

CHALLENGES OF INTERNATIONAL TRADE: BALANCING SECURITY AND COMMERCE

Michael A. Kuliasha
Oak Ridge National Laboratory
Oak Ridge, Tennessee, USA
(865) 574-4169 kuliashama@ornl.gov

ABSTRACT

There was an old saying in the nuclear industry that stated that *an accident anywhere was an accident everywhere*. The interconnected nature of global trade in a post-9/11 world is presenting the same dilemma as the U.S. tries to balance security and commerce when each day thousands of cargo shipments arrive at more than 300 U.S. ports of entry from all over the world. Managing the risks of terrorism inherent in a global transportation system without disrupting commerce is a major challenge for the U.S. and its trading partners. A number of initiatives are underway to implement a multi-layered approach to homeland security in the context of international trade. Many elements of this security strategy are dependent on new technologies that are currently under development. Technologies under development in the areas of information technology, screening and inspections systems, chain-of-custody and tamper detection, crisis management, and consequence management are described and related to overall security. Benefits beyond homeland security resulting from the deployment of these technologies are also discussed.

NATURE OF BIOTERRORISM THREAT

The anthrax letter attack that started in September 2001 was a seminal event in the history of terrorism in the U.S. because bioterrorism moved from a threat to reality. The overall magnitude of the attack was small. Four anthrax letters were recovered, three additional letters are presumed given the locations of contamination, 22 cases of anthrax were confirmed (11 inhalation and 11 cutaneous), and 5 of the inhalation cases were fatal.¹ While the dimensions of the attack were modest, the anthrax decontamination facts are staggering: 23 sites were contaminated, 7 of which are still contaminated; 6000 samples and 30 tons of waste were generated from the Senate Office Building alone; \$500 million has been spent on decontamination so far, with \$150 million having been spent on Brentwood postal facility alone (which is still closed); and current estimates are that decontamination expenditures will exceed \$750 million before the clean-up is completed.²

The facts surrounding the anthrax letter clean-up highlight a disturbing reality of terrorism, namely a little terrorist money can force an expensive response. Also, an attack anywhere in the world is likely to prompt a response everywhere in the world. The situation is very analogous to that faced by the nuclear power industry over the years where it has been said that *an accident anywhere is an accident everywhere*. Thus, even though the outcome of the war on terrorism is not in doubt, the real challenge may be how do we keep from losing while winning?

To provide for economic security in addition to homeland security, the U.S. strategy must recognize that the benefits of appropriately designed security systems go beyond security. For example, if shipments are secure and tracked in real-time, production and distribution will benefit from dramatically improved logistics. The National Institutes of Health has stated that biodefense research will be a boon to the public healthcare system because the research will apply to fighting infectious diseases. Pathogen detection systems will greatly improve food safety. First responders who are better equipped and trained and who have interoperable communications systems will be much more effective in responding to routine emergencies in addition to terrorist events. Advanced monitoring systems for chemical and biological attacks can also be used to monitor environmental quality. Improved cyber security will enable on-line commerce and new forensic techniques will improve law enforcement.

The threat of bioterrorism and biowarfare are not new. In particular, the Department of Defense (DOD) has had a robust program in chemical and biological warfare for many years.³ However, bioterrorism is more difficult to protect against than biowarfare for several reasons: potential bioterrorism agents are more numerous than tactical agents; the civilian population is significantly more diverse than the military with regard to age and health; military plans emphasize vaccine prevention which becomes much more difficult when you consider the host of agents beyond the six on the Centers for Disease Control and Prevention (CDC) Category A agents list; and civilian attacks will be sudden and unexpected. However, many of the scientific advances that have been sponsored by the DOD Chemical and Biological Defense Program are applicable to bioterrorism.

Homeland security budget requests for the last two fiscal years put much more emphasis on bioterrorism relative to chemical and nuclear weapons of mass destruction (WMD). Nuclear weapons require extensive infrastructure to produce. Chemical weapons require greater quantities of material to produce mass casualties. Chemical and nuclear weapons are not self-replicating after an attack. Biological weapons are relatively easy to manufacture and bioterrorism infrastructure can be hidden within legitimate health infrastructure. A biological attack may not be immediately apparent, giving an infectious agent time to spread. Also, biological agents can be used against crops and livestock inflicting economic damage and threatening food supplies.

STRATEGY FOR REDUCING BIOTERRORISM THREATS

Homeland security is like quality assurance — you can't inspect it in at the end. Security is the result of a process that starts with information and continues through consequence management. Because of the global economy, the movement of people, knowledge, and materials is an international problem that will require international cooperation to solve. Even if successful on the international front, the U.S. must also prepare for domestic threats.

The *National Strategy for Homeland Security*⁴ lists three priorities for homeland security:

- Prevent terrorist attacks within the United States;
- Reduce American's vulnerability to terrorism; and
- Minimize the damage and recover from attacks that do occur

The document goes on to outline a plan for homeland security that seeks to create a layered defense using a risk management approach. The plan recognizes that it is not feasible to defend against all conceivable events and places emphasis on catastrophic events. The consequences of those events that do occur will be minimized through prior mitigation planning and effective emergency response.

To achieve its three priorities, the *National Strategy for Homeland Security* identifies 6 critical mission areas:

- Intelligence and Warning
- Border and Transportation Security
- Domestic Counterterrorism
- Protecting Critical Infrastructure and Key Assets
- Defending Against Catastrophic Threats
- Emergency Preparedness and Response

These priorities and missions can be regrouped into a biological threat reduction strategy that consists of three main elements:

- Prevention
 - Reduce access to dangerous pathogens
 - Limit access to production capability
 - Improve intelligence
 - Keep dangerous people and materials out
- Preparedness
 - Vaccines and diagnostics
 - Equipment and drug stockpiles
 - Planning and training
 - Improve facilities
- Emergency Response
 - Detection and surveillance systems
 - Communications, command and control, logistics support

PREVENTION

Biological weapons are relatively easy to manufacture, requiring straightforward technical skills, basic equipment, and a seed stock of pathogenic microorganisms. While efforts have been underway for many years to control the production of biological weapons through treaties, only recently has attention turned to securing potential feed stocks of many pathogens. Because many of the pathogens of interest are the subject of active medical research programs, there are numerous potential sources for feed stocks.

On June 12, 2002, President Bush signed the Public Health Security and Bioterrorism Preparedness Response Act of 2002 (Public Law 107-188). In response to PL 107-188, the CDC has implemented the Select Agent Program. The Select Agent Program requires registration of facilities including government agencies, universities, research institutions, and commercial entities that possess biological agents or toxins deemed a threat to public health. Section 213(b) of PL 107-188 requires all persons possessing biological agents or toxins deemed a threat to animal or plant health to notify the U.S. Department of Agriculture (USDA). The Animal and Plant Health Inspection Service has been designated as the USDA agency responsible for providing guidance on this notification. Through the registration of more than 300 laboratories, the Select Agent Program has significantly increased oversight and security of pathogens.

Of course, securing domestic sources of pathogens is not particularly useful if there are not comparable international programs. Securing pathogens at their source will be much more effective than depending on border and transportation security to keep them out. Particularly with biological threats, there is the question of what one can realistically hope to achieve with border and transportation security. Even nuclear materials, which are much easier to detect than pathogens, present daunting challenges for border and transportation security. In addition to the nuclear detection challenges presented by time, distance, and shielding, interdiction is further complicated by the fact that in the U.S. alone there are 3 million legitimate radioactive material shipments each year (>7500/day), and most are exempt from external markings. Add in the many natural products that are radioactive and it becomes clear why identification must be used together with detection to limit false positives.

While it is unlikely that border and transportation security will intercept a small tube of culture, there is a definite role for border and transportation security in biological threat reduction. Threats are created by both people and materials, and keeping dangerous people out is the same challenge regardless of the type of threat. There is also the question of large vs small quantities of materials. As quantity goes up, so does the probability of detection. The larger the quantity of threatening material, raw material, or production equipment, the more likely it is to be detected either in production, transportation, or deployment. Terrorists prefer large quantities because there is a consequence multiplier effect if they succeed in overwhelming the response system. Finally, there is no point in making the borders any more secure than appropriate given the difficulty of acquiring the same capability domestically.

A brief look at key transportation statistics⁵ shows why it is critical to use intelligence and information technology to improve inspection statistics above random sampling. 730 million people travel on commercial aircraft each year. 700 million pieces of luggage are screened for explosives. 500 million people cross the border annually into U.S. of which 330 million are non-citizens. 11.2 million trucks and 2.2 million rail cars cross into the U.S. each year. 7,500 foreign flagships make 51,000 calls in U.S. ports annually. 200 million sea containers move annually between the world's seaports and 6 million containers are unloaded at 361 U.S. ports of entry.

There are two components to the information and intelligence challenge presented by these numbers. First, systems must be in place to collect the data of interest on each transaction. Second, tools are needed to comb through massive and dissimilar data sets to recognize suspicious events from innocent events. A number of initiatives are underway to provide data on international movement of people and cargo. For example, Customs is now requiring that sea carriers provide shipping manifests for U.S.-bound cargo 24 hours before loading at foreign ports and airlines are required to electronically submit passenger lists for all flights to the U.S. The Coast Guard requires 96-hour advance notice of arrival of all vessels heading to U.S. ports and has deployed small, elite marine safety teams to look into any suspicious activity.

How all this data will be used to enhance border and transportation security is the subject of several massive information technology initiatives. Customs is developing the Automated Commercial Environment (ACE) at an estimated cost of \$1.3 billion. The genesis of ACE is the International Trade Data System (ITDS) which is an interagency effort that started in 1995. Customs has integrated ITDS into ACE. ACE is currently focused on cargo import and export operations but in the future will expand to include passenger processing, investigative and intelligence support, human resources, and financial management programs. The goal of the project is to provide a federal data base containing information on all aspects of an international transaction — cargo, conveyance and crew.

The feasibility of systems such as ACE has been previously demonstrated. The U.S. Department of Transportation (DOT) has demonstrated the Electronic Supply Chain Manifest System (ESCM). Jointly funded by DOT's

Intelligent Transportation Systems program, the Federal Aviation Administration, and the state of Illinois, ESCM allows positive identification of the person responsible for the cargo and tracking capabilities for cargo movement within transportation modes as well as from one mode to another.⁵ One of the more important findings of the project is that appropriately designed security systems can dramatically improve business processes.

Once systems are in place to collect and process data on people and cargo entering the U.S., inspection and detection technologies are needed to verify that they are non-threatening and accurately identified. It is greatly preferable to inspect a cargo at the point of origin during loading rather than attempt to inspect a loaded container at its point of entry or final destination where it may be too late to do anything about a dangerous cargo. In January 2002, Customs launched the Container Security Initiative (CSI) with the objective of enhancing the security of sea cargo containers. CSI involves placing Customs inspectors at major foreign seaports to pre-screen cargo containers before they are shipped to America. Customs officials, working with their foreign counterparts, will be in a position to detect potential WMD in U.S.-bound containers at these foreign ports. Since nearly 70 percent of all U.S.-bound sea containers pass through 20 major seaports around the globe, Customs is initially focusing on these 20 ports.

There are two additional components to ensuring border and transportation security. The first component is inspection and detection technologies to ensure that baggage and cargo do not contain dangerous materials. The second component is tamper detection and chain-of-custody systems that ensure that dangerous materials are not introduced into baggage and cargo after inspection.

To date, baggage and cargo inspection and detection systems have relied primarily on x-ray systems and visual inspection. Baggage x-ray systems are deployed at airports and large x-ray systems for containers and trucks are deployed at select ports and border crossings. Congress mandated in the Aviation and Transportation Security Act that airports screen all baggage for explosives. Approved methods include explosives detection and explosives trace detection machines, canine teams, hand searches, and passenger-bag matching. The experience with explosives detection systems has shown high rates of false positives to the extent that Transportation Security Administration inspectors are inspecting many more bags by hand.⁶ The National Nuclear Security Administration is the lead government agency for nuclear nonproliferation and has both domestic and international radiation portal monitors. Customs is installing radiation detection equipment at border crossings and ports.

Unfortunately, the ability to definitively detect and identify pathogens in a reasonable amount of time in air, soil, and water is in its infancy and there are no detection systems capable of interrogating a sealed container. DOD has fielded a number of biowarfare point detection systems including the Biological Integrated Detection System and is in pre-production testing of a number of other systems including the Joint Biological Point Detection System and the Block II Chemical Biological Mass Spectrometer. A number of efforts are underway to modify these biowarfare detectors for homeland security applications. In addition to DOD, the development of advanced biological detection systems is being sponsored by the Department of Homeland Security (DHS) and the National Institutes of Health. However, the current circumstance is that there are no means to detect and identify biological threats in baggage and cargo.

After inspection, tamper detection and chain-of-custody systems are needed to ensure that dangerous materials are not introduced into baggage or cargo. Operation Safe Commerce (OSC) is a Customs and DOT initiative to provide a test-bed for new security techniques to increase the security of container shipments from point of origin to final destination. The nation's top three ports, Los Angeles/Long Beach, New York/New Jersey and Tacoma/Seattle are serving as test-beds for new security techniques that have the potential to increase the security of container shipments. DOT and Customs will use the program to identify existing vulnerabilities in the supply chain and develop improved methods for ensuring the security of cargo entering and leaving the United States. Those security techniques that prove successful under the program will then be recommended for implementation system-wide.

PREPAREDNESS

U.S. bioterrorism preparedness efforts have two major components. The National Institute of Allergy and Infectious Diseases (NIAID) within the National Institutes of Health is leading the effort on basic research and the development of medical interventions including vaccines and therapeutics. CDC is leading efforts on surveillance and detection, improving health infrastructure, planning, and training local response teams. CDC has historically had the lead for maintaining the National Pharmaceutical Stockpile. However, Congress recently transferred

responsibility for maintaining vaccine and medical supply stockpiles from CDC to DHS and the stockpile has been renamed the Strategic National Stockpile.

NIAID research programs in bioterrorism are well-described in two plans.^{7,8} Major research efforts are underway to develop vaccines or improved vaccines for all six agents on CDC's Category A agents list and a number of agents on the Category B list. Vaccines currently funded for development include:

- Tularemia Vaccine
- Smallpox Vaccine
- Recombinant Botulinum Vaccine
- Plague Vaccine
- Multivalent Eastern Equine Encephalitis
- Western Equine Encephalitis
- Venezuelan Equine Encephalitis Vaccine
- Ricin Vaccine
- Next Generation Anthrax Vaccine
- Staphylococcal Enterotoxin(s) Vaccine

A key component of bioterrorism infrastructure is the Strategic National Stockpile, which Congress recently transferred from CDC to DHS. The stockpile contains drugs, vaccines, and other medical supplies and equipment that can be delivered to any place in the country within 12 hours of a request for assistance. The President's FY04 budget request includes \$400 million to purchase additional drugs, vaccines, and equipment. The FY04 budget request also includes \$900 million for DHS to pre-purchase vaccines and medication for biodefense under an initiative called Project Bioshield.

CDC's strategy for responding to infectious diseases focuses on four goals: improving disease surveillance and outbreak response; supporting research to understand and combat emerging infectious threats; preventing infectious diseases by implementing disease control programs and communicating public health information; and rebuilding the infectious disease-control component of the public health infrastructure.⁹ CDC has a grant program to help upgrade state and local public health jurisdictions' preparedness for and response to bioterrorism, other outbreaks of infectious disease, and other public health threats and emergencies.¹⁰ The priority areas are immunization and infectious diseases, environmental health, public health infrastructure, and surveillance and data systems.

EMERGENCY RESPONSE

On June 12, 2002, President Bush signed the \$4.6 billion Public Health Security and Bioterrorism Bill that primarily focused on the development of vaccines and related health care issues. In the press release, Bush is quoted as saying "Biological attacks can be carried out quietly. Our health care professionals are likely to recognize that there has been an attack. The speed with which they detect and respond to a threat to public health can be the difference between containment and catastrophe."

It was a fortuitous set of circumstances that resulted in the diagnosis of the first inhalation anthrax case in Florida and the isolation of *Bacillus anthracis* at the patient's place of work in less than a week. It is a sobering fact that alert clinicians are the first line of warning of a bioterrorism attack. CDC has a number of initiatives underway to establish surveillance networks that comb reported data for unusual illnesses or deaths. However, rather than waiting for human "canaries" to start displaying symptoms, what is desperately needed is a nationwide, real-time system for detecting and responding to biological attacks.

The Biological Aerosol Sentry and Information System (BASIS), developed by Los Alamos National Laboratory and Lawrence Livermore National Laboratory, uses distributed sampling units to collect aerosols. The filters are collected periodically and taken to a mobile field laboratory for testing and analysis. DNA in the samples is analyzed using polymerase chain reaction techniques to identify an organism based on its genetic signature. Depending on the collection frequency and analysis load, the system can detect known pathogens within 24 hours. With a 24-hour identification time, the objective of the system is to detect an attack to initiate timely treatment. The BASIS system was deployed at the Winter Olympics in Salt Lake City and DHS has recently announced expanded deployment as the Bio-Watch biosurveillance network.¹¹

While detect-to-treat surveillance systems are currently the leading-edge of what is technically feasible, what the emergency response community would like to have is a real-time detection system for bioterrorist attack. What is currently lacking are reliable, real-time detection and identification systems for biological agents. However, as mentioned above, DOD and others have been supporting the development of a number of near real-time (few minutes) biological sensor systems including the Block II Chemical Biological Mass Spectrometer being developed at Oak Ridge National Laboratory (ORNL). Anticipating that one or more of these biological sensor developments will be successful, recognizing that radiation detection is mature, and aware that a number of chemical agent sensors are either commercially available or in testing, ORNL is developing a second-generation sensor system for chemical, biological, or nuclear attacks called SensorNet. SensorNet is being developed with partners American Tower Corporation and the National Oceanic and Atmospheric Administration. SensorNet is a concept for an integrated, real-time system for detection, emergency response, and consequence management utilizing existing cell phone tower infrastructure. SensorNet is envisioned as a modular system consisting of 4 key components. Sensors for chemical, biological, and nuclear hazards are deployed on cell towers and other locations and connected to a central response center using existing communications infrastructure. Upon detection, detailed environmental transport and population modeling are used together with measured data to predict population at risk. Next, an integrated command and control system is used to advise at-risk population on appropriate emergency response and to dispatch first responders. Finally, a logistics system supports effective utilization of manpower and materials throughout the emergency. The communications backbone and common data highway are being developed to be plug-and-play and independent of any particular sensor technology, so that as improved sensors or models become available, they can be integrated into the system. SensorNet was field tested on March 12, 2002, in 3 Tennessee cities and a number of demonstration nodes are currently operating.

SUMMARY

The U.S. is faced with a delicate balancing act. A terrorist event anywhere in the world can prompt an expensive response everywhere. Also, because of the interconnected nature of the global economy, security measures that impede commerce increase homeland security at the expense of economic security. Homeland and economic security can both be achieved if security measures are implemented such that they provide benefits beyond security, such as container tracking enabling improved logistics or bioterrorism research improving human health.

The *National Strategy for Homeland Security* outlines a homeland security strategy that seeks to create a layered defense using a risk management approach. The priorities and missions can be regrouped into a biological threat reduction strategy that consists of three main elements: prevention, preparedness, and emergency response. Prevention initiatives include: the Select Agent Program that limits access to dangerous biological agents and toxins within the U.S.; the Automated Commercial Environment that will provide detailed data on all aspects of an international transaction including cargo, conveyance and crew; the Container Security Initiative that is inspecting containers before they are loaded in foreign ports; and Operation Safe Commerce that is providing a test-bed for new security techniques to increase the security of container shipments from point of origin to final destination. These initiatives are being supported by new technologies for inspection, tracking, and tamper detection. Technologies for detecting and identifying nuclear materials are available. Some sensors for explosives and chemical agents are commercial while improved technologies are in pre-production testing. Sensors and diagnostics for detecting and identifying biological agents and toxins are the least mature.

Preparedness initiatives include the development of new vaccines and therapeutics being led by NIAID while CDC is leading efforts on surveillance and detection, improving health infrastructure, planning, and training local response teams. DHS is now responsible for the Strategic National Stockpile of drugs, vaccines, and other medical supplies and equipment that can be delivered to any place in the country within 12 hours.

Emergency response is being supported by the symptom surveillance systems implemented by CDC to detect a bioterrorism event. Detect-to-treat biosurveillance systems such as BASIS and Bio-Watch are being deployed that will provide confirmation of a bioterrorist attack within 24 hours and real-time detect-to-respond sensor systems for chemical, biological, and nuclear attacks such as SensorNet are under development.

REFERENCES

1. Jernigan DB, Raghunathan PL, Bell BP, Brechner R, Bresnitz EA, Butler JC, et al., Investigation Of Bioterrorism-Related Anthrax, United States, 2001: Epidemiologic Findings, *Emerging Infectious Diseases*, October 2002, p. 1-2. Available from: URL: <http://www.cdc.gov/ncidod/EID/vol8no10/02-0353.htm>
2. Zarba, C., Overview of EPA Biodefense Research Priorities, Programs, and Funding , *Federal Biodefense Research FY2003, December 3-4, 2002*, Washington, DC.
3. Department of Defense Chemical and Biological Defense Program, *Volume 1: Annual Report to Congress*, April 2002.
4. Office of Homeland Security, *The National Strategy for Homeland Security*, July 2002.
5. Bureau of Transportation Statistics, *National Transportation Statistics 2001*, BTS02-06, July 2002.
6. Airports to Search More Bags By Hand, in Shift of Procedure , *Wall Street Journal*, November 5, 2002.
7. National Institute of Allergy and Infectious Diseases, *NIAID Research Agenda for CDC Category A Agents*, National Institutes of Health, February 2002.
8. National Institute of Allergy and Infectious Diseases, *NIAID Strategic Plan for Biodefense Research*, National Institutes of Health, February 2002.
9. Centers for Disease Control and Prevention, *Preventing Emerging Infectious Diseases: A Strategy For The 21st Century*, U.S. Department of Health and Human Services, October 1998.
10. Centers for Disease Control and Prevention, *Guidance for Fiscal Year 2002 Supplemental Funds for Public Health Preparedness and Response for Bioterrorism*, Announcement Number 99051 Emergency Supplemental, February 15, 2002.
11. Kathy Sawyer, Biowarfare Monitors Are Deployed in U.S. , *Washington Post*, January 23, 2003, p. A06.