Viewpoint

Needed: A Nuclear Dragnet for Homeland Security?

JAMES E. DOYLE

Dr. James E. Doyle is a technical staff member in the Nonproliferation and International Security Division at Los Alamos National Laboratory. His professional focus is on systems analysis, strategic planning, and policy development. Dr. Doyle holds a Ph.D in International Security Studies from the University of Virginia. Previously, Dr. Doyle was a senior policy analyst at Science Applications International Corporation.

Since the devastating September 11, 2001, attacks, America has awakened to the possibility of an even greater catastrophe that could result should terrorists strike with nuclear or radiological weapons. Whereas the explosive energy of the aircraft impacts on the World Trade Center and the Pentagon was about 500 tons of TNT, a terrorist-constructed improvised nuclear device (IND) could yield explosive energy equivalent to several *thousand* tons of TNT. Such a device, if detonated in lower Manhattan, could level every building in the Wall Street financial area, instantly killing many tens of thousands of people. In addition, a significant portion of total military medical, airlift, and ground transportation assets could be needed to respond to a powerful nuclear explosion in one or more American cities. A successful attack on Washington, DC, could destroy elements of our national leadership and degrade the capabilities of some federal agencies. The toll of the human losses and the psychological impact would be incalculable. Economic consequences would dwarf those resulting from the 9/11 attacks.[1] Fundamental civil liberties, free social patterns, and open commerce might be challenged and constrained in the aftermath of a devastating attack. In short, a successful nuclear terrorist attack could severely disrupt our bases of national power and degrade our quality of life.

A NEW STRATEGIC ENVIRONMENT

Consequently, the United States faces a completely changed security environment. During the Cold War the only forces that could inflict such strategic damage on the U.S. homeland were the nuclear weapons of the former Soviet Union, and to a lesser extent those of China. Today the global diffusion of nuclear materials and technology, and of knowledge relevant to the construction of nuclear or radiological devices, has created the possibility that small groups of individuals, with or without the sponsorship of a state, can pose catastrophic threats to the security of the United States and its allies. In the new strategic environment, uncontrolled nuclear materials are the strategic weapons and terrorists are the delivery vehicles.

This threat is real, and perhaps worsening. The National Nuclear Security Administration (NNSA) maintains a team of technical specialists who help assess the credibility of communicated nuclear threats against the United States. Since 9/11, the number of such threats has increased.

Terror organizations have already expressed interest in conducting nuclear attacks against the United States and may be trying to execute such attacks even now. In 1998 Osama Bin Laden asserted that acquiring weapons of mass destruction was a religious duty and part of an edict calling for attacks on Americans throughout the world.[2] Evidence that Al-Qaeda was investigating the materials and technologies for nuclear terrorist devices was discovered in Afghanistan.[3] In March 2002, Jose Padilla, a U.S. citizen and Al-Qaeda convert, reportedly expressed his interest in conducting a nuclear attack against America to Abu Zubaydah, Al-Qaeda's operations chief.[4]

RESPONDING TO THE THREAT

The U.S. government has recently acknowledged the critical need to improve its defense and response capability against terrorist nuclear threats. For example, the National Strategy For Homeland Security, issued by the White House on July 16, 2002, asserts, "Our top scientific priority must be preventing terrorist use of nuclear weapons."[5] In addition, the National Academy of Science's recent report *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* asserts: "The development of a well-tested, national integrated detection network (for nuclear materials) would be a powerful component of the layered homeland defense system."[6]

Stopping a nuclear terrorist attack on the U.S. homeland will indeed require layered, in-depth defensive capabilities. What capabilities exist for such an effort? The first layer of defense consists of programs and technologies to prevent the acquisition of nuclear weapons or nuclear materials by adversaries.[7] All states that possess nuclear weapons and materials understand the responsibility of securing them from theft. Unfortunately this task requires a commitment of resources, trained personnel, and effective administration that are beyond the capabilities of some states. For a decade the United States has been providing financial and technical assistance to Russia, Ukraine, and Kazakhstan to improve the security of their nuclear materials in the aftermath of the Soviet collapse. These efforts are being sustained and expanded where appropriate.[8] There are still serious concerns among national security analysts that nuclear weapon and material security improvements are urgently needed in countries such as India and Pakistan. At present there is no official U.S. program of assistance to those states.[9]

According to the International Atomic Energy Agency (IAEA), 25 kilograms (kg) of U-235 and 8 kg of plutonium (total element), is sufficient to make a nuclear explosive device. Unfortunately, these materials are produced in more than 15 countries worldwide and have been distributed to dozens of others for research purposes. States that have nuclear arsenals or large commercial nuclear power sectors have inventories of fissile materials ranging from tens to hundreds of metric tons.[10] There is also the possibility that rogue states such as North Korea or Iran could willingly supply or sell nuclear materials to terrorists planning to attack the United States.[11]

The materials and technology required to build radiological dispersal devices (RDD) or "dirty bombs" are much easier to obtain than those needed for a weapon producing a nuclear explosion.[12] An RDD causes no nuclear explosion, but instead uses chemical explosive or passive means to spread harmful radioactivity. It could cause severe economic disruption and panic in an urban area, without causing large numbers of fatalities. However, the IAEA reports that more than 100 countries may have inadequate controls to prevent or even detect the theft of radioactive materials needed for an RDD.[13]

Recognizing the inherent limitations of the first line of defense and the consequent risk that nuclear weapons or materials could be diverted from official control, the United States has created a second line of defense against nuclear terrorism. This layer is composed of equipment and training provided to many states across Europe, Russia, and other states of the former Soviet Union. The U.S. Second Line of Defense (SLD) program works with customs and border authorities in these states to improve their capabilities for detecting unauthorized transfers of nuclear materials across international borders. The United States has supplied radiation detection equipment for inspection of pedestrians, vehicles, and railcars and is beginning to work at large international ports. Training on the use and maintenance of this equipment and on cooperating with international organizations to prevent nuclear smuggling are also part of the assistance programs.

Like efforts to prevent the loss or theft of nuclear materials, SLD program efforts to stop nuclear smuggling will not be completely effective. Nuclear materials can still be successfully hidden within other cargo or transported around checkpoints. It is not fundamentally any more difficult to smuggle nuclear materials than to smuggle drugs, weapons, people, or other contraband—activities that nations have been trying to stop for thousands of years, unsuccessfully.

THE THIRD LAYER: DEFENSE OF THE HOMELAND

The discussion above leads to a troubling conclusion: It is likely that nuclear or radiological attacks against the U.S. homeland will be attempted, and this threat will persist for decades to come. This is because dangerous nuclear materials are widely used and dispersed throughout the world, current global controls over such materials are weak, and terror organizations committed to attacking the United States may already possess such materials. It is therefore critical to construct a third layer of defense, designed to detect and defeat nuclear terror attacks against the U.S. homeland.

Today only an extremely limited capability exists for this mission in the form of small teams of nuclear emergency response and special operations forces from NNSA and the Department of Defense (DoD). No single U.S. government agency or department has the designated lead responsibility for homeland defense against nuclear terrorism. Currently the Department of Homeland Security (DHS), the NNSA, and the DoD all have programs under way to address this threat, but an overall strategy for deployment of national defenses against nuclear terrorism has yet to emerge.

Can America build a national nuclear material detection and tracking system that can help prevent or mitigate the consequences of nuclear and radiological attacks on the U.S. homeland? What would be the major elements of such a system? What key uncertainties exist regarding its potential effectiveness?

Developing a Strategic Vision

A layered nuclear materials detection and tracking network could be the key hardware element of homeland defense against nuclear terrorism. Strategic defensive systems deployed during the Cold War provide some useful analogies. One such system was the Distant Early Warning (DEW) system, constructed as a top-priority effort to detect and track a possible Soviet attack from the north. This was an integrated warning system consisting of multiple, geographically spaced radar installations and multiple types of detection radars and communications links. It included the DEW line on the outer fringe of northern Canada and Alaska, the Pinetree line, and the Mid-Canada line.

Another layered, networked element of our Cold War defense was the Sound Surveillance System (SOSUS). This system was a network of fixed and mobile hydrophones providing deep-water, long-range detection capability for enemy nuclear submarines. SOSUS detectors were installed across the ocean bottom at key locations throughout the world. The objective of this system was to track continually strategic submarines that threatened the United States, thus providing target information in the event of a conflict or upon detection of an attack. The SOSUS system enjoyed tremendous success during the Cold War. Advanced elements of the system remain in service today.

While the DEW line and the SOSUS network were not barriers, they provided deterrence against an attack and, if an attack came, information for warning, assessment, targeting, and early interdiction that was critical to the effectiveness of the response. It is possible that, given the severity of the threat that we face from nuclear terrorism, investment in a robust nuclear material detection and tracking system could have enormous payoffs in terms of preventing or reducing the consequences of a nuclear terrorist attack.

The command center of a system for homeland defense against nuclear terrorism would itself be a system of multiple, integrated elements. One element would be a computer-based information system containing all information currently available on every state's inventory of dangerous nuclear materials and with updates to those inventories made on a continual basis. Most states with civil nuclear materials share some of this information with the IAEA, and there are international nuclear watchdog organizations that gather similar data. However, such an information system would also have to contain the best available intelligence estimates of nuclear material inventories not declared by states, and their locations. This information system would provide the baseline knowledge regarding quantities, forms, locations, and trends for global inventories of dangerous nuclear materials.

The key objective of this element of the system would be early detection of loss or theft of dangerous materials anywhere in the world. Many states may be willing to provide early notification to the United States or the IAEA regarding the loss of any dangerous nuclear materials. This information could immediately be transferred to the other elements of the U.S. homeland defense system. Such a cuing of the system, and a description of the missing materials, could greatly increase the probability of detection and recovery by the detector and response elements.

Another critical feature of a nuclear material detection and tracking system would be the interface with government counterterrorist and law enforcement agencies. As President Bush has said, "The gravest danger to freedom lies at the crossroads of radicalism and technology."[14]

Because extremist groups and smugglers have revealed their interest in nuclear materials, the capabilities that are used to identify and track terrorists must be integrated with those for tracking nuclear materials. Any information on terrorist plans, the individuals involved, their movements, and the type of materials they are seeking or possess could help in the detection and interdiction of a nuclear terrorist device. Even information on non-nuclear materials and types of containers that terrorists might have could provide clues about the kind of nuclear materials they possess or seek.

A third element of the homeland defense layer would be the ability to display, assess, and transfer real-time data from nuclear materials detectors deployed throughout the United States. This layer would include the deployment of detectors at borders, ports, airports, and strategic chokepoints and around key assets such as large urban areas, critical infrastructure, national monuments, military bases, and government facilities. Mobile and wide-area detection networks could also be integrated into this national nuclear dragnet for random or focused searches.

Potential Benefits

The potential strategic benefits of a nuclear materials detection and tracking system could include:

- A capability to detect nuclear materials as they approach or enter our borders, military bases, or urban areas, so they could be interdicted before they are used in an attack
- The ability to identify the type of nuclear material that has been introduced, to help gauge the threat and select appropriate response measures
- Help in determining where threatening nuclear materials are likely or unlikely to be, given that some information about their movement is known, but not their precise location
- Ability to reduce the recovery time for lost or stolen material
- The capability to characterize the strength and type of nuclear explosion or radiological dispersal immediately after it occurs (this information could significantly reduce casualties and damage)
- The ability to identify the nature and origin of nuclear materials after an attack and, perhaps, some data on the path they took to their target; this would be vital to identifying all who took part in the attack and attributing the nuclear weapons or materials to their source, key to apprehending terrorists and preventing new attacks
- An improvement in the effectiveness of both random searches for materials and of warning systems that might issue alerts and trigger mitigating actions even when indicators of an attack are uncertain
- Better accountability for the movement and possession of nuclear materials, which could help deter and detect source loss or theft
- The ability of the U.S. Customs Service and other officials to verify that radioactive materials entering the country are bound for an intended, legitimate recipient, helping to prevent defensive measures from having too great an impact on commerce.

Current Limitations

While it is encouraging to consider the benefits that such a system could provide, it is also useful to identify its likely limitations. It is not currently possible to construct a system that would detect any and all attempts to smuggle nuclear materials into the United States. First, dangerous nuclear materials can be transported by road, rail, air, or sea, or even by a single individual using remote trails or tunnels, and can therefore be introduced into the United States at almost any point along our coasts and borders. Because the quantities of nuclear materials needed to build a weapon are so small and the quantity of freight and materials entering America daily is so vast, the problem, at one level, resembles the search for a "needle in a haystack."

Second, there is the problem of distinguishing threatening nuclear materials from those being used for beneficial purposes. For example, highly radioactive sources are used in everyday life to treat cancer patients, to preserve food, to check for welding errors in pipelines and buildings in industrial radiography, to generate electricity in remote locations, and a variety of other purposes. Radiological sources are essential to our societies, and it is impractical to secure and control every item, everywhere. Perfect information on the status of nuclear materials worldwide will never be available.

Third, even at established points of entry such as border crossings, ports, and airports, the flow of human and freight traffic is so large that scanning everything for the presence of nuclear materials is impossible without adding significant delay and cost to commerce.

Finally, some dangerous nuclear materials can be shielded from detection by covering them with common materials such as various metals or synthetic materials. Sophisticated adversaries will be aware of the technical limitations of detector systems and seek to exploit them.

Despite these limitations it appears possible that a significant portion of people and freight entering and traveling within the United States could be adequately screened for the presence of nuclear materials, including highly enriched uranium (HEU), without causing unacceptable delays or increased cost to commerce. In addition, radiological defense of point targets such as military bases, government facilities, selected urban areas, large public gatherings, monuments, and key infrastructure might be even more feasible as technology is developed and deployed.

A challenge for the technical and national security communities is to determine the relationship between increased radiation detection capabilities and the actual probability of interdicting unauthorized nuclear materials before they can be used in an attack. There are many unknown variables in this relationship. Detection capabilities are just one component of a potential national defense against nuclear terrorism. Other vital elements are intelligence data to focus search efforts and specialized personnel to isolate and stop the individual or vehicle carrying the nuclear material once it is detected. These limitations highlight the need for a layered, integrated system involving multiple capabilities for detection, assessment, and response.

BUILDING A NUCLEAR DRAGNET FOR HOMELAND SECURITY

Although never initiated with the fanfare or orchestration of President Reagan's 1983 Strategic Defense Initiative, work is under way on technologies and systems that could provide the foundations of a national defense system against nuclear terrorism. Early generations of these technologies have been used for several years around limited areas for defense against nuclear terror threats. The DHS is now coordinating an interagency effort to evaluate deployments of nuclear material detection systems for border and transportation security and wide-area urban defense.[15]

Specifically, the 2004 DHS budget contains $137 million to develop radiological/nuclear countermeasures that aim to prevent the importation, transportation, and subsequent detonation of a radiological or nuclear device within our borders. Key initiatives will be directed at the deployment, evaluation, and evolution of detection systems at ports of entry and within the transportation infrastructure; the development of advanced technologies for more effective crisis response; and the development of science-based consequence management approaches and tools.[16]

Some of the objectives of this research program are likely to be a better understanding of detector performance, selection of optimum locations and configurations for deployment, effective testing techniques and operating protocols, and a link between the detector network and other information systems and countersmuggling capabilities. Other objectives will no doubt include development of systems architecture designs and command system designs, and confirmation and interdiction strategies. Considering these aspects of a national nuclear material detection and tracking network early in the planning and development process may have significant payoffs later in terms of system performance.

A key element for homeland defense against nuclear terrorism is radiation detection technology. Radiation emitted by nuclear materials in an IND or an RDD can be measured via neutrons, gamma rays, or heat and differs in strength according to the isotopic composition of the material. For example, the neutrons emitted by plutonium, which can be used for nuclear weapons, are very strong and readily penetrate most other materials such as wood, plastic, and metal. Cesium and cobalt, possible ingredients in an RDD, are high-energy gamma emitters and penetrate most materials except dense materials such as lead. The radiation emitted by HEU, which is suitable for the construction of an actual nuclear bomb, is relatively weak and can be shielded from detection by enclosing the HEU in certain metals.

A variety of well-established technologies and procedures exist for controlling and accounting for nuclear materials.[17] These technologies can measure certain "signatures" produced by the particles of ionizing radiation emitted by nuclear materials without opening the container in which they are transported and stored. Measurement of these particles and their energies can potentially provide detailed information on nuclear materials within a container or vehicle, including its mass, isotopic composition, shape, age, and perhaps other attributes.

Detecting most nuclear materials within various shipping containers or vehicles can be done quite successfully if the container remains stationary and the detector can be brought close, to within a meter or so of the target. In the cases of a very large container, such as a maritime shipping containers, the detector may have to be moved along the length of the container to be effective in finding a small amount of nuclear material. Successful detection at greater distances and within very short periods of time as a vehicle passes by a detector is far more difficult. This is true in part because the number of detectable particles emitted by weapons-grade and radiological materials decreases by a factor of 100 as the target is moved from 1 meter to 10 meters away from the detector. The natural background radiation surrounding suspected nuclear materials is also large and variable throughout the vast range of locations in which detectors could be deployed.

Highly enriched uranium, a very dangerous material due to its suitability for the construction of a nuclear bomb, can be shielded from detection by common materials. This makes its effective detection impossible by passive means. Some other detection techniques that can activate the emission of particles from shielded uranium have promise but are more challenging than passive detection for a number of reasons, including risks of public exposure to radiation and the effects of radiation on shipped goods. However, active detection systems would not create any significant amount of additional radioactivity. Some of these approaches operate at extremely low doses, in some cases only a small increase above the natural background radiation levels.

Although it will remain impossible to search all cargo entering the United States, the chance of finding smuggled nuclear materials can be improved with techniques that can identify a subset of total incoming containers or vehicles more likely to have been used by terrorists. Such tools are already in use for interdiction of drugs, stolen goods, and even illegal immigrants. They allow evaluation of all information on a given shipment and identification of key characteristics—such as manufacturer, shipper, point of origin, shipping documentation, and end-user description—that could indicate higher risk.

The analysis of other signatures for nuclear materials may also hold some promise for improving detection. Dense material used to shield nuclear materials may present a detectable signal and tip inspectors to examine that shipment or item more closely. Important characteristics of many materials can be determined with advanced X-ray and gamma-ray equipment, already in use by U.S. customs. Acoustic signatures of liquid cargos in highly uniform containers may also provide useful data for detecting smuggled nuclear material.

In many cases the configuration of the cargo or its location enroute from shipper to receiver will help to determine which detection methodology should be used. For example, the long period aboard ship when a container is stationary could provide an opportunity to do longer-term measurements without causing any delay in the shipment.

CURRENT DETECTOR TESTING AND DEPLOYMENT

Several U.S. government agencies are currently testing or expanding radiation detection systems. The variety of commercially available nuclear materials detectors is growing to meet security demands. Specialized cargo scanners, vehicle and rail portal monitors, portable handheld radiation detectors, and wider-area detectors are all available or undergoing testing. Examples of this activity follow.

- In 2002, Lawrence Livermore National Laboratory researchers tested 19 commercially available handheld instruments that are being used or might be used by various government agencies to detect nuclear materials. One such instrument was a small portable gamma-ray detector called Cryo-3 that can accurately detect and identify nuclear materials without the need for cooling with liquid nitrogen, giving it an advantage over more traditional high-resolution gamma detectors.[18]
- FedEx shipping company is conducting trial runs of advanced radioactive monitoring sensors at its Indianapolis hub. However, it has been difficult to calibrate the sensors to detect undeclared shipments, while at the same time not creating false alarms for legal radioactive cargo such as pharmaceuticals.[19]
- The DHS is using the national laboratories to rapidly assess radioactive shipments detected by customs at U.S. points of entry. U.S. Customs has already installed more than 60 radiation detectors and is planning an additional 300 installations in 2004, ultimately leading to more than 1,900 installations, covering all U.S. points of entry.
- Nuclear material detectors have also been deployed by states or federal agencies to scan cargo containers at the port of Norfolk, Virginia, and at truck weigh stations in California and New Mexico.
- DHS has begun stationing U.S. customs inspectors in the world's 20 largest cargo ports, as measured by the number of shipments to the United States. Participating governments will provide the U.S. inspectors

with high-level detection equipment, including radiation monitors.[20]
- The Defense Threat Reduction Agency (DTRA) is implementing a multi-year program to develop systems that can detect, give early warning about, and establish a successful response to an attack involving nuclear or radiological weapons on military installations. Testing is taking place at Kirtland Air Force Base, New Mexico; Naval Submarine Base Kings Bay, Georgia; Marine Corps Base Camp Lejeune, North Carolina; and the Army base Fort Leonard Wood, Missouri. Testing activities include using roadway sensors to identify and track nuclear materials in vehicles at both highway speeds (~60 mph) and speeds typical of cars crossing through automated tollbooths. Waterway detection of nuclear materials is also part of this program.[21]
- Bridges, tunnels and subways in New York City and Washington D.C. are being outfitted with radiation detection systems, and the U.S. Departments of Justice and Energy are providing surplus radiological detection instrumentation to state and local emergency first responder agencies nationwide.

All of these efforts are essential. But they are also preliminary steps that need careful coordination, data sharing, and well-designed follow-up actions to yield the greatest insights into the future design of a national or global radiation detection and tracking network. The biggest challenges for detector use are likely to be certifying accurate performance, training, procedures, processing of false and innocent alarms, and response to real instances of nuclear material detection. It is therefore critically important that a team of homeland security officials can assess the cumulative operational and experimental data from all these early testing activities. Currently some of these efforts are going forward in isolation, preventing knowledge gained from one activity to improve the performance of other technologies or procedures, or to discount an approach because superior equipment or methods have already been identified.

Integrating the Detector Networks

Another key factor in the overall effectiveness of any national nuclear materials detection system is its ability to guarantee that data from a wide array of sensor technologies deployed at hundreds or thousands of locations throughout the country and the world can be accessed and analyzed in near real time at central locations. For this reason data will need to be formatted and packaged in ways compatible with rapid transmission and access by remote computers running a variety of software tools. This capability requires early decisions on the architecture of the central data handling system and the connections to it.

The use of proprietary encrypted software for data formatting in some of the commercially available nuclear materials detection equipment could hinder data transfer and system integration. All data-formatting software must be completely open to designers of a national system so that they can ensure efficient integration and security. A guidance document defining standard data architecture should be created for an evolving national nuclear materials detection network. This document should be made available to government agencies that might purchase radiation detection equipment and to industry providers of detectors and other equipment.

One potential route to follow is to define and require standard data packaging and interface requirements for system designs. For example, all nuclear material detection sensors used for homeland security measures could be required to interface with a central data-handling architecture. This approach was taken by the designers of the Biological Aerosols Sensor and Information System (BASIS), which monitors urban environments for the presence of biological agents, and was used during the 2002 Winter Olympic Games at Salt Lake City.

Another issue is data security. The results of radiation measurements, especially those taken at or near military bases, could be sensitive or classified. Data security is necessary to guarantee that only authorized personnel have access to data and that the data in the system can be trusted—that is, protected from tampering or spoofing. Consequently, data will have to be encrypted while traveling through nonsecure network connections. Any information security requirements must be balanced against the need for the data to be rapidly exportable to a broad and geographically dispersed set of agencies and decisionmakers.

Deployment Strategy

No decision has yet been made on deployment of a multilayered national system for radiation detection. Rather, the testing and development activities described above are partially designed as "proof of concept," or pilot efforts, to determine the optimum type and configuration of detectors for several threat scenarios at different locations. An exception to this is the DHS program to install detectors at all U.S. points on entry. However, this program also highlights the need for a system with multiple, overlapping layers because terrorists could simply move a weapon into the United States without crossing through an official point of entry. The nation's key cities, such as New York, Washington DC, Los Angeles, Chicago, San Francisco, and Dallas, are likely to be high priorities for early deployments of radiation detection systems to prevent nuclear terrorism. Linking any cities to both local and national command centers will require a tremendous planning effort.

A project to build high-fidelity computer models of urban environments—including transportation nodes and patterns—could pay off in terms of conceptualizing a nationwide detection system. These models could provide a better picture of the scope of the problem and allow some automated assessment of potential sensor coverage, and perhaps costs. Also, they could be useful in identifying transportation bottlenecks that might lie on approaches to potential urban targets, providing natural opportunities for detector installation. Consistent with this need, the U.S. national laboratories for DHS are creating the National Infrastructure Simulation and Analysis Center (NISAC) to provide modeling and analytic support for a national nuclear detection system architecture as well as other programs.

Another approach that should be investigated is the possibility of leveraging existing transportation and information infrastructure in order to construct a flexible, rapidly deployable nuclear detection system. For example, it might be possible to install radiation detectors in all government, postal, and local law enforcement vehicles cost-effectively. These might serve as random moving elements of a nationwide detection system.[22] Integrated cellular phone communication links in new vehicles are becoming more common, again possibly providing an efficient communication link for sensor output.

More sensors might even be deployed with individuals. Many government employees already use inexpensive, reliable, and accurate dosimeters to determine occupational radiation doses. A community, city, or state might issue dosimeters to a sample of employees on a rotating basis, possibly providing an efficient way to detect nuclear materials in public buildings or at large gatherings. In addition, it might be possible with such a distributed system to create radiation maps of areas of interest and begin to define normal variations in radiation patterns over time. This capability could be critical to detecting and then localizing off-normal readings, which might signal a threat or attack. For example, within a few hours after the 9/11 attacks on the World Trade Center (WTC), radiation levels were measured to determine if the attacks also included radiological dispersal. However, because there were no baseline measurements of the background radiation level at the WTC site, a low level RDD attack would likely have gone undetected.

Aerial platforms might also provide an opportunity for sensor deployment to sample wide areas. While commercial jet aircraft fly too high to do a good job of detecting radiation sources on the surface, many of the world's urban environments are over flown daily by aircraft and helicopters operating at lower elevations. Deploying specialized, low-cost, slow-flying unmanned aerial vehicles for radiation detection might be another option.

While some significant improvements in technology can be anticipated, distributed and wide-area detection system concepts currently suffer from a fundamental weakness. It is very difficult to efficiently identify the type of radioactivity detected and sort out threats from legitimate radioactive materials used for health or industry. Current detectors need their targets to be stationary for efficient isotope identification, and plans for deploying "forests" of networked detectors to provide coverage of wide areas quickly raise the issue of cost.

In addition, radiation detection technology is only one part of a national defense against nuclear terrorism. Challenges equal to or greater than developing effective detection systems include processing the data from the detector networks, determining the least disruptive procedures for scanning large flows of people and cargo, training equipment operators, developing policy, making rules, and coordinating national, state, and local organizations. Ensuring that properly trained and equipped response forces are continuously available across the nation will also require a great deal of resources and planning. A decision to build a national system poses challenges that will require dedication and time to overcome.

CONCLUSIONS

Should the United States attempt to build a homeland defense system against nuclear terrorism? There is a strong consensus within the national security community that nuclear terrorism presents the most serious threat to the U.S. homeland. International efforts are under way to improve the security of nuclear materials so that terrorists cannot acquire them and to prevent nuclear smuggling. However, the limited success of these efforts is well known. It is likely that terrorist organizations already have access to nuclear materials suitable for a "dirty bomb," and it is not inconceivable that they could steal fissile material or an actual nuclear weapon. Their motivation to attack America is not in doubt, and may be increasing.

A nuclear detonation or a severe dispersal of radioactivity in an American city would cause strategic damage to our nation. Current and improved generations of radiation detection technology integrated into a nationwide system offer solid prospects for improving the capabilities that currently exist for locating and stopping a nuclear terrorist attack against the U.S. homeland. The impact that such a system would have on commerce is unknown, but most concepts for radiation detection systems appear capable of keeping this impact at acceptable levels.

With these facts in mind, the current level of national investment for homeland defense against nuclear terrorism is puzzling. For 2004, less than $300 million has been requested for the combined activities of the DHS, DoD, and NNSA that relate to preventing the terminal phase of a terrorist nuclear attack against the U.S. homeland. Even with the $300 million to $400 million for improving the security of foreign nuclear materials added in, the investment does not seem adequate to the threat. Compare this figure to the $7.5 billion that America is expected to spend annually on national defense against ballistic missiles for the period 2002-2005.[23] In addition, unlike the U.S. Missile Defense Agency, which conducts development and deployment of national missile defenses, there is no centralized agency for defense against nuclear terrorism. The chance that the United States will be attacked with a nuclear-armed ballistic missile is considered to be extremely low. The nations that have the most missiles capable of hitting America, like Russia and China, are not currently considered adversaries. Even hostile states with improving missile capabilities like North Korea or Iran would be foolish to launch one because its origin would be known and America would immediately launch a devastating nuclear retaliation. Yet the huge level of spending toward ballistic missile defense is being maintained, even while the technical feasibility of effective missile defense remains in question.

It is clear that continued research and development will be required to learn more about the feasibility of homeland defense against nuclear terrorism based on increased use of radiation detection systems. However, the current level of technology should allow the deployment of pilot operational systems in several U.S. metropolitan areas if the proper levels of funding are provided. At this stage the costs for such a pilot system are unknown, but for a city such as New York, Los Angeles, or Washington, DC, it would certainly be more that $300 million annually. A national command center for homeland defense against nuclear terrorism should also be created.

Unfortunately, America is vulnerable to nuclear terrorism. Its consequences are potentially devastating. Radiation detection technology offers the prospects of improved capabilities for prevention and defense now and in the future. Even if these capabilities are limited during initial deployments, America should rapidly expand its effort to use this technology in defense of the homeland. It should also make the appropriate investments in research and development to improve the future effectiveness of a national defense against nuclear and radiological terrorism.

---

[1] Estimates of the cost of 9/11 range from approximately $50 billion to $200 billion. See Robert Looney, "The Economic Costs of 9/11," Strategic Insight, Center for Contemporary Conflict, August 2002, <http://www.ccc.nps.navy.mil/rsepResources/si/aug02/homeland.asp>; Review of Studies of the "Economic Impact of the September 11, 2001, Terrorist Attacks on the World Trade Center," U.S. General Accounting Office, GAO-02-7000R, May 2002.

[2] PBS Frontline, "Osama Bin Laden v. the U.S.: Edicts and Statements," 2001, <http://www.pbs.org/wgbh/pages/frontline/shows/binladen/who/edicts.html>.

[3] David Albright, Kathryn Buehler, and Holly Higgins, "Bin Laden and the bomb," *Bulletin of the Atomic Scientists* 58, January/February 2002, pp. 23-24.

[4] Amanda Ripley, "The Case of the Dirty Bomber; How a Chicago street gangster allegedly became a soldier for Osama bin Laden," *Time Magazine*, June 16, 2002, <http://www.time.com/time/nation/printout/0,8816,262917,00.html>.

[5] The White House, "The National Strategy for Homeland Security: Office of Homeland Security," July 16, 2002, <http://www.whitehouse.gov/homeland/book/>.

[6] Committee on Science and Technology for Countering Terrorism, National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* (Washington, DC: National Academies Press), p. 56.

[7] U.S. House of Representatives, Committee of Government Reform, *Preventing Nuclear Terrorism: Testimony by Matthew Bunn in the Hearing of the National Security, Veterans Affairs, and International Relations Subcommittee*, 107th Cong., 2nd sess., September 24, 2002, <http://www.iraqwatch.org/government/US/HearingsPreparedstatements/hgrc-bunn-092402.htm>.

[8] Matthew Bunn, John P. Holdren, and Anthony Wier, "Securing Nuclear Weapons and Materials: Seven Steps for Immediate Action," Project on Managing the Atom, Belfer Center for Science and International Affairs, John F. Kennedy School of Government, Harvard University, May 2002, <http://www.nti.org/e_research/securing_nuclear_weapons_and_materials_May2002.pdf>; Matthew Bunn and George Bunn, "Strengthening Nuclear Security Against Post-September 11 Threats of Theft and Sabotage," *Journal of Nuclear Materials Management*, Spring 2002, <http://www.inmm.org/topics/contents/strengthening.pdf>.

[9] For two articles that argue in favor of such a program, see Arian L. Pregenzer, "Securing Nuclear Capabilities in India and Pakistan: Reducing the Terrorist and Proliferation Risks," *Nonproliferation Review* 10 (Spring 2003), and Robert E. Rehbein, "Managing Proliferation in South Asia: A Case for Assistance to Unsafe Nuclear Arsenals," *Nonproliferation Review* 9 (Spring 2002).

[10] David Albright and Mark Gorwitz, "Tracking Civil Plutonium Inventories: End of 1999," Institute for Science and International Security, October 2000, <http://www.isis-online.org/publications/puwatch/puwatch2000.html>.

[11] Thomas E. Ricks and Glenn Kessler , "U.S., N. Korea Drifting Toward War, Perry Warns: Former Defense Secretary Says Standoff Increases Risk of Terrorists Obtaining Nuclear Device," *The Washington Post*, Tuesday, July 15, 2003, p. A14.

[12] Charles D. Ferguson, Tahseen Kazi, and Judith Perera, *Commercial Radioactive Sources: Surveying the Security Risks*, Occasional Paper #11 (Monterey, CA: Center for Nonproliferation Studies, 2003).

[13] International Atomic Energy Agency, Press Release, March 13, 2003, "Stronger Controls Needed to Prevent Terrorist 'Dirty Bombs,'" PR 2003/03, <http://www.iaea.org/worldatom/Press/P_release/2003/prn0303.shtml>.

[14] The White House, "The National Security Strategy of the United States of America," September 17, 2002, <http://www.whitehouse.gov/nsc/nss.html>.

[15] U.S. House of Representatives, Committee on Government Reform, *Container Security: Current Efforts to Detect Nuclear Materials, New Initiatives, and Challenges: Statement of Jay Etta Z. Hecker in the Hearing of the National Security, Veterans Affairs, and International Relations Subcommittee*, 107th Cong., 2nd sess., November 18, 2002.

[16] U.S. Department of Homeland Security, "Department of Homeland Security Budget in Brief," 2003, <http://www.dhs.gov/interweb/assetlibrary/FY_2004_BUDGET_IN_BRIEF.pdf>.

[17] An excellent summary of common technologies for conducting NDA measurements on nuclear materials can be found in Atomic Weapons Establishment, "Confidence, Security and Verification: The challenge of global nuclear weapons arms control," paper prepared for the United Kingdom Ministry of Defence, AWE/TR/2000/001, April 2000, Appendix A. Also see U.S. Department of Energy, Office of Nonproliferation Research and Engineering, *Technology R&D for Arms Control*, Spring 2001, <http://www.llnl.gov/nai/pdf/acnt_war.pdf>.

[18] Will Knight, "New radiation detector is very cool," *New Scientist*, July 5, 2002.

[19] Paul Mann, "Labs Push Hard For Counter-terror Science," *Aviation Now News*, July 17, 2002.

[20] Philip Shenon, "U.S. Expands Plan for Cargo Inspections at Foreign Ports," *New York Times*, June 12, 2003.

[21] U.S. House of Representatives, Committee on Energy and Commerce, *Securing America: The Federal Government's Response to Nuclear Terrorism at Our Nation's Ports and Borders: Testimony of Dr. Stephen M. Younger Subcommittee on Oversight and Investigations*, October 17, 2002, <http://energycommerce.house.gov/107/hearings/10172002Hearing749/Younger1236.htm>.

[22] Steven Johnson, "Stopping Loose Nukes," *Wired* 10, November 2002, <http://www.wired.com/wired/archive/10.11/nukes_pr.html>.

[23] Missile Defense Agency, Press Release, "Fiscal Year (FY) 2004/FY 2005 Biennial Budget Estimates Submission," <http://www.acq.osd.mil/bmdo/bmdolink/pdf/budget04.pdf>.