

Bioterrorism—a clear and present danger

Until a few years ago, the thought of anyone highjacking a crowded airliner and deliberately crashing it into skyscraper buildings in one of the world's major cities would have been dismissed as fantasy. The event would have been unthinkable. But then, on September 11, 2001 fantasy was turned into chilling fact.

However, long before the tragic happenings of 9/11, bioterrorism has been recognized as a creditable threat and its employment is not new. Until recently, the threat was more popularly known as germ or chemical warfare and, as such, the tactic is centuries old though today it is more sophisticated. In addition to its use in times of war, terrorists have long since discovered that they can use food as a weapon to obtain funds for their cause or to attack and even destroy a country's economy.

All stages of food production are vulnerable, from seeds being grown to crops being harvested, packaged, shipped and supplied to manufacturers as well as to the factories in which food products are manufactured and the network through which they are distributed and sold to the public. Even crop dusting techniques could be employed with devastating effects on growing crops. In addition, the rapid spread of diseases such as the foot and mouth epidemic in the United Kingdom and avian flu in the Far East as well as the anthrax scares in the United States and the devastating effects of the release of sarin gas on the Japanese subway underline the fact that bioterrorism poses a very real threat.

Certainly, the threat to the US food supply is more than theoretical. When American troops entered the caves and safe houses of members of the al-Qa'eda terrorist network in Afghanistan in the months following the 9/11 attacks they found hundreds of pages of US agricultural documents that had been translated into Arabic.¹ A significant part of the terrorists' training manual

¹ Katherine Peters, *Officials fear terrorist attack on US food supply*, Government Executive (June 10, 2003).

was reportedly devoted to agricultural terrorism such as the destruction of crops, livestock, and food processing operations.

However, scientists regard those outbreaks as 'low tech'. They are concerned that the findings of life science research could be used to engineer deadly viruses that could be unleashed on the world. The threat is sufficiently credible for the Royal Society, the United Kingdom's most respected body of scientists, and the Wellcome Trust to have called a meeting of scientists and policy makers to discuss the issue.

Speaking in London on October 7, 2004 Professor Julia Higgins, vice-president of the Royal Society, said: "Scientists have a responsibility to minimise the possibility of their work being misused. At the moment cutting-edge work such as targeted modification of viruses is probably well beyond the capabilities and resources of those who wish to cause harm. However, as the technologies progress these processes are likely to become cheaper and easier to perform.

"What we want to look at in this meeting is whether it is possible to monitor the flow of information into the public domain without unduly hindering scientific progress and how we can raise awareness with scientists that their work may be open to misuse."

Dr Mark Walport, director of the Wellcome Trust, said: "SARS (Severe Acute Respiratory Syndrome) and bird influenza are recent examples of human vulnerability to new and dangerous natural infections. Responsible international research conducted in an open fashion is essential to understand and find effective vaccines and treatments for infections such as these. While it is always important to do what we can to minimize the risk of research being used for evil purposes, we must guard against inhibiting the vast majority of medical research which is carried out for the benefit of mankind."

A report of the meeting was being submitted to the government's Foreign & Commonwealth Office to help with the preparation for the annual meeting of the Biological Weapons Convention in 2005, which will be chaired by the UK government. It will focus on how the content, dissemination and adoption of codes of conduct for scientists could strengthen the convention.

Obviously, any epidemic on such a scale would be a matter for the relevant government to handle and be beyond the resources of individual companies or industries, as had already been pointed out, but there are advantages in being well-informed while keeping such threats in perspective.

In the United States, the Center for Infectious Disease Research and Policy² at the University of Minnesota lists six diseases (Category A agents) as most likely to be spread by terrorists. They are anthrax, botulism, plague, smallpox, tularemia or 'rabbit fever' and viral hemorrhagic fever (VHF) of which Lassa fever, Ebola, Rift Valley and Indonesian dengue fever are examples. At present, healthcare systems and effective drugs and vaccines are nearly non-existent.

A measure of the seriousness with which such threats are viewed is that, on November 2, 2004, the National Institute of Allergy and Infectious Diseases

² <http://www.cidrap.umn.edu/cidrap/content/bt/bioprep/index.html>

(NIAD) awarded contracts worth \$73 million to study the mechanisms by which certain infectious agents, including potential bioterror agents, trigger immune reactions.

Examples of bio-warfare

Bioterrorism is not new. As early as 184 BC Hannibal is reputed to have ordered pots filled with serpents—presumably poisonous snakes—to be thrown onto the decks of enemy ships. At the same time, in the days of the Roman Empire, soldiers catapulted corpses and dead animals into besieged cities.

In 1346, it is recorded that Tatar forces besieging Kaffa (now Feodosia in the Ukraine) catapulted plague corpses into the city. More recently, in 1763, a British officer distributed smallpox infected blankets to native Indians during the French and Indian War in North America.

In 1942, as the United States began research into biological weapons, Britain tested anthrax on sheep on the uninhabited Scottish Island of Gruinard. It is still believed to be contaminated.

Iraq used chemical weapons against Iran during its 1980–1988 war with its neighbor. Some years later, Iraq also used chemical weapons on Kurds living in the north of the country, killing large numbers of men, women and children as well as livestock.

During subsequent wars in Iraq—Desert Storm and Operation Iraqi Freedom—there were fears that the country's dictator, Saddam Hussein, would use chemical and biological weapons against coalition troops but they did not materialize.

In the late 1970s, Palestinian terrorists were reported to have spiked Israeli citrus fruit for export to Europe with liquid mercury. In 1986, Tamil separatists threatened to poison tea exports from Sri Lanka with arsenic but no traces were found despite every consignment being checked by importing countries for many years afterwards.

During World War I, the Germans used various human and animal pathogens as agents of germ warfare in Europe.

During World War II, the Japanese used germ warfare against the Chinese and Russians. In 1995, a cult placed containers of deadly sarin nerve agent on five trains on three major lines of the subway system in Tokyo, Japan's capital city. Twelve people died and over 5500 were injured as the gas spread through the trains.

More recently, in 2001, many facilities in the United States received anthrax-threat letters. Some of the envelopes were empty, others contained a white powder. The attacks led to deaths and illness.

Fourteen contracts were approved for the Large-Scale Antibody and T Cell Epitope Discovery Program. Studying epitopes, the regions of infectious agents that elicit immune responses, may uncover new targets for vaccines, therapies, and diagnostic tools against potential terror agents. Such research could also reveal targets among emerging and re-emerging infectious diseases like influenza and West Nile virus.

The NIAD director Anthony S. Fauci, MD, said: “The information generated by this program will deepen our understanding of how components of the immune system defend against certain infectious agents, enabling researchers to design new and improved medical countermeasures.”

Institutions in the United States, the United Kingdom and Denmark are involved in the work.

Realistically, much of the responsibility for preventing or detecting the contamination of food products must lie with the growers, shippers, and processors of our food products. Governments would have to deal with the aftermath.

In September 2002, in a paper published under the aegis of the University of Florida and entitled *Impact of the Bioterrorism Threat on the Food Industries*,³ Douglas L. Archer and Fred H. Degnan⁴ remarked: “What would such an attack on the food supply accomplish? It is difficult to envision that widespread serious harm and death would result, at least no more so than we experience in large outbreaks of food-borne disease. Nevertheless, even if relatively little harm to human health resulted, economic consequences could be great and consumer confidence in the food supply and regulatory agencies shaken.

“The Tylenol tampering episodes of the early 1980s provide a good model of the types of considerations and prophylactic steps the industry should be considering. The episodes energized Food and Drug Administration (FDA)-related industries to implement meaningful anti-tampering plans, including new or modified drug forms and tamper-resistant packaging.

“FDA and the regulated industry developed a cooperative relationship as never before and industry did the creative problem solving.

“In the current situation, FDA likely has its hands full in generally improving its state of preparedness and ability to respond to a bioterrorism emergency. Increased inspection of imported foods also will stress FDA’s existing work force and its program priorities will shift dramatically.

“Recognizing that the level of sophistication in the response to potential bioterrorism will vary with the size of a given company, among other factors, there seem to be some common points for food growers, packers, shippers and processors to consider in the light of current circumstances.

“In the absence of better knowledge about the nature and seriousness of a threat, the distinction between under-reaction and over-reaction is blurred.

“A strong focus on facility and personnel security is a must. Where possible, background checks for all personnel should be required. No one who is not so authorized should have access to the finished food product.

“Do you know who is delivering raw material to your facility and who is transporting the finished product out? What security precautions are those entities taking?

³ http://edis.ifas.ufl.edu/BODY_FS091

⁴ D.L. Archer is a professor in the Food Science and Human Nutrition Department of the Institute of Food and Agricultural Sciences at the University of Florida, Gainesville. F.H. Degnan is a partner in King & Spalding and a distinguished lecturer at the Catholic University School of Law in the United States.

“Anti-tampering plans, if they exist, should be re-evaluated. If they do not exist they should be developed, adopted and implement.

“GAPs (Good Analytical Practices), GMPs (Good Manufacturing Practices) and HACCP (Hazard Analysis and Critical Control Point system) plans should be re-evaluated. Are they sufficient to protect from purposeful acts of food contamination? Do they cover the following points: raw material integrity, packaging integrity, air flow systems, end-line activities, storage and transportation.”

Archer and Degnan then list procedures and practices that already should be commonplace in food companies. Consumer complaint handling practices should be checked and fine tuned as should product recall procedures. Companies should know whom to contact at their local enforcement authority—the FDA office in the United States—and how to reach them. They should also know who could provide quick access to analytical methods or microbiological or chemical analyses and improve preparedness among all employees through regular training or simulations.

Companies should also be aware that they should deal differently with a possible bioterrorism event. In any such situation, the enforcement agency should be contacted early in any investigation.

They note: “False alarms will be one price of vigilance.” Nevertheless, companies should be aware that the enforcement authorities are likely to be in a helpful mode because everyone recognizes that terrorism is the fault of the terrorists and not that of a farm or a food company.

“Large companies will likely have the resources to take a risk-analysis approach to their operation and use a team of experts to devise prevention strategies, intervention strategies, containment strategies and education strategies . . . aimed at dealing with possible bioterrorism.

“The sharing of strategies and experience among companies with similar attributes, or sharing facilitated by trade organizations will strengthen the whole of the effort and should be encouraged by government. At all costs, complacency needs to be avoided for, as time passes, the spectre of possibly more and more sophisticated terrorist acts looms.”

Much useful advice and guidance can be obtained from various Internet sites, especially those of major governments as well as bodies like the World Health Organization (WHO). Obviously, prominent international companies and heavily advertised products are the most likely targets but it is sensible for even the smallest business to be aware of these sources of information and advice.

The WHO has published a 30-page document entitled *Terrorist Threats to Food*. It can be downloaded from the Food Safety Department’s site.⁵ In the Introduction, the document warns that threats from terrorists, criminals, and other anti-social groups who target the safety of the food supply are already a reality. It also notes that, in May 2002, the 55th World Health Assembly adopted a resolution expressing serious concern about threats against civilian populations by deliberate use of biological, chemical or radionuclear agents. The purpose of the publication is to provide policy guidance to member states

⁵ <http://www.who.int/fsf/>

for integrating consideration of deliberate acts of sabotage of food into existing prevention and response programs. It details special measures for consideration by the food industry.

In the United States, the Bioterrorism Act of 2002 became law because it was considered necessary following the events of September 11, 2001, which reinforced the need for security to be enhanced. The Act deals with national preparedness for bioterrorism and other public health emergencies; enhancing controls of dangerous biological agents and toxins; protecting the safety and security of food and drug supply; and also water security and safety. The best starting point to check details of the Act is its home page.⁶ It lists the relevant web sites of the federal government as well as those of state and local government and provides copious guidance and advice.

America's first bio-attack

The largest germ warfare attack in America's history occurred in 1984. In a bizarre plot to influence the result of an election for a county commissioner, followers of a 10 000-member religious sect contaminated salad bars in 10 restaurants in The Dalles, a small town in Oregon, with *Salmonella*. As a result, 751 people became ill and 45 people were hospitalized.

The Bhagwan Shree Rajneesh cult reproduced the *Salmonella* strain and slipped it into salad dressings, fruits, vegetables, and coffee creamers at the restaurants.

When that attack proved successful they plotted to take over the Wasco County Commission by making so many people ill on election day that they would be unable to vote, thereby paving the way for the cult's own candidates to be elected.

However, that threat did not materialize. The cult collapsed in 1985 after its leader was convicted of immigration fraud and deported to India, where he died in 1990. His top aide was convicted for masterminding the *Salmonella* attack and other crimes.

One of the largest naturally occurring food-borne outbreak's in American history infected some 220 000 people in 1994. It was the result of a national brand of ice cream becoming contaminated with the same pathogen at the factory.

A 49-page report entitled *Agroterrorism: Threats and Preparedness*⁷ was submitted to the US Congress on August 13, 2004. It was prepared by Jim Monke, an analyst in agricultural policy at the Resources, Science and Industry Division of the Congressional Research Service. In it he writes: "The potential of terrorist attacks against agricultural targets (agroterrorism) is increasingly recognized as a national security threat, especially after the events of September 11, 2001. Agroterrorism is a subset of bioterrorism, and is defined

⁶ <http://www.fda.gov/oc/bioterrorism/bioact.html>

⁷ <http://www.fas.org/irp/crs/RL32521.pdf>

as the deliberate introduction of an animal or plant disease with the goal of generating fear, causing economic losses and/or undermining stability. Attacks against agriculture are not new and have been conducted or considered by both nation-states and substate organizations throughout history.

"The result of an agroterrorist attack may include major economic crises in the agricultural and food industries, loss of confidence in government and possibly human casualties. Humans could be at risk in terms of food safety or public health, especially if the chosen disease is transmissible to humans (zoonotic). Public opinion may be deliberately sensitive to a deliberate outbreak of disease affecting the food supply. Public confidence in government could be eroded if authorities appear unable to prevent such an attack or to protect the population's food supply.

"Agriculture has several characteristics that pose unique problems for managing the threat. Agricultural production is geographically dispersed in unsecured environments. Livestock are frequently concentrated in confined locations, and then transported and commingled with other herds. Pest and disease outbreaks can quickly halt economically important exports. Many veterinarians lack experience with foreign animal diseases that are resilient and endemic in foreign countries.

"Agriculture and food production generally have received less attention in counter-terrorism and homeland security efforts. But more recently, agriculture has garnered more attention in the expanding field of terrorism studies. Laboratory and response systems are being upgraded to address the reality of agroterrorism."

The report also pointed out that the number of lethal and contagious biological agents was greater for plants and animals than for humans. Most of the diseases were environmentally resilient, endemic in foreign countries and not harmful to humans. This made it easier for terrorists to acquire, handle, and deploy the pathogens.

It continued: "Thus, the general susceptibility of the agricultural and food industry to bioterrorism is difficult to address in a systematic way due to the highly dispersed yet concentrated nature of the industry and the inherent biology of growing plants and raising animals."

However, the report also made the point that because an agroterrorist attack might not necessarily cause human casualties, be immediately detectable or have the 'shock factor' of an attack against the more visible public infrastructure or human populations, it might not be the terrorist's first choice of targets. Nevertheless, some types of agroterrorism could be relatively easily achieved and have significant economic impacts. Thus, the possibilities were treated seriously.

Health Canada's Population and Public Health Branch⁸ is another example of a government agency providing useful advice in connection with the measures being taken to protect the security of the nation's food supply. Much additional information can also be obtained by a web search using the keyword 'bioterrorism'. Many sites will be listed, including those of respected universities and

⁸ <http://www.hc-sc.gc.ca/pphb-dgspsp/publicat/ccdr-rmtc/01vol27/dr2704ea.html>

other bodies who have made special studies of the implications of a bioterrorist threat or attack.

Many Internet resources are listed on the site of the Institute for Bio-security at Saint Louis University School of Public Health.⁹ At a different site,¹⁰ the Institute also lists key documents, including documents produced by a wide variety of professional organizations.

Even though businesses should be aware of the threat posed by bioterrorism, international terrorists are more likely to resort to conventional methods as their first choice, like the use of explosive devices. International terrorists are patient. They do not plan outrages to occur on the anniversaries of particular events. They wait for an opportunity to strike when circumstances are right for them and they are unlikely to be caught. The events of 9/11 and the outbreaks of animal diseases like foot and mouth disease and bird flu have taught them that a comparatively small or highly targeted attack can have devastating effects on an industry, a country or even a number of countries.

⁹ <http://www.bioterrorism.slu.edu/bt/internet/academic.htm>

¹⁰ http://www.bioterrorism.slu.edu/bt/key_ref/professional.htm