio-hackers operating in the suburbs.[54] While enhanced security measures in laboratories now make it more difficult for a scientist to stockpile or steal controlled substances such as anthrax, the DNA codes of many of these, according to Goodman and Hessel, exist in public data bases. Advances in synthetic biology allow the building of synthetic organisms, thereby sidestepping even the safeguards currently in place for protecting select agents stockpiled in secure sites.

The second threat scenario described by Goodman and Hessel, identity theft, is a ''new take'' on an old enabler of crime. They argued that, as countries increase their holdings of DNA in national databases for criminal identification, more opportunities will develop for these to be compromised, resulting in peoples' identities being stolen and enabling identity-related and other crimes. Additionally, they foresaw a confluence of situations, whereby genetic identity theft could enable people to commit such frauds as circumventing health and employment restrictions based on their genetic data. Genetic cloning or impersonation (leaving another

person's DNA at a crime scene) could also frustrate intelligence operations or law enforcement investigations.

The third interesting threat scenario, "biological piracy," presents several security, ethical, policy, and legal challenges that remain largely unaddressed. Goodman and Hessel suggested that a wide variety of biological and genetic materials are likely to be pirated, as digital media has been. The field of synthetic biology, which is working towards developing therapies and treatments for cancers and other diseases, provides opportunities for organized crime groups to provide pirated versions.[55]

Emerging threats need to be examined by addressing both dimensions of threat assessment—intention and capability. But this is where the challenge begins. The industrialization of biology is happening at a dynamic and rapid pace, making difficult any reliable estimates of both the intentions and capabilities of those interested in exploiting biotechnologies for criminal or terrorist reasons. As one recent workshop of experts suggested, "The angles of the attack are almost infinite and very difficult to anticipate."[56]

Part of the challenge relates to the type of analytical framework used by those in the national security communities and by biosecurity researchers to understand threat and risk. Some frameworks argue for a steady linear increase in biotechnology, resulting in a greater access to skills and technology by bio-criminals and bio-terrorists.[57] In contrast, others have adopted frameworks that estimate a less linear increase in biotechnology. They argue that mere access to technology and even "knowhow" does not automatically create either the motivation or the ability for bio-criminals or bio-terrorists to exploit biotechnology for harmful purposes. Adherents to this framework suggest that there is a lot more uncertainty as to how biotechnologies may develop in the future, since other non-technological variables, such as social, economic, and organizational factors, will also influence the growth of technology and the extent to which it is exploited by individuals or groups for nefarious reasons.[58]

Careful consideration of how the biosecurity threat context will evolve must also include an assessment on the likelihood that more individual or group threats will arise, along with the consequences for policymakers and first responders. For example, as biotechnological knowledge becomes increasingly commoditized and equipment less expensive, will the rhetoric of well-established international terrorist groups (such as the al-Qaeda inspired franchises: al-Qaeda in the Arabian Peninsula [AQAP], or al-Shabab, or even Islamic State) declaring an intent to use a virus or bacteria that they have synthesized or acquired via a third party increase? Alternatively, will intentions to use biosynthetic agents be increasingly expressed by less established domestic terrorist groups, or even individuals, each with a different agenda, whether jihadists, ultra-nationalists, anarchists/bio-hackers, or environmentally-motivated individuals?

Not enough cases of bio-terror attacks permit making analytical generalizations about the specific motivations of various groups or the desires of individual to weaponize conventional biological agents. Getting ''into the heads'' of threat actors who are not yet on the radar of intelligence and law enforcement agencies remains extremely difficult.

Doubly difficult is assessing whether bio-criminals and terrorists will have the capabilities to either access or produce harmful biological agents that have been synthesized in a laboratory. In contrast to dealing with the ''intent'' side of the threat equation, some intelligence agencies with mandates to assess the threat and risk of bio-weapons have done a lot more work on estimating the capabilities required by an individual or group in weaponizing various biological agents, including those resulting from genetic engineering or biotechnology. Of course, much of this is classified, but the focus is on the level of expertise and equipment required to operationalize different biotechnological-based threat scenarios. This seems to be a useful place to start. If agencies continue to have limited visibility on an individual's intentions prior to an attack, then carefully re-examining variables related to capability (knowledge and equipment) may provide more accurate assessments about the likelihood of various ''high tech bioterrorism threats.''[59] If intelligence agencies can develop a more evidence-based approach to estimating bio-threat capabilities, they will then be better able to provide more accurate assessments to the policymakers, public health, scientists, and security managers responsible for developing strategies that mitigate these threats where possible.

But the difficulty with working on the capability side of the threat formula, meaning knowledge and equipment, is to potentially either over- or under-emphasize both the level of expertise and the margins of difficulty in accessing the equipment required to carry out an attack. Some authors recognize the various technical steps required to synthesize a dangerous pathogen, yet argue that these may be less difficult to overcome than apparent for a ''do it yourself'' biologist/terrorist.[60] Others likely underestimate the threat. For example, during an over-the-horizon scanning project conducted by the U.S. Center for Biosecurity of the UPMC most of the scientists interviewed stated that simple paths exist for skilled individuals to making bio-weapons that ''render more technically difficult approaches unattractive and therefore less likely to be pursued.''[61] Or, as stated in the project teams' report, perhaps in blunter words: ''the bad guys aren't going to waste their time with sophisticated pie in the eye sky stuff.''[62] In most cases, assessing actual capabilities will remain challenging, and an evidence-based approach built over time is needed to avoid over- or under-assessing knowledge, equipment, and skills.

THE ROLE OF INTELLIGENCE IN RESPONDING TO EMERGING BIO-THREATS

The first critical point to make about the role of intelligence in detecting and responding to emerging bio-threats is that it will vary depending on the kind of issue. With some issues intelligence will play a greater role—particularly if some detected ''operational noises'' indicate that a bio-attack is developing. For example, tracking predicate steps towards a planned attack including irregular financial transactions may be possible, or detecting a series of suspicious supply orders for equipment may provide some insights. In other cases of dual-use biology, emerging threat scenarios may still be out of the current collection and analytical bandwidth. In these cases, ''red teaming'' various, potential threat scenarios and developing indicators that would allow some further collection and monitoring becomes important. In these more over-the-horizon cases, a challenge to analytical biases for both under- or overestimating the role of technology in various threats is necessary. A future bio-attack could be as simple as planning a systematic food poisoning of passengers on multiple trans-Atlantic flights over a one-week period. In summary, when thinking about the role of intelligence and early warning, realistic expectations are necessary as to what intelligence capabilities can deliver in such a complex threat environment.

Also necessary is consideration of levels of decisionmaking (i.e., tactical, operational, and strategic) used by intelligence agencies. Whether a national security or a local law enforcement agency, the role of each will depend on the level of decisionmaking support it must address.

The time span for providing strategic intelligence is usually one-to-five years in the future, though in the military context it could be one or two decades. Operational intelligence seeks to determine the commonalities among different threat actors and how best to disrupt them not only individually but collectively, as a category of security threats. Depending on an agency's reach, whether national or local, the time frame for providing operational intelligence could be from weeks to one year, though some complex investigations such as the Bruce Ivins case will take years to complete. Tactical intelligence overlaps with operational intelligence in time frames and focus, though it is generally the kind of intelligence support for decisions being made today, this week, or in less than six months about a specific case under investigation.[63]

The third way to conceptualize the role of intelligence in improving early warning of biosecurity threats is to examine how it can provide warning through various stages of the intelligence cycle, which includes the following stages—direction, collection, analysis, and dissemination. Other intelligence practitioners and scholars might include a longer version of the intelligence cycle and argue for the inclusion of a collation and evaluation

stage, but these additional steps can be subsumed into the cycle's briefer version.[64] For example, collation is an early activity of ''analysis,'' and ''evaluation'' can be part of the dissemination stage, as disseminating intelligence isn't done without thinking how it should be evaluated.

Agencies must consider what they can offer in improving early warning on biosecurity threats by examining how they might be involved at various levels of decisionmaking support and at different stages of the intelligence cycle. The first stage of the intelligence cycle—direction—is critical because this is where decisionmakers test the intelligence agencies' capability to assess various biosecurity-related threats. Although the kind of tasking may differ depending on where the decisionmaker functions at the strategic (e.g., U.S. President or UK Prime Minister) or operational levels (e.g., task force commander). The tasking of the intelligence sector will also be influenced in part by what this capability has previously provided about particular threat issues. A decisionmaker's perception of the threat or risk will also be influenced by the extent to which threat methodologies resemble a valid assessment of threats. Given the gaps in knowledge about the intentions of bio-threat actors and disagreements about their capabilities to exploit various biotechnologies, intelligence agencies will need to manage policymakers' expectations about the validity of threat and risk methodologies.

While national tasking suggests that a national level agency such as the FBI, the Department of Homeland Security (DHS), the Royal Canadian Mounted Police (RCMP), or the Australian Federal Police (AFP) may take on the assignment, these tasks will normally have regional, state, and local dimensions, and the challenge is to engage sub-national agencies in nationally significant intelligence tasks. The activities which take place at next stage—collection—will depend on whether its purpose is for strategic, operational, or tactical decisionmaking. The mixture of secret vs. open sources of intelligence will likely differ at these three levels as well. For example, at the strategic level, collection efforts will be proportionally greater from open sources, particularly from the scientific, medical, and research communities, due to the focus on the evolution of various broad drivers, especially those related to technological advances in dual use research. At this level, strategic intelligence collection should focus on exploring where key vulnerabilities lay and whether diplomatic, operational, legislative, oversight, or normative remedies may be useful.

At the operational level, the likelihood is that more covert intelligence collection efforts (for example, human sources, surveillance, microbial forensics, and even geo-spatial intelligence) will be useful in providing insights into the activities of an emerging group, individual, or a series of similar threat types. Additionally, an important part of collection at the operational level will be outreach to both the public and private

biotechnology sectors. The other challenge at the operational level is how to best harness the limited collection resources of sub-national law enforcement and other stakeholders. Should greater capabilities or "clusters of excellence" in biosecurity issues be developed in existing fusion centers across the U.S. and other countries in order to more efficiently harness collection and analytical efforts? Finally, at the tactical level, collection will involve all of the covert sources used operationally, but their application will be more focused in support of one case under investigation.

At both the tactical and operational levels many other challenges arise in collecting intelligence useful in building a brief of evidence that results in the successful prosecution of a bio-criminal or bio-terrorist. Even if an investigation determines that the release of a biological agent was intentional, attributing this specific agent to an individual perpetrator is very difficult. For instance, the 2001 anthrax postal attack investigation led by the FBI took nearly a decade to complete. Though very resource-intensive it failed to conclusively attribute the action to a single perpetrator, despite the strong evidence against Bruce Ivins and the advanced genetic profiling completed on anthrax used. Yet, much was learned from this investigation, including the need for public health and security agencies to share information and for scientists to work more closely with investigators in the collection of information.[65] Multiple other challenges are present at the tactical intelligence level, specifically in determining what kind of scientific or microbial forensic information is admissible in court, and how it can be used with other information gathered during the investigation.[66]

At the analytical stage of the intelligence cycle, the many challenges for those working on emerging biosecurity threats mirror in some ways those confronted in the strategic, operational, and tactical collection of intelligence. At the strategic level, intelligence agencies must continue to seek external expertise on a range of bio-threats, given the impossibility of one agency to employ an endless number of scientists to work on a potentially infinite and diverse spectrum of potential threats. Recent budgetary constraints on national security communities in Australia, the UK, and the U.S. make further development of existing outreach programs to the scientific community essential.

Also important is for the larger intelligence assessment agencies, those with the greatest remit to report on bio-threats, to retain analysts highly skilled in biological sciences or public health to work on priority topics. Professional and organizational cultural challenges are at play here in both attracting and retaining competent scientific analytical staff. Analysts with scientific training need to adapt their empirical scientific frameworks to the work of organizations that rely on inductive and interpretational approaches to information processing. This scientific-analytical cadre will also need to adapt to working in closed secure environments, and be content to

''publish'' quickly classified papers that will have a much more restricted audience than the broader scientific community.

The analytical stage can also provide opportunities for analysts to remove themselves from their often overwhelming responsibilities for producing current intelligence. The bulk of an intelligence analyst's work is providing assessments on ''what is happening now.'' But analysts need more time to discuss potential bio-threat scenarios with counterparts in the scientific and academic communities using structured analytical techniques such as ''red teaming'' and ''black hatting.''[67] Opportunities already exist in the Australian, the UK, Canadian, NZ, and U.S. intelligence communities to do such work periodically—though they could be scheduled more frequently and include both local law enforcement and first responders, who bring ''outsider'' perspectives on issues of risks, threats, and vulnerability.

At the sub-national level, an enhancement of current intelligence fusion relationships that bring together the knowledge and assessments of biological experts with intelligence analysts will also likely enhance intelligence support to operational and tactical decisionmaking. But merely fusing the intelligence efforts of federal, state, and local authorities together, as done since 9/11, is no guarantee that intelligence support to decisionmakers will be necessarily more effective. Much will depend on the governance arrangements among participating agencies given their different agendas, cultures, and resource constraints.[68]

The final phase in the intelligence cycle, dissemination, is crucial, regarding the extent to which intelligence—whatever level of decisionmaking it is aimed—can influence decisionmakers in a timely manner. A common theme at the collection and analytical stages is the sharing of information. That finished intelligence products are disseminated as widely as possible is critical. At the operational and tactical levels, where a possible planned bio-attack has been identified or activated, sharing intelligence with clinicians, scientists, security managers, and emergency responders is vital to managing the threat and its public health consequences. A report on an investigation into the Boston bombings revealed that difficulties remain in the degree to which national and local agencies more quickly share intelligence.[69]

In an unfolding bio-terrorism crisis, first responders such as front line police and the security managers of public buildings and critical infrastructure will need a combination of national security intelligence and epidemiological intelligence to support their on-the-spot decisionmaking. Without this information, they won't know where the contagion might be spreading, thereby delaying strategies to minimize such risks as the separation of infected and uninfected staff and public, or the shutting down of physical environments that have become contaminated. Equally, the prompt dissemination of intelligence to security managers can assist

them proactively in implementing security procedures against emerging bio-threat scenarios.

Rapid dissemination by intelligence agencies of information about evolving bio-threats and vulnerabilities will also help local law enforcement and private sector security managers implement crime prevention and risk reduction strategies. Security managers responsible for protecting airports, seaports, sports arenas, malls, theaters, critical infrastructure, food companies, and scientific facilities are well placed to feed back to intelligence agencies information that enhances their own understanding of various bio-threats. By necessity, a culture of secrecy will always form around intelligence sources and, for operational reasons, some aspects of ongoing investigations will not be able to be shared. In the main, though, redacted forms of intelligence assessments should be quickly shared with front line staff to better mitigate risks.

WHAT IS EARLY WARNING?

Several discussions of intelligence and early warning (strategic) processes can be found in the literature.[70] In simple terms, though, intelligence and early warning provide the bridge between assessing current threats and estimating emerging ones. An effective intelligence and early warning system must be able to help analysts look for indicators suggesting that either a well-known current threat is changing or that a new one may be emerging that decisionmakers need to know about. The timeframes for providing early warning to decisionmakers will differ depending on the nature of the threat and the intelligence operating environment. For example, an intelligence and early warning system for the military may operate for a decade or more, the time required for another country to develop a new weapons program, whereas in the law enforcement context the warning system may well be shorter—one to two years—the time usually taken for an organized crime group to shift its involvement from one illicit drug market to another. Regardless of the type of threat or intelligence operating environment (law enforcement, national security, or private sector), a well-functioning intelligence and early warning system requires a well-integrated intelligence framework. In particular, an effective intelligence early warning system relies on systematic and enduring tactical and operational intelligence collection efforts that allow analysts to assess the significance of various ''warning indicators'' against a range of incoming information sources. Strategic (or estimative) intelligence does not try to estimate or ''predict'' what will happen. As Thomas Fingar correctly pointed out, the goal is to ''identify the most important streams of developments, how they interact, where they seem to be headed, what drives the process, and what signs might indicate a change of trajectory.''[71]

The job of a good intelligence and early warning process is to provide assessments that enable decisionmakers to ''shape the future not predict what it will be.''[72] Unfortunately, national security and law enforcement agencies have historically had a mixed record in both investing in or sustaining reliable strategic (estimative) intelligence or early warning capabilities. The influence of Sherman Kent in the immediate post-World War II period provided a foundation for the development of a strategic intelligence capability in the U.S. Intelligence Community.[73] In particular the CIA developed the National Intelligence Estimate (NIE), which generally seeks to provide a medium- to long-term assessment of a designated subject for the President.[74] The degree to which senior decisionmakers have engaged with longer term assessments such as the NIE or seen their value has not been consistent.[75] Partly this has been due to the ''mixed track record'' that warning intelligence has achieved post-1945.[76] Many agencies still have no appetite for estimative products that attempt to go beyond a year or two.[77]

For many public sector agencies an operational cycle requires a timeframe of one to two years. This is possibly as ''strategic'' as many can go due to budgetary, political, or organizational culture reasons. For example, over the past few decades several Australian police agencies have formed, abolished, and then reformed their estimative intelligence functions. Some police leaders seem willing to invest in those capabilities only to the extent that demands for immediate operational and tactical intelligence support require the reallocation of resources. This ''tactical drag'' results in strategic resources being pulled away from the development of effective estimative capabilities in policing agencies.[78] For law enforcement agencies to provide intelligence and early warning on emerging biosecurity threats without a sustainable, resourced estimative intelligence capability is obviously very difficult.

IMPROVING STRATEGIC EARLY WARNING CAPABILITIES FOR MONITORING BIO-THREATS

A strategic early warning capability consists of a series of intelligence processes and products that provides a bridge between assessing current threats and estimating emerging ones. To do so, strategic warning capabilities need to be both effective and reliable at the agency or intelligence community level. This in turn requires strong, viable core intelligence processes, involving tasking and coordination, collection, analysis, production, and evaluation, along with key enabling activities, meaning governance, collection, ICT, human resources, legislation, and research.[79]

The interplay of fully functioning core intelligence processes and key enabling activities results in an intelligence capability adaptable to the changing demands of the security environment. If one or more of the components in either category is not functioning optimally the overall capability is affected, underscoring the point that such capability can be effective only if built on an already fully functioning intelligence framework. Historically, the development of intelligence and early warning capabilities—and more broadly strategic (estimative) intelligence capabilities—has been patchy in both national security and policing contexts, partly due to one or more elements of an intelligence structure not being optimally built to support either a strategic or early warning function.

For many law enforcement agencies, a large number of "here and now" threats must always be dealt with in short time frames. That most collection and analytical resources have remained focused on tactical and operational level threats is not surprising. Additionally, intelligence agencies had a mixed record in assessing bio-threats accurately during the Cold War, and later, perhaps most spectacularly, on the extent to which Iraq still had a bio-weaponry program in 2003 prior to the second Gulf War.[80] Hence, decisionmaker expectations and perceptions of the value of strategic intelligence products have influenced investments in "over the horizon" intelligence capabilities.

Another important factor weighing on the effectiveness of strategic early warning capability for bio-threats arises from the different interests and expectations among public health and intelligence officials as to how health data might be used in a warning system. For example, the use of public health syndromic surveillance systems underscores how tensions can occur between local public health officials utilizing this information to maximize positive health outcomes in an epidemic and the requirements of intelligence agencies looking for outliers in the health data suggestive of bio-terrorism.[81]

BASIC REQUIREMENTS

In summary, improving strategic early warning capabilities can come about only if an effective intelligence framework is in place (including strong, viable core intelligence processes and key enabling activities) and if political leaders can appreciate the value of strategic intelligence products in helping them better understand emerging threats and how to utilize opportunities to prevent or disrupt them.

No simple pathway is available for managing the role of intelligence and improving strategic early warning practice to better prevent, disrupt, and control emerging biosecurity threats. Although assessing motivation is

particularly difficult, the application of an intelligence and early warning system for biosecurity will nonetheless help agencies improve their ability to track emerging threats, particularly from dual use research. Although many of the emerging bio-threats represent ''wicked problems,'' they still need addressing and comprehension. Many may be in the ''high impact, low probability'' threat category, but that doesn't mean ''no probability.'' Improving intelligence and early warning on biosecurity is important and should be the responsibility of a ''whole of intelligence enterprise''—meaning federal, state, and local—response, and not be left to a few analysts in a few nationally prominent agencies.

REFERENCES

[1] William Aldis, ''Health Security as a Public Health Concept: A Critical Analysis,'' *Health Policy and Planning*, Vol. 23, 2008, p. 370.

[2] Kenneth Bernard, ''Health and National Security: A Contemporary Collision of Cultures,'' *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, Vol. 11, No. 2, 2013, p. 157.

[3] Stefan Elbe, ''Pandemic Security,'' in J. Peter Burgess, ed., *The Routledge Handbook of New Security Studies* (Abingdon, UK: Routledge, 2010), pp. 163–173.

[4] Stefan Elbe, ''Pandemics on the Radar Screen: Health Security, Infectious Disease and the Medicalisation of Insecurity,'' *Political Studies,* Vol. 59, No. 4, 2011, pp. 848–866.

[5] Stefan Elbe, ''Pandemic Security,'' p. 163.

[6] Andrew Lakoff and Stephen J. Collier, *Biosecurity Interventions: Global Health and Security in Question* (New York: Columbia University Press, 2008), p. 26.

[7] Gregory Koblentz, ''Biosecurity Reconsidered,'' *International Security*, Vol. 34, No. 4, 2010, p. 104.

[8] *Ibid.*, p. 105.

[9] *Ibid.*

[10] National Research Council, *Globalization, Biosecurity and the Future of the Life Sciences*, Committee on Advances in Technology and the Prevention of their Application to next Generation Biowarfare Threats, National Research Council, (Washington, DC: National Academies Press, 2006), p. 32.

[11] Patrick F. Walsh, *Intelligence and Intelligence Analysis* (Abingdon, UK: Routledge, 2011), p. 10.

[12] The Human Security Centre, *The Human Security Centre: Human Security Report* (Oxford, UK: Oxford University Press, 2005).

[13] Patrick F. Walsh, ''Managing Intelligence and Responding to Emerging Threats: The Case of Biosecurity,'' in Martin Gill, ed., *Handbook of Security* (Basingstoke, UK: Palgrave Macmillan, 2014), pp. 837–856.

[14] Patrick F. Walsh, *Intelligence and Intelligence Analysis*, p. 62.

[15] *Ibid.*, p. 47.

[16] See William McNeil, *Plagues and People* (New York: Anchor Books, 1998), and Dorothy Crawford, *Deadly Companions: How Microbes Shaped Our History* (New York: Oxford University Press, 2007).

[17] These agents are referred to as "Category A" bioagents (denoted as such because they have the greatest capacity for harm if used in a bioterrorist attack). Refer to either the World Health Organization (WHO) or the U.S. Centers for Disease Control (CDC) websites for good overviews of these agents and others on the Category A list, such as smallpox, viral hemorrhagic fevers, and botulism.

[18] Ken Alibek, *Biohazards: The Chilling True Story of the Largest Covert Biological Weapons Program in the World—Told from the Inside by the Man Who Ran it* (New York: Random House, 1999), pp. 229–301.

[19] Gregory Koblentz, *Living Weapons: Biological Warfare and International Security* (Ithaca, NY: Cornell University Press, 2009), pp. 17–18.

[20] UNMOVIC, United Nations Monitoring, Verification and Inspection Commission (UNMOVIC), *Compendium of Iraq's Programmes in the Chemical, Biological and Missile Areas* (New York: United Nations, 2007), pp. 768–790.

[21] Gregory Koblentz, *Living Weapons: Biological Warfare and International Security,* pp. 220–227.

[22] William Rosenau, "Aum Shinrikyo's Biological Weapons Program: Why Did It Fail?," *Studies in Conflict and Terrorism,* Vol. 24, 2001, pp. 289–301.

[23] Rene Pita and Rohan Gunaratna, "Revisiting Al-Qaida's Anthrax Program," *CTC Sentinel*, Vol. 2, No. 5, 2009, pp. 10–13.

[24] George Tenet, with Bill Harlow, *At the Center of the Storm: My Years at the CIA* (New York: HarperCollins, 2007), pp. 278–279.

[25] William Rosenau, "Aum Shinrikyo's Biological Weapons Program: Why Did It Fail?." p. 296.

[26] Patrick F. Walsh, *Intelligence and Intelligence Analysis*, p. 49.

[27] Seth Carus, *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents Since 1900* (Washington, DC: National Defense University, 2001), pp. 6–10.

[28] Tim Inglis, Edward Eitzen, and Andrew Robertson, "Forensic Investigation of Biological Weapon Use," in John Gall and Jason Payne-James, eds., *Current Practice in Forensic Medicine* (Chichester, UK: John Wiley and Sons, 2011), pp. 17–35.

[29] For example, a number of recent incidents related to food production illustrate this sector's vulnerability to criminal exploitation, see Alice Yan, "Memories Still Too Raw for Chinese Parents to Trust Baby Formula," *South China Morning Post,* 2 July 2013; Simon Neville, "Horsemeat Lasagna Scandal Leaves Findus Reputation in Tatters," *The Guardian*, 9 February 2013; Claire Trevett, "Fronterra Chief Gets 'Frank and Thorough Grilling,'" *New Zealand Herald*, 9 August 2013.

[30] Patrick F. Walsh, *Intelligence and Intelligence Analysis.*

[31] The National Academies committee produced a report in 2004 called ''Biotechnology Research in an Age of Terrorism'' (sometimes also referred to as the ''Fink Report''). The Report contained seven recommendations to ensure responsible oversight of biotechnology research with potential bioterrorism applications. One was to create a National Science Advisory Board for Biodefense to provide advice, guidance, and leadership for a system of review and oversight of experiments of concern. See National Research Council, *Biotechnology Research in an Age of Terrorism* (Washington, DC: National Academies Press, 2004).

[32] Richard Henkel, Thomas Miller, and Robbin Weyant, ''Monitoring Select Agent Theft, Loss and Release Reports in the United States—2004–2010,'' *Applied Biosafety*, Vol. 17, No. 4, 2012, pp. 171–180.

[33] Marie French, ''Anthrax, Bird Flu Safety Breaches Shutdown CDC Labs,'' *Bloomberg*, 12 July 2014.

[34] Patrick F. Walsh, ''Managing Intelligence and Responding to Emerging Threats: The Case of Biosecurity,'' p. 843.

[35] *Ibid.*

[36] *Ibid.*

[37] *Ibid.*

[38] *Ibid.*, p. 844.

[39] Ryan Burnette, ed., *Biosecurity: Understanding, Assessing, and Preventing the Threat* (Hoboken, NJ: John Wiley & Sons, 2013), p. 97.

[40] See Christos Nicolaides, Luis Cueto-Felgueroso, Marta Gonzalez, and Ruben Juanes, ''A Metric of Influential Spreading During Contagion Dynamics Through the Air Transportation Network,'' *Plos One,* Vol. 7, No. 7, 2012, pp. 1–10; Bruno Goncalves, Duygu Balcan, and Alessandro Vespignani, ''Human Mobility and the Worldwide Impact of Intentional Localized Highly Pathogenic Virus Release,'' *Scientific Reports,* Vol. 3, No. 810, 2013, pp. 1–7.

[41] See, for example, Catriona McLeish and Paul Nightingale, ''Biosecurity, Bioterrorism and the Governance of Science: The Increasing Convergence of Science and Security Policy,'' *Research Policy*, Vol. 36, 2007, pp. 1635–1654; Dana Shea, ''Oversight of Dual-Use Biological Research: The National Science Advisory Board for Biosecurity,'' *Congressional Research Service Reports*, Paper 33, Washington, DC; Jonathan Tucker, ed. *Innovation, Dual Use and Security,* (Cambridge, MA: MIT Press, 2012). Bryn Williams-Jones, Catherine Olivier, and Elise Smith, ''Governing 'Dual Use,' Research in Canada: A Policy Review,'' *Science and Public Policy*, 2013, pp. 1–18.

[42] Catriona McLeish and Paul Nightingale, ''Biosecurity, Bioterrorism and the Governance of Science: The Increasing Convergence of Science and Security Policy,'' p. 1636. For details of these three papers see: Jeronimo Cello, Aniko Paul, and Eckard Wimmer, ''Chemical Synthesis of Poliovirus cDNA: Generation of Infectious Virus in the Absence of Natural Template,'' *Science*, No. 297, 2002, pp. 1016–1018; Ariella 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 Academy of Sciences, 99, 8808, R-8813. R, 2002; and Ronald Jackson et al., ''Expression of Mouse Interleukin-4 by Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox,'' *Journal of Virology,* Vol. 75, 2001, pp. 1205–1210.

[43] Terrence Tumpey et al., ''Characterization of the Reconstructed 1918 Spanish Influenza Virus,'' *Science*, Vol. 310, 2005, pp. 77–80; Lawrence Wein and Yifan Liu, ''Analyzing a Bioterror Attack on the Food Supply: The Case of Botulinum Toxin in Milk,'' *Proceedings of the National Academy of Sciences of the United States of America*, Vol. 102, 2005, pp. 9984–9989.

[44] Masaki Imai et al, ''Experimental Adaptation of an Influenza H5 HA Confers Respiratory Droplet Transmission to a Reasortant H5 HA/HIN1 Virus in Ferrets,'' *Nature*, No. 486, 2012, pp. 420–428; Sander Herfst et al., ''Transmission of Influenza A/H5N1 Virus Between Ferrets,'' *Science*, 22 June 2012, pp. 1534–1541. The 2013 letter can be found in Ron Fouchier et al., ''Letters, Gain of Function Experiments on H7N9,'' *Science.* Vol. 341, 2013, pp. 612–613.

[45] Brendan Maher, ''The Biosecurity Oversight,'' *Nature,* Vol. 485, 2012, pp. 431–434.

[46] See, for example, Ron Fouchier et al., ''Letters, Gain of Function Experiments on H7N9.''

[47] The White House, The Office of Science and Technology Policy, ''Doing Diligence to Assess the Risks and Benefits of Life Science Gain of Function Research,'' Media Release, 17 October 2014, at www.whitehouse.gov

[48] The Center for Biosecurity of UMPC, *The Industrialization of Biology and its Impact on National Security* (Baltimore, MD: Center for Biosecurity of UMPC, 2012).

[49] *Ibid.*, p. 7.

[50] Life Technologies, ''Life Technologies Introduces the Benchtop Ion Proton™ Sequencer; Designed to Decode a Human Genome in One Day for $1,000,'' Press release, 10 January 2012, at http://www.lifetechnologies.com/content/lifetech/us/en/home/about-us/news-gallery/press-releases/2012/life-techologies-itroduces-the-bechtop-io-proto.html

[51] James Randerson, ''Revealed: The Lax Laws that Could Allow the Assembly of Deadly Virus DNA,'' *The Guardian,* 14 June 2006.

[52] See National Research Council, *Globalization, Biosecurity and the Future of the Life Sciences*. See also National Research Council, *Positioning Synthetic Biology to Meet the Challenges of the 21st Century: Summary Report of a Six Academies Symposium*, National Research Council and National Academy of Engineering (Washington, DC: National Academies Press, 2013); and Jonathan Tucker, ed., *Innovation, Dual Use and Security*.

[53] Marc Goodman and Andrew Hessel, ''The Bio-Crime Prophecy: DNA Hacking the Biggest Opportunity Since Cyber Attacks,'' *Wired,* 2013, 28 May 2013.

[54] The Center for Biosecurity of UMPC, *The Industrialization of Biology and Its Impact on National Security*, p. 16.

[55] Marc Goodman and Andrew Hessel, "The Bio-Crime Prophecy: DNA Hacking the Biggest Opportunity Since Cyber Attacks."

[56] The Center for Biosecurity of UMPC, *The Industrialization of Biology and Its Impact on National Security,* p. 15.

[57] Christopher Chyba, "Biotechnology and the Challenge to Arms Control," *Arms Control Today.* Vol. 36, No. 8, 2006, pp. 11–17.

[58] Kathleen Vogel, "Framing Biosecurity: An Alternative to the Biotech Revolution Model?" *Science and Public Policy*, Vol. 35, No. 1, 2008, pp. 45–54.

[59] Jonathan Suk et al., "Dual Use Research and Technological Diffusion Reconsidering the Bioterrorism Threat Spectrum," *PLOS Pathogens*, Vol. 7, No. 1, 2011, pp. 1–3.

[60] Jared Burr, "The Mad (and Not So Mad) Scientists Next Door: A Holistic Approach to Do It Yourself Biology," *Journal of Biosecurity, Biosafety and Biodefense Law*, Vol. 3, No. 1, 2012, pp. 1–20.

[61] The Center for Biosecurity of UMPC, *The Industrialization of Biology and Its Impact on National Security*, p. 16.

[62] *Ibid.*

[63] Patrick F. Walsh, "Managing Intelligence and Responding to Emerging Threats: The Case of Biosecurity," p. 850.

[64] Patrick F. Walsh, "Intelligence and National Security Issues," in Phillip Birch and Victoria Herrington, eds., *Policing in Practice* (Melbourne, Australia: Palgrave Macmillan, 2011), pp. 113–117.

[65] Patrick F. Walsh, *Intelligence and Intelligence Analysis*, p. 53.

[66] Lisa Danley, "Duties and Difficulties of Investigating and Prosecuting Biocrimes," *Journal of Biosecurity, Biosafety and Biodefense Law*, Vol. 3, No. 1, 2012, pp. 1–19.

[67] Richards Heuer and Randolph Pherson, *Structured Analytical Techniques for Intelligence Analysis* (Washington, DC: CQ Press, 2011).

[68] Patrick F. Walsh, *Intelligence and Intelligence Analysis.*

[69] U.S. Department of Homeland Security, "The Road to Boston: Counter-Terrorism Challenges and Lessons From the Boston Marathon Bombings" (Washington, DC, 2014).

[70] See for example, Cynthia Grabo, *Anticipating Surprise Analysis for Strategic Warning* (Washington, DC: University Press of America, 2005); Thomas Fingar, *Reducing Uncertainty* (Stanford, CA: Stanford University Press, 2011); Patrick F.Walsh, *Intelligence and Intelligence Analysis;* and James J. Wirtz, "Warning in an Age of Uncertainty," in Roger George and James Bruce, eds., *Analyzing Intelligence: National Security Practitioners' Perspectives* (2nd ed.) (Washington, DC: Georgetown University Press, 2014).

[71] Thomas Fingar, Reducing Uncertainty, p. 53.

[72] *Ibid.*

[73] Sherman Kent, *Strategic Intelligence* (Princeton, NJ: Princeton University Press, 1949).

[74] Patrick F. Walsh, *Intelligence and Intelligence Analysis*, p. 171.
[75] Roger George and James Bruce, eds., *Analyzing Intelligence*, p. 229.
[76] James J. Wirtz, "Warning in an Age of Uncertainty," p. 219.
[77] Patrick F. Walsh, *Intelligence and Intelligence Analysis,* p. 172.
[78] *Ibid.*, p. 172.
[79] *Ibid.*, pp. 147–151.
[80] See Gregory Koblentz, *Living Weapons: Biological Warfare and International Security,* pp. 141–199, and Kathleen Vogel, *Phantom Menace or Looming Danger?: A New Framework for Assessing Bioweapon Threats* (Baltimore, MD: John Hopkins University Press, 2013).
[81] Lyle Fearnley, "Redesigning Syndromic Surveillance for Biosecurity," in Andrew Lakoff and Stephen J. Collier, eds., *Biosecurity Interventions: Global Health and Security in Question* (New York: Columbia University Press, 2008), pp. 61–88, at p. 84.