Preventing Armageddon II: Confronting the Specter of Agriterror

Strategic Insights, Volume III, Issue 12 (December 2004)

by Barry S. Zellen

Strategic Insights is a monthly electronic journal produced by the Center for Contemporary Conflict at the Naval Postgraduate School in Monterey, California. The views expressed here are those of the author(s) and do not necessarily represent the views of NPS, the Department of Defense, or the U.S. Government.

For a PDF version of this article, click here.

Introduction

Deep in America's heartland—where our country's vast agricultural system sustains not only the nutritional requirements of nearly 300 million people, but contributes over $50 billion US each year to America's export-economy—there is a new, lingering worry on our security experts' minds. This new, dark fear is of a deliberate terror attack of America's food supply.

Indeed, this fear was recently articulated publicly—and clearly—by outgoing Secretary of Health and Human Services (HHS) Tommy Thompson during a candid question period following the announcement of his resignation on December 3, 2004, during which he shared his grave concern about the possibility of a terrorist attack on the nation's food supply:

"For the life of me, I cannot understand why the terrorists have not attacked our food supply because it is so easy to do."[1]

Such a deliberate attack of our nation's food supply would be a unique and nefarious form of terrorism—called "agriterror" by some—which could include the biological infection of our livestock; the contamination of our food processing and distribution systems through exposure chemical, radiological or biological agents; and/or the physical destruction of our crops—whether through introduction of pests, destruction of irrigation systems, or the intentional setting of a prairie fire.

While the very scale of America's food production system and its vast, continental expanse suggests an inherent invulnerability, as 9/11 has shown, it only takes one successful, symbolic attack of our infrastructure to paralyze our nation, shake our confidence, and spread fear across the land.

Agriterror is not a new invention. Some believe that agriterror is, ironically, an American invention, and during the world's first truly modern "total war," the U.S. Civil War—which introduced a potent form of mechanized warfare by wedding the power of industrialization with the mass-mobilization of the nation—that resulted in the near total destruction of the secession-minded Confederacy's

economic infrastructure. During General Sherman's infamous "March to the Sea," his troops intentionally torched Confederate cities and set aflame its farms, destroying the rebellious South's capacity to feed itself while at the same time destroying the backbone of its agrarian economy, King Cotton.

Destroying an enemy's food production capability is an ancient tactic, dating back to the days of Rome's conflict with Carthage, whose fields it salted to render them forever barren and unproductive. But with General Sherman, the scale and speed of destruction achieved a new level, bringing agriterror into the modern age—as a tool of total warfare.

In our new age of international terrorism, it no longer requires an army of mechanized armor and mobile infantry to destroy a nation's infrastructure and food production capabilities. Now, one well-placed and virulent bio-weapon could do the trick.

Just as the recent SARS outbreak—which revealed how real today's bioterror threat is, and how easily a new pandemic can spread globally—quickly settled down, an even newer threat emerged, this time right in the American heartland: monkey pox, a close but less-deadly cousin of the dreaded smallpox. Monkey pox had its very first outbreak in the western hemisphere last spring, an ominous and in some ways fortuitous warning of the dangers we face in this new world of boundless terror.

As Steve Mitchell, medical correspondent for *United Press International* (UPI), reported last year, over the course of just a few weeks, dozens of Americans were infected with monkey pox. Doctors in Wisconsin saw the first patient on May 22, 2003 when a 4-year-old girl developed a rash similar to that caused by smallpox.[2] In spite of the risk of potential spread, local health officials as well as the national Center for Disease Control and Prevention (CDC) in Atlanta were not notified until 13 days later. Mitchell reported the CDC, in turn, did not make the case known publicly until June 7th, three days after it had learned of the case in Wisconsin. By then, there were 19 suspected monkey pox cases in Wisconsin, Indiana and Illinois.

Mitchell observed that despite the CDC's claim "that the nation has improved its preparedness to respond to a bioterrorist attack and emerging infectious diseases, the monkey pox experience indicates there still is no rapid communication system to alert physicians and health agencies around the country." Indeed, "the recent outbreak of monkey pox in the United States, and the delay in alerting healthcare personnel to its spread, highlights the need for a national communications system to alert physicians and public health officials rapidly about bioterrorist attacks or emerging diseases such as SARS and West Nile virus." Mitchell said "quicker notification of the country's medical community might have been particularly prudent because monkey pox has spread, now infecting as many as 54 people in several additional states, including Texas, New Jersey, Pennsylvania and South Carolina. The outbreak has become such a concern the CDC is taking the unprecedented step of recommending experimental use of the smallpox vaccine—which can have severe side effects, including death—in infected people, healthcare workers and those who were exposed to sick prairie dogs, which appear to be the source of the monkey pox." Mitchell sounds the alarm over monkey pox because it "could have been smallpox." And, he added, "some bioterrorist experts have expressed concerns terrorists could try to use monkey pox itself as a bioweapon."

Project BioShield

So how can America protect itself from future biothreats? The Bush Administration's solution, announced in January 2003 during the President's State of the Union, is called Project BioShield. In his speech, President Bush called on Congress to bolster America's biodefenses, but in the months to follow, legislation went in circles in the U.S. Congress.[3] An editorial six months later published by *The Washington Times*, the conservative D.C. daily, castigated Congress for

dawdling, arguing that “it appears unlikely to pass before Congress returns from its July 4 recess—if at all,” as both the House and Senate versions of the bill have been held up in committee.[4] Without a Congressional mandate to secure America from this invisible but worryingly potent threat, *The Washington Times* noted that pharmaceutical companies saw little commercial potential in searching for treatments to the plague, anthrax or ebola, and have avoided the necessary investment of time and resources to equip America with the defensive tools it needs. *The Washington Times* argued that “while lawmakers have made holding the line on spending a top priority, terrorists are making it their first priority to develop biological weapons. Congress needs to move quickly to support Project BioShield, an essential component of U.S. defense against bioterrorism.”

Both the House and Senate agreed that BioShield was needed, but not on the amount to spend. President Bush didn’t want to impose a cap on spending, but some in Congress did. It would take another year before a deal was concluded, and on July 21, 2004—more than a year after *The Washington Times* accused Congress of dawdling—President Bush signed Project BioShield into law, providing “new tools to improve medical countermeasures protecting Americans against a chemical, biological, radiological, or nuclear (CBRN) attack.” It allocated $5.6 billion US over ten years for developing the necessary vaccines and medicines to protect Americans from a bioattack—guaranteeing government purchase of the new biomedical products.

According to the terms of the final legislation signed into law this past July, Project BioShield will:[5]

- Expedite the conduct of NIH research and development on medical countermeasures based on the most promising recent scientific discoveries.
- Give FDA the ability to make promising treatments quickly available in emergency situations—this tightly controlled new authority will enable access to the best available treatments in the event of a crisis.
- Ensure that resources are available to pay for “next-generation” medical countermeasures. Project BioShield will allow the government to buy improved vaccines or drugs. The fiscal year 2004 appropriation for the Department of Homeland Security included $5.6 billion over 10 years for the purchase of next generation countermeasures against anthrax and smallpox as well as other CBRN agents.

As the result of the Project BioShield legislation, the Administration has already begun the process of acquiring several new medical countermeasures, including:

- 75 million doses of a second generation anthrax vaccine to become available for stockpiling beginning next year.
- New medical treatments for anthrax directed at neutralizing the effects of anthrax toxin.
- Polyvalent botulinum antitoxin.
- A safer second generation smallpox vaccine.
- Initial evaluation of treatments for radiation and chemical weapons exposure.

With the new BioShield authorities, the White House announced that Secretary Thompson “will launch multi-year initiatives to develop advanced treatments and therapeutics for exposure to biological agents and radiation poisoning,” adding that signing Project BioShield into law “is just the latest step the President has taken to win the War on Terror and protect our homeland.”

Al Qaeda’s Agriterror Ambition

Al Qaeda computer records, abandoned on hard drives found in caves and safe houses scattered across Afghanistan during Operation Enduring Freedom, suggest that the terror network was

keenly interested in bio-weapons prior to 9/11, as they are widely considered to be “the poor man’s WMD,” requiring far less technical and financial investment to produce than nuclear weaponry. As well, Al Qaeda had developed an interest in America’s agriculture, and its training manual examined methods to commit agricultural terrorism.

As reported by *GovExec.com's* Katherine McIntire Peters, “It shouldn't be surprising that a determined enemy like al Qaeda would consider ways to disrupt U.S. food supplies.[6] The history of warfare is full of examples of burned crops, poisoned wells and slaughtered herds. Agriculture is an obvious target for terrorists: infecting plants or animals with deadly disease is easier, cheaper and less risky than infecting humans directly; the economic consequences of a widespread attack would be enormous; and the panic and fear such an attack might reap could lead to wide-scale social disruption.”

She notes that Al Qaeda “left behind many clues to their aspirations in “hundreds of pages of U.S. agricultural documents that had been translated into Arabic,” and that “a significant part of the group's training manual is reportedly devoted to agricultural terrorism-the destruction of crops, livestock and food processing operations.” As a consequence, McIntire Peters says U.S. state and federal governments “have beefed up security and increased inspections of food and agricultural facilities across the country” but that given the vast scale and complexity of the agricultural system in the U.S., “security is an elusive concept. From sprawling farms to feed lots, from state fairs to food processing plants, there are countless points at which terrorists could access the food supply system with relative ease.”

The U.S. Department of Defense has conducted high-level crisis simulations, McIntire Peters reported, noting that a *RAND Review* article last summer observed that “the farming and food industries are highly vulnerable to both deliberate and accidental disruption for several reasons.” The National Defense University has identified five potential targets of agricultural bioterrorism: field crops, farm animals, food items in the processing or distribution chain, market-ready foods at the wholesale or retail level, and agricultural facilities. And officials of the RAND Corporation “estimate that no major U.S. city has more than a seven-day supply of food,” revealing an Achilles’ heal that Al Qaeda has already recognized.

According to McIntire Peters, 20 states have passed—or are considering—legislation related to agriterrorism, according to data compiled by the Council of State Governments. Many states have also hired more farm and food inspectors, developed guidelines for improving physical security at agricultural facilities, and are building more effective disease surveillance networks. Federal responsibility for agricultural security is shared by the Department of Agriculture (DoA), the Department of Health and Human Services (DHHS), and the Department of Homeland Security (DHS). At DoA, the Food Safety and Inspection Service monitors meat and poultry products, and plans for responding to outbreaks of food-borne illness, while a division of the Animal and Plant Health Inspection Service (APHIS) is responsible for protecting agricultural crops and plants from disease. At DHHS, the Food and Drug Administration (FDA) is responsible for ensuring the safety of seafood, plant and dairy foods and beverages and other food products. And DHS has taken over the inspection of food and agricultural products entering the United States, formerly the responsibility of APHIS' Agricultural Quarantine Inspection program.

To ensure the security of America ’s food supply, there is the need for greater federal inter-agency cooperation, though McIntire Peters noted that in the “last 18 months, agencies have taken steps to boost their inspection and analysis capabilities.” Further, the USDA has hired 20 new "import surveillance liaison" inspectors, to reinspect imported meat and poultry products. Additionally, as a result of the 2002 Public Health Security and Bioterrorism Preparedness and Response Act, the FDA is tightening food safety regulations—by requiring food processing facilities to register with the agency, mandating that companies provide advance notice of imported food shipments, and maintaining better records to make it easier to trace tainted food to its source.

As McIntire Peters reported, many agricultural experts believe the greatest threat to U.S. agriculture would be the deliberate or accidental introduction of foot-and-mouth disease—a "highly contagious viral disease that attacks cloven-footed animals, including cattle, swine, sheep, deer and elk" that is "so swift and debilitating that milk and meat production could be severely cut nationwide."

Indeed, in 1997, foot-and-mouth disease appeared in pigs in Taiwan, and "spread throughout the island within six weeks, forcing authorities to slaughter more than 8 million pigs and halt pork exports." The origin of the disease has been traced to a single pig from Hong Kong—"and China was suspected of deliberately introducing the disease into Taiwan." The total cost of this outbreak to Taiwan: $19 billion US. At the time, some speculated this was a case of bioterror directed against Taiwan by mainland China.

And every bit as worrisome as a foot-and-mouth disease attack of America's livestock would be an attack of America's crops, which "make up more than half the total value of American farm commodities and contribute more to exports." So how can America secure its foodstuffs?

With over half a million farms and 57,000 food processing facilities spread across the vast continental U.S., the challenge is huge. New policies, and inter-agency and inter-departmental cooperation is one key, spreading the burden across various government departments. And technology is another.

Toward a Bioterrorism Surveillance System

As Tom Ramstack reported in *The Washington Times*, "Continuing bioterrorism scares are breathing new life into obscure scientific projects as the nation gropes for a way to defend itself from deadly microbes."[7] One solution that is emerging is a handheld "microarray" system that "tests white blood cells to detect viruses within 36 hours of exposure, sometimes even before victims know they are sick. The device is supposed to be an early warning system against biological bombs. It was developed by the Walter Reed Army Institute of Research for the malaria soldiers might encounter in other countries," and the "Army plans to refine the system to detect anthrax, smallpox and other diseases."

Another case of technology innovation is the use of radar to detect bioterror attacks. In one test of such a use of the U.S. national weather radar grid, "a crop duster released a mixture of grain alcohol, clay dust and water and polyethylene glycol over central Oklahoma March 24. The Army and the Environmental Protection Agency were testing whether radar could detect a bioterrorist attack." Ramstack said that "they hope to develop computer technology for a nationwide bioterrorism detection program," and that the "EPA has done similar tests in Maryland, Utah and Florida since 2001."

Federal Computer Week's Sara Michael reported that "in an effort to detect bioterrorism attacks at an early stage, Centers for Disease Control and Prevention officials are studying ways to access and analyze prediagnostic health data for indications of a disease outbreak."[8] BioSense is a new proposal being discussed with CDC's parent agency, DHHS. "By examining syndromic data from several national sources, public health officials may be able to detect a trend, allowing for a more rapid response. BioSense would draw on several national data sources, such as requested lab tests, over-the-counter drug sales and managed care hot lines that patients call with questions or concerns."

CIO's Sarah D. Scalet observed that health officials are working toward a sophisticated IT network that could detect the early warning signs of bioterrorism, but formidable obstacles remain."[9] She cited Rosemary Nelson, chairman of National Preparedness and Response, a new bioterrorism task force created by the Healthcare Information Management and Systems

Society (HIMSS), who said such a system, to "sound the alarm in that precariously short window of time when the spread of disease could be stopped," is now "being defined and created." Scalet reported that today"it might take weeks or months for the CDC to gather sufficient information to spot a bioterrorist attack"—but "with a sophisticated IT network, it would take just days." At New Mexico's Sandia National Labs, Scalet observed researchers have developed a system called the Rapid Syndromic Validation Project, which "requires health-care providers to actually log on to a secure website and type in information about a patient's symptoms in return for trend and treatment information," nearly instantly.

In addition, the CDC has developed the National Electronic Disease Surveillance System (NEDSS), which "lays out a sort of meta-standard for both healthcare information and IT standards," and all state health department systems must be NEDSS-compatible "if they want a piece of the $918 million in bioterrorism grants that the CDC is handing out this year." With such "pocketbook persuasion," Scalet believes things could get better—but currently, "a national bioterrorism surveillance system seems far off, indeed."

In addition to technology, new policies are being crafted to help America cope with the new threat of bioterror. Ramstack reported that "Congress responded to the October 2001 anthrax scare by passing the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, known as the Biopreparedness Act," which created "new restrictions on who can handle dangerous microbes, which ones they can handle and how and where they can be used. In addition, industry must follow stricter procedures to prevent contamination of food and water supplies."[10]

The $500 billion food-processing industry must now "register facilities and give prior notice of any imports companies accept," and the FDA has "also increased its inspections of foods that could be contaminated with anthrax or other toxins." Other provisions of the Biopreparedness Act impose criminal penalties on unauthorized handling of organisms and chemicals, some of which are commonly used in academic research.

With this evolving mix of new, and more pro-active, policies to more thoroughly monitor the U.S. food supply, and emerging technologies to better detect and track a bio-attack from its earliest of stages, America is getting better able to respond to a the nightmare-scenario of bioterrorism if it has to. And, as Secretary Ridge has pointed out, this could effectively deter such an attack from ever happening.

As they say, an ounce of prevention is worth a pound of cure. When it comes to agriterrorism, one might argue that an ounce of prevention is worth a ton of cure, maybe more.

References

1. Robert Pear, "U.S. Health Chief, Stepping Down, Issues Warning," The New York Times, December 4, 2004.

2. Steve Mitchell, "Monkey pox shows gap in bioterror readiness," United Press International (UPI), June 12, 2003.

3. For a transcript of the President's 2003 State of the Union, you may view a transcript at "Transcript of State of the Union" on CNN's website.

4. "Still no bioshield," *Washington Times,* June 22, 2003.

5. "Project BioShield: Progress in the War on Terror," *Whitehouse.gov*, July 21, 2004.

6. Katherine McIntire Peters, "Officials fear terrorist attack on U.S. food supply," *GovExec.com,* June 10, 2003.

7. Tom Ramstack, "Germ research gets urgent," *The Washington Times,* June 8, 2003.

8. Sara Michael, "BioSense would sniff out bioterror," *Federal Computer Week* , June 16, 2003.

9. Sarah D. Scalet, "Immune Systems," *CIO* magazine, June 2003.

10. Ramstack, *op. cit*.