ONE

Biological and Nuclear Risks

The greatest danger of another catastrophic attack in the United States will materialize if the world's most dangerous terrorists acquire the world's most dangerous weapons.

—*The 9/11 Commission Report*

Biological Risks

They were agents on a mission and they came not at night, which might have looked suspicious, but in broad daylight. Hiding in plain sight on a city street in Atlanta, they walked the perimeter of one of America's five biological laboratories where scientists worked on the world's most deadly pathogens. They had come to this lab at Georgia State University in 2008 as part of their assignment to quietly case facilities designated as Biosafety Level 4 (BSL-4) labs, the highest level of biological containment, required for work with the most dangerous viruses. They were looking for even the slightest security vulnerability—anything that might give an edge to terrorists seeking to steal small quantities of Ebola virus or other lethal disease agents for which there are no treatments, no known cures.

These individuals discovered that in a number of places, the lab was unprotected by barriers and that outsiders could walk right up to the building housing these deadly pathogens. Around back, they watched and took notes as a pedestrian simply strolled into the building through an unguarded loading dock.

On another day, the same people went to San Antonio to check out another BSL-4 lab, the Southwest Foundation for Biomedical Research. They discovered that the security camera covered only a portion of the perimeter, and that the only barrier to vehicles was an arm gate that would swing across the roadway. The guards assigned to protect this facility were unarmed. Once again, these individuals walked the perimeter. This time they spotted a window through which, standing outside, they could watch the scientists as they worked with top-security pathogens. Now they knew exactly where the world's most deadly pathogens were kept.

This was precisely the lethal trove that al Qaeda's terrorists had been seeking for years. But luckily, these operatives on this mission were not from al Qaeda—they were from the Government Accountability Office (GAO), the investigative arm of the U.S. Congress, and

they visited five of America's labs that are designated BSL-4. For more than a decade, U.S. government inspection teams have traveled to facilities in the former Soviet Union and reported back on the poor security and lax practices used in storing biological pathogens. Now, this latest study by GAO has shown that when it comes to materials of bioterrorism, America's vulnerability may well begin at home.

The GAO report gave high marks to three of the five facilities investigated. The investigators measured how the labs fared in 15 security control categories, and these labs met the standards for, respectively, 13, 14, and all 15. Among the 15 security controls were having armed security guards visible at all public entrances to the lab, full camera coverage of all exterior entrances, and closed-circuit television and a command and control center so that any security breach could be instantly known throughout the facility.

But the two lowest-scoring BSL-4 labs passed in only 3 and 4 of the 15 categories—a score that is even more troubling because, as GAO noted, both still met the requirements of the Division of Select Agents and Toxins of the Centers for Disease Control and Prevention (CDC).

Despite these shortcomings, the United States is actually at the forefront of laboratory security in the world today and has by far the most stringent regulations to restrict access to dangerous pathogens. Most developing countries, in contrast, have largely ignored the problem of biosecurity because of competing demands for their limited budgets. Security gaps at laboratories that store and work with dangerous pathogens, both in the United States and around the world, are worrisome because of continued interest in biological weapons. Director of National Intelligence Michael McConnell said in a recent speech, "One of our greatest concerns continues to be that a terrorist group or some other dangerous group might acquire and employ biological agents . . . to create casualties greater than September 11."

Al Qaeda has long sought to obtain biological and chemical weapons. One of its leading experts in the quest for such weapons was Midhat Mursi al-Sayid Umar, an Egyptian also known as Abu Khabab al-Masri. According to media accounts, he was killed in July 2008 by an airstrike over Pakistan's northern tribal area.

On July 17, 2008, the Afghanistan National Police arrested Aafia

Siddiqui, a Pakistani woman believed to have ties to al Qaeda, who reportedly had been acting suspiciously outside the governor's compound in Ghazni province. Educated at the Massachusetts Institute of Technology and at Brandeis University, where she earned a Ph.D. in neuroscience, she had been wanted by the FBI since 2004—the first woman sought by the law enforcement agency in connection with al Qaeda. According to media accounts, when arrested she had in her possession a list of New York City landmarks, documents describing how to produce explosives, and details about chemical, biological, and radiological weapons. She was extradited to New York for trial on charges of attempted murder and assault of U.S. officers in Afghanistan.

The world is fortunate that al Qaeda to date is not known to have successfully stolen, bought, or developed agents of bioterror. But scenarios of just how such an incident might occur have been developed for planning purposes. The Homeland Security Council has created a chilling scenario of how terrorists could launch an anthrax attack in the United States—and the horrific chain of events that would follow:

> This scenario describes a single aerosol [anthrax] attack in one city delivered by a truck using a concealed improvised spraying device in a densely populated urban city with a significant commuter workforce. It does not, however, exclude the possibility of multiple attacks in disparate cities or time-phased attacks (i.e., "reload"). For federal planning purposes, it will be assumed that the Universal Adversary (UA) will attack five separate metropolitan areas in a sequential manner. Three cities will be attacked initially, followed by two additional cities 2 weeks later.
>
> It is possible that a Bio-Watch [atmospheric sensor] signal would be received and processed, but this is not likely to occur until the day after the release. The first cases of anthrax would begin to present to Emergency Rooms (ERs) approximately 36 hours post-release, with rapid progression of symptoms and fatalities in untreated (or inappropriately treated) patients.
>
> The situation in the hospitals will be complicated by the following facts: The release has occurred at the beginning of an unusually early influenza season and the prodromal [early]

symptoms of inhalation anthrax are relatively non-specific. Physician uncertainty will result in low thresholds for admission and administration of available countermeasures (e.g., antibiotics), producing severe strains on commercially available supplies of medications such as ciprofloxacin and doxycycline, and exacerbating the surge capacity problem.

Social order questions will arise. The public will want to know very quickly if it is safe to remain in the affected city and surrounding regions. Many persons will flee regardless of the public health guidance that is provided. Pressure may be placed directly on pharmacies to dispense medical countermeasures directly, and it will be necessary to provide public health guidance in more than a dozen languages.

The attack results in 328,848 exposures; 13,208 untreated fatalities; and 13,342 total casualties. Although property damage will be minimal, city services will be hampered by safety concerns.

° ° °

In September 2001, an American public already reeling from the worst terrorist attack in U.S. history was stunned by news that envelopes containing anthrax had been delivered via the U.S. mail to targets in the news media. A week after September 11, letters containing 1–2 grams of dried anthrax bacterial spores were sent to three major television broadcast networks, the *New York Post,* and American Media International (AMI) in Florida, a publisher of supermarket tabloids. On October 5, the tainted letters claimed their first victim: Robert Stevens, a photo editor at AMI, died of inhalational anthrax. On October 9, two more letters bearing the same New Jersey postmark and containing a more refined preparation of dried anthrax spores were mailed to the Washington, D.C., offices of Senators Tom Daschle and Patrick Leahy.

During their journey, the anthrax letters passed through automated mail-sorting machines that forced the microscopic anthrax spores out through tiny pores in the envelopes, thereby infecting a number of postal workers. The tainted sorting machines also cross-contaminated other letters, which were delivered and sickened some of their recipients. By November 2001, 22 people in New York, New Jersey, Con-

necticut, Florida, and the District of Columbia had contracted anthrax, half of them through the skin (causing cutaneous anthrax) and the other half through the lungs (causing inhalational anthrax). Five of the 11 victims who contracted inhalational anthrax died.

Former NBC news anchor Tom Brokaw, who was one of the targets of the anthrax letters, testified about his experience at the Commission's public hearing in New York City. About a week after September 11, 2001, Brokaw said, two of his assistants handled a letter addressed to him that contained a granular powder. Several days after coming in contact with the powder, both women developed fever, malaise, and ugly black skin lesions. Their mysterious illness touched off several days of confusion and missteps. Three times Brokaw was told by various health officials, including experts at the U.S. Army's biodefense research center at Fort Detrick, in Maryland, that his assistants' skin lesions had been caused by the bite of a brown recluse spider. Finally, nearly three weeks after the initial exposures, officials from the U.S. Centers for Disease Control and Prevention (CDC) made the correct diagnosis of cutaneous anthrax. Prior to this diagnosis, Brokaw recalled, there was "kind of an unsettled feeling in the [NBC] building, but we're confining it because we don't want to cause undue panic. You know, we're operating based on what we've been told by very authoritative sources. Well, when we're told that it is in fact an anthrax attack, that [my assistants] have cutaneous anthrax, all hell broke loose at 30 Rock. There were no [response] systems in place."

In August 2008, the Department of Justice declared that it had identified the perpetrator of the 2001 anthrax attacks as Bruce E. Ivins, a government biodefense scientist who had worked for decades at the U.S. Army's biodefense research laboratory at Fort Detrick. Ivins had committed suicide shortly before he was to be indicted for the crime.

The anthrax mailings revealed serious gaps in U.S. preparedness for bioterrorism that have been only partly addressed over the past seven years. Since 2001, however, no further bioterrorist attacks have occurred. What is the risk of another incident? How worried should the public be? And in the future, how will the bioscience revolution and the globalization of the biotechnology industry change the nature of the biological weapons threat?

What Are Biological Weapons?

Biological weapons are disease-causing microbes (chiefly bacteria and viruses) and toxins (poisonous substances produced by living creatures) that have been harnessed for the purpose of incapacitating or killing humans, livestock, or crops. Examples include the bacteria that cause anthrax and plague, the viruses that cause smallpox and Ebola hemorrhagic fever, and poisons of natural origin such as ricin and botulinum toxin.

Each of these agents has distinct characteristics that affect its suitability for use as a weapon. These are *infectivity* (the ability to infect a human host and cause disease), *virulence* (the severity of the resulting illness), *transmissibility* (the ability of the disease to spread from person to person), and *persistence* (the duration of a microbe's survival after its release into the environment).

The process of turning a natural pathogen into a WMD begins with acquiring a sample of a disease-causing microbe from a natural source (such as a person or sick animal) or stealing it from a laboratory or culture collection. But just as a bullet is a harmless lump of lead without a cartridge and a rifle to deliver it, so most pathogens and toxins are not effective weapons in their natural state and must be processed ("weaponized") and combined with a delivery system to make them capable of producing large numbers of casualties.

The anthrax bacterium is considered an ideal biological warfare agent because it is relatively easy to grow, highly lethal when inhaled, and able to transform itself into a hearty spore that can persist in soil or contaminate a target area for years. If an individual is treated with antibiotics shortly after inhaling anthrax spores, the infection can usually be cured. If treatment is delayed, however, the bacterial toxins will be released, and extraordinary medical intervention is then needed for the victim to have any chance of survival.

Despite the small quantity of dried anthrax spores used in the 2001 letter attacks—a total of about 15 grams—the ripple effects of the mailings extended far beyond those sickened or killed. Professor Leonard Cole of Rutgers University has estimated the total economic impact of the anthrax letter attacks at more than $6 billion. If only 15 grams of dry anthrax spores delivered by mail could produce such an

enormous effect, the consequences of a large-scale aerosol release would be almost unimaginable.

As deadly as anthrax can be, it fortunately is not contagious. Because persons infected with the disease cannot transmit it to others, only those who are directly exposed to anthrax spores are at risk. Contagious diseases such as plague or smallpox, in contrast, can be transmitted through person-to-person contact, turning the initial set of victims into secondary sources of infection.

Many factors would affect the outcome of a biological attack, including the type and strain of agent; the time of day that it is released, and the prevailing wind, weather, and atmospheric conditions; and the basic health of the people who are exposed to it. Also important are the speed and manner in which public health authorities and medical professionals detect and respond to the resulting outbreak. A prompt response with effective medical countermeasures, such as antibiotics and vaccination, can potentially blunt the impact of an attack and thwart the terrorists' objectives.

The State Threat

During the Cold War, both the United States and the Soviet Union produced and stockpiled biological agents. But in November 1969, the Nixon administration renounced the U.S. offensive biological weapons program and then began to destroy its stockpile. This unilateral action opened the way to the successful negotiation of the 1972 Biological Weapons Convention (BWC), a multilateral treaty banning the development, production, and stockpiling of biological and toxin weapons.

Although the BWC was supposed to end all efforts by states to develop the capability to employ disease as a weapon, it has unfortunately failed to achieve this goal. Because the materials and equipment needed to produce biowarfare agents also have legitimate uses in scientific research and commercial industry, it is difficult to verify the BWC with any degree of confidence. A number of countries have secretly violated the treaty. The most egregious case was that of the Soviet Union, which created a massive biological weapons development and production complex employing more than 50,000 scientists and technicians.

Today, several important countries—Egypt, Israel, and Syria among them—remain outside the Biological Weapons Convention. The U.S.

State Department has also expressed concern that some parties to the treaty, such as Russia, China, North Korea, and Iran, may be pursuing offensive biological weapons programs in secret.

The Non-State Threat

States do not have a monopoly on biological weapons. In the past, a number of terrorist organizations and rogue individuals have sought to acquire and use biological or toxin agents. Such weapons may be attractive to terrorists because of their potential to inflict mass casualties or to be used covertly. In addition, as the anthrax letter attacks of autumn 2001 clearly demonstrated, even small-scale attacks of limited lethality can elicit a disproportionate amount of terror and social disruption.

The 2001 anthrax mailings were not the first incident of bioterrorism in the United States. In 1984, the Rajneeshees, a religious cult in Oregon, sought to reduce voter turnout and win control of the county government in an upcoming election by temporarily incapacitating local residents with a bacterial infection. In a test run of this scheme in September 1984, cult members contaminated 10 restaurant salad bars in a town in Oregon with salmonella, a common bacterium that causes food poisoning. The attack sickened 751 people, some seriously.

A decade later, members of a Japanese doomsday cult called Aum Shinrikyo released anthrax bacterial spores from the roof of a building in Tokyo. Fortunately, this attack failed because the cult produced and dispersed a harmless strain of anthrax that is used as a veterinary vaccine. Had Aum succeeded in acquiring a virulent strain and delivered it effectively, the casualties could have been in the thousands.

Islamist terrorist groups such as al Qaeda have also sought to acquire biological weapons in the past. Former CIA Director George Tenet wrote in his memoir that in 1999, in parallel with planning for the September 11 terrorist attacks, al Qaeda launched a concerted effort to develop an anthrax weapon that could inflict mass casualties. The group hired a Pakistani veterinarian named Rauf Ahmad to set up a bioweapons laboratory in Afghanistan, but he became disgruntled with the amount of money he was paid and eventually quit. To continue the anthrax work, al Qaeda then hired a Malaysian terrorist, Yazid Sufaat, who had studied biology at California State University in Sacramento. But in December 2001, after the U.S. invasion of Afghanistan,

Sufaat fled; he was captured by authorities as he tried to sneak back into Malaysia.

The cases of the Rajneeshees, Aum Shinrikyo, and al Qaeda underscore not only the dangerous potential of bioterrorism but also the technical difficulties that terrorist groups seeking such weapons are likely to encounter. Aum's failure to carry out a mass-casualty attack, despite its access to scientific expertise and ample financial resources, suggests that one should not oversimplify or exaggerate the threat of bioterrorism. Developing a biological weapon that can inflict mass casualties is an intricate undertaking, both technically and operationally complex.

Because of the difficulty of weaponizing and disseminating significant quantities of a biological agent in aerosol form, government officials and outside experts believe that no terrorist group currently has an operational capability to carry out a mass-casualty attack. But they could develop that capability quickly. In 2006 congressional testimony, Charles E. Allen, Under Secretary for Intelligence and Analysis at the Department of Homeland Security, noted that the threat of bioterrorism could increase rapidly if a terrorist group were able to recruit technical experts who had experience in a national biological warfare program, with knowledge comparable to that of the perpetrator of the 2001 anthrax letter attacks. In other words, given the high level of know-how needed to use disease as a weapon to cause mass casualties, the United States should be less concerned that terrorists will become biologists and far more concerned that biologists will become terrorists.

The last point bears repeating. We accept the validity of intelligence estimates about the current rudimentary nature of terrorist capabilities in the area of biological weapons but caution that the terrorists are trying to upgrade their capabilities and could do so by recruiting skilled scientists. In this respect the biological threat is greater than the nuclear; the acquisition of deadly pathogens, and their weaponization and dissemination in aerosol form, would entail fewer technical hurdles than the theft or production of weapons-grade uranium or plutonium and its assembly into an improvised nuclear device.

The difficulty of quantifying the bioterrorism threat to the United States does not make that threat any less real or compelling. It involves both motivation and capability, and the first ingredient is clearly present. Al Qaeda had an active biological weapons program in the past, and it is unlikely that the group has lost interest in employing infectious

disease as a weapon. That roughly a half-dozen countries are suspected to possess or to be seeking biological weapons also provides ample grounds for concern.

The Future Threat

In addition to the current threat of bioweapons proliferation and terrorism, a set of over-the-horizon risks is emerging, associated with recent advances in the life sciences and biotechnology and the worldwide diffusion of these capabilities. Over the past few decades, scientists have gained a deep understanding of the structure of genetic material (DNA) and its role in directing the operation of living cells. This knowledge has led to remarkable gains in the treatment of disease and holds the promise of future medical breakthroughs. The industrial applications of this knowledge are also breathtaking: it is now possible to engineer microorganisms to give them new and beneficial characteristics.

Activity has been particularly intense in the area of biotechnology known as *synthetic genomics.* Since the early 1980s, scientists have developed automated machines that can synthesize long strands of DNA coding for genes and even entire microbial genomes. By piecing together large fragments of genetic material synthesized in the laboratory, scientists have been able to assemble infectious viruses, including the polio virus and the formerly extinct 1918 strain of the influenza virus, which was responsible for the global pandemic that killed between 20 million and 40 million people.

As DNA synthesis technology continues to advance at a rapid pace, it will soon become feasible to synthesize nearly any virus whose DNA sequence has been decoded—such as the smallpox virus, which was eradicated from nature in 1977—as well as artificial microbes that do not exist in nature. This growing ability to engineer life at the molecular level carries with it the risk of facilitating the development of new and more deadly biological weapons.

The only way to rule out the harmful use of advances in biotechnology would be to stifle their beneficial applications as well—and that is not a realistic option. Instead, the dual-use dilemma associated with the revolution in biology must be managed on an ongoing basis. As long as rapid innovations in biological science and the malevolent intentions of terrorists and proliferators continue on trajectories that

are likely to intersect sooner or later, the risk that biological weapons pose to humanity must not be minimized or ignored.

Nuclear Risks

Pelindaba sprawls across the rolling hills west of Pretoria, a series of low, flat buildings among clusters of trees far greener than the brownish grasslands of the region. Its name is familiar to the citizens of South Africa, though few of them have ever seen it. It is known to be a repository of hundreds of kilograms of weapons-grade highly enriched uranium (HEU) that are the leftovers of the nuclear weapons program that produced six bombs before South Africa famously became the world's first and only nuclear nation to go the route of complete nuclear disarmament. It is also known as one of South Africa's most tightly secured installations, surrounded by 10,000-volt security fences, protected by a well-armed security force, and monitored by around-the-clock closed-circuit television cameras.

The attack came without warning, in the early morning hours of November 8, 2007.

Two armed teams struck the facility. The first consisted of four men: they burst into the facility's eastern block and headed for the control room. Later, authorities would say the four had gotten into the compound by cutting a hole in the high-voltage fence.

Inside the control room was the nuclear installation's emergency services operational officer and the control room's night shift supervisor. As the attackers burst in, the emergency services officer, Anton Gerber, pushed the control room supervisor under the desk—because she happened to be his fiancée and, he would later explain, he just wanted to protect her. The attackers shot him in the chest; the bullet, which narrowly missed his heart, broke a rib and punctured his lung—missing his spine by 2 centimeters, a doctor later said. Gerber said that after being shot, he continued trying to fight off the intruders as they attacked him with a screwdriver.

Then, as quickly as they had arrived, the intruders left—without making any effort to steal the nuclear material or sabotage the control room, the reactors, or anything else. They had grabbed one computer as they fled but dropped it when Pelindaba's security forces finally got to the scene, an estimated 45 minutes after the attackers had entered

the compound. They got away cleanly. Later that night, a second team attacked. But guards spotted them early this time and sounded the alarm, and these attackers also fled.

South African authorities found the whole episode baffling—was this an inside caper with some sort of personal motive or was it really about nuclear terrorism? Why was it that the attackers spent 45 minutes inside the compound without being detected by either the high-tech equipment or the security guards?

International nuclear nonproliferation officials and nongovernmental experts found it frightening—focusing on what might have been. Could the attackers have stolen enough highly enriched uranium to fashion a nuclear bomb? Could South Africa's weapons-grade nuclear material have wound up in the possession of terrorists?

After reviewing the incident with South African authorities, the International Atomic Energy Agency (IAEA) determined that the HEU was never in any real danger, because the intruders never made it to the areas where the nuclear material was stored. Still, as Matthew Bunn, an associate professor of public policy at Harvard University, stated in his April 2008 testimony to the Senate Homeland Security and Governmental Affairs Committee, "This incident is nevertheless a potent reminder that inadequately secured nuclear material is a global problem, not one limited to the former Soviet Union."

So far as we know, the world has been the beneficiary of both skill and luck that terrorists have not yet obtained nuclear weapons-grade material and made it into a bomb. For nuclear thefts have occurred, as well as some well-known attempts by terrorists to buy bomb-making material on the black market.

° ° °

The world today confronts a growing nuclear risk. Even as some states seek to acquire nuclear weapons, others are looking to expand their arsenals. Concern about the spread of nuclear weapons intensifies with the possibility of a large increase in nuclear power production to meet growing energy demands—a nuclear renaissance. As additional countries acquire nuclear facilities—particularly if they build uranium enrichment facilities or reprocessing facilities, ostensibly to provide fuel for their power plants and reduce the waste associated with the spent nuclear fuel—the number of states possessing the knowledge and capa-

bility to "breakout" and produce nuclear weapons will increase significantly. This also increases the risk that such materials could be diverted to, or stolen by, terrorist groups.

In addition, there is already a surfeit of nuclear material in the world. More than 40 countries possess nuclear material that could be used in a nuclear weapon, though at present almost all of it (about 95 percent) is in Russia and the United States. Hence those two countries have a special role to play in accounting for, securing, and reducing nuclear materials.

Most black market sources of actual weapons-grade nuclear material that terrorists seek appear to have originated from Russia or other former Soviet states. Much of it was most likely diverted or stolen by an individual with access to a facility designed to hold such materials. There have been multiple seizures by authorities in Russia and elsewhere of kilogram quantities of HEU. Even more disconcerting are reports that in 1998 the Russian Federal Security Service uncovered a plot by employees in a nuclear facility to steal 18.5 kilograms of material described only as suitable for the "production of components for nuclear weapons." Taken together these attempts represent enough material to produce at least one nuclear weapon.

More recently, there was a sting operation pulled off by the law enforcement officials of the Republic of Georgia. In February 2006, Georgian officials arrested Oleg Khintsagov, a Russian merchant from the North Ossetia region, on charges that he was trying to sell 100 grams of highly enriched uranium; they also took four Georgians into custody. After saying little publically about the case for a year, officials put out the word that the key to the arrest was a Georgian who spoke Turkish and pretended to be a Muslim from an organization interested in buying bomb-making fuel. Khintsagov claimed that he got the uranium from a source in the Siberian academic city of Novosibirsk. Russians said that their tests on the sample were inconclusive and expressed concerns that the arrest was politically motivated; Georgian officials said that the uranium appeared to be Russian. Khintsagov was sentenced to eight years in jail.

In another case, a small-time nuclear thief from Russia became a big-time nightmare for officials of the International Atomic Energy Agency.

Leonid Smirnov was a foreman at the Luch Scientific Production

facility in Podolsk, just two hours by train from Moscow. His job was to weigh and inventory nuclear material, then dispense it to other workers. Because the scales at Luch were not very accurate, all measurements recorded for inventory were assumed to have a 3 percent margin of error. So, in the first years of the post-Soviet Russia, Smirnov figured that he would steal just a little bit at a time—always within the margin of error. And that's what he did. Night after night, he carried home a small amount of enriched uranium and put it in a lead-lined container that he kept on the balcony of his apartment, which overlooked a children's playground. In four months, he had collected 1,598 grams of 90-percent enriched uranium. Meanwhile, no discrepancies were visible in the ledgers at Luch.

Not being a practiced thief, Smirnov did not know how to sell it on the black market. When he sought advice from some friends who were thieves, they told him they were going to take the train to Moscow to sell some batteries; he could come along and bring his loot with him. But as it happened, the Podolsk police had been watching his pals and they were arrested. In the police station, after his friends were booked and led away, the police asked what he had in his lead container. Uranium, said Smirnov. The police ran out of the building into the street—and Smirnov ran after them, politely reassuring his captors and insisting that they were perfectly safe. He was arrested, and his helpfulness earned him a light sentence.

What led officials at IAEA to call Smirnov a nightmare was that he could have stolen enough material to make a bomb and sold it to terrorists—with the books at Luch still showing all the uranium accounted for and without IAEA officials ever having a clue that there was a problem.

This story underscores how U.S.-Russian cooperation can help secure so-called loose nukes—and that sometimes even small acts can lead to major improvements in security. Under the U.S. Cooperative Threat Reduction Program, also known as the Nunn-Lugar program (after its two respected congressional sponsors, Senators Sam Nunn and Richard Lugar), the United States paid for new digital state-of-the-art scales for the Luch facility. The result: no more rounding off within margins of error, and thus no more opportunities for small-time nuclear thieves like Leonid Smirnov to steal a bomb's worth of uranium, bit by bit.

° ° °

Unlike the uncertainties of a biological attack, which could occur silently and without being noticed for a number of days, a nuclear attack would be obvious, and most people understand the level of devastation and death it could cause. Still, it is instructive to review the damage that would follow a nuclear incident. Perhaps the best description has been provided by a member of our Commission, Graham Allison, director of the Belfer Center for Science and International Affairs at Harvard University, in his book *Nuclear Terrorism: The Ultimate Preventable Catastrophe* (2004).

Allison's scenarios:

> New York City—Al Qaeda rents a van, drives a Russian 10-kiloton nuclear bomb into Times Square, and detonates it. Times Square disappears instantly, as the heat from the blast would reach tens of millions of degrees Fahrenheit. The theater district, Grand Central Terminal, Rockefeller Center, Carnegie Hall, and Empire State Building would be gone, literally in a flash. Buildings further away, such as the United Nations Headquarters on the East River, the Flatiron Building, and the Metropolitan Museum would look like bombed-out shells. Half a million people who at noontime are in that half-mile radius of the blast site would be killed. Hundreds of thousands of others would die from collapsing buildings, fire, and fallout.
>
> San Francisco—A nuclear bomb is detonated in Union Square. Everything to the Museum of Modern Art would be vaporized. Massive destruction would exist from the Transamerica Building to Nob Hill.
>
> Chicago—A nuclear bomb explodes at Sears Tower. Everything from Navy Pier to the Eisenhower Expressway disappears. The United Center and Grant Park are destroyed. A firestorm sweeps from the White Sox's U.S. Cellular Field on the South Side to the Cubs' Wrigley Field on the North Side.
>
> Washington—A nuclear bomb at the Smithsonian Institution would destroy everything from the White House to the Capitol lawn. The Supreme Court would be rubble. The Pentagon, across the Potomac River, would be engulfed in flames.

° ° °

For all these reasons, our Commission joins the calls made by many others before us emphasizing the urgency of securing nuclear materials useful for weapons—right now, *before* they fall into the hands of terrorists.

At the same time, we cannot lose sight of concerns regarding the spread of nuclear weapons. Since the United States exploded the first nuclear bomb in 1945, seven additional states are known or suspected to have joined the nuclear weapons club: Russia, China, the United Kingdom, France, Israel, India, and Pakistan. In addition, South Africa built six nuclear weapons in the 1980s and dismantled them just before power was transferred to the post-apartheid government. North Korea conducted a nuclear weapons test in 2006, thus becoming the first country to have ratified the NPT and then break out of it by producing a nuclear weapon. In the past several years, the United States and Russia have significantly reduced their arsenals of nuclear weapons, while Pakistan, India, and China have been increasing their nuclear capabilities and reliance upon nuclear weapons in their strategic postures.

The emergence of this new kind of arms race in Asia raises the prospect of a nuclear war whose effects would be catastrophic both regionally and globally. Analysts estimate that a nuclear exchange between India and Pakistan that targets cities would kill millions of people and injure millions more. The risk of a nuclear war between the two neighbors is serious, given their ongoing dispute over Kashmir and the possibility that terrorist attacks by Pakistani militant groups might ignite a military confrontation.

Pakistan's nuclear weapons program is driven by its perception of the conventional and nuclear threat from India, while India's program is focused on both Pakistan and China. China is also fueling the arms race, both by increasing its own strategic forces and by not stopping Chinese entities from supporting Pakistan's strategic programs. At present, all three are expanding their nuclear arsenals with no clear end in sight.

At the same time, nuclear developments in Iran, North Korea, and Syria are also disturbing, because they represent a possible tipping point toward cascading nuclear proliferation. The continued production and testing of nuclear weapons by North Korea could provoke Japan or South Korea to reconsider its nuclear postures. Similarly, Iran's

continued pursuit of a fissile material production capability, combined with the recent revelation that Syria was constructing a plutonium production reactor with North Korean assistance, increases the pressure on Saudi Arabia, Egypt, and other states in the region to pursue their own programs. In this context, increased U.S., French, Russian, and Chinese contributions to civilian nuclear programs in the Middle East and South Asia are potentially destabilizing, if not managed properly.

The path leading to proliferation apparently was not difficult to follow. Some states pursued the development of nuclear technologies and capabilities within their own borders, and some relied on direct state-to-state transfers. Others employed espionage to acquire the technology and knowledge they needed, and still others relied on independent, illicit procurement agents to acquire nuclear technology that was mainly dual-use from other weapons and civil nuclear programs. Some benefited from the marketing of nuclear technology and expertise by scientists from other state programs. Most used a combination of these methods as they tried to achieve their goal.

Several states have tapped into black markets and illicit networks that supply nuclear materials, designs, and expertise to almost any buyer who is interested. The best known of these networks, run by the Pakistani scientist A. Q. Khan, assisted Iran, Libya, North Korea, and perhaps others in acquiring the technologies and designs needed to develop illicit nuclear programs. It unraveled in 2003 after authorities intercepted the BBC *China,* a cargo ship on its way to Libya with gas centrifuge components on board. It is unlikely that Khan's network could be reconstituted, but black-marketing of dangerous technologies, designs, and expertise continues to this day and is a major concern.

The recent discovery that North Korea provided Syria with a nuclear reactor for plutonium production escalates existing concerns about future nuclear proliferation. North Korea, after all, has already sold nuclear weapons–capable ballistic missiles to Pakistan, Iran, and several other states in the Middle East.

Nonetheless, past decisions by other countries may offer some hope for U.S. and international nonproliferation efforts. Belarus, Kazakhstan, and Ukraine agreed to the removal of nuclear weapons from their territory after the fall of the Soviet Union, and South Africa agreed to give up its nuclear weapons in 1991. Taiwan, South Korea, Argentina, Brazil, and Libya formerly had nuclear weapons programs

but have reversed course. An additional 20 countries that at one time considered building nuclear weapons ultimately subscribed to norms of nonproliferation. But even when countries give up their nuclear weapons programs, there is still a risk that their nuclear know-how and materials will fall into the hands of terrorists or others.

At the moment, al Qaeda is judged to be the sole terrorist group actively intent on conducting a nuclear attack against the United States. For the foreseeable future, no extremists or groups to which they belong will be able on their own to produce nuclear weapons–usable materials. As a result, terrorists can successfully employ a nuclear device only if they acquire a weapon or weapons-usable materials from a state nuclear program. It is therefore imperative that authorities secure nuclear weapons and materials at their source.

Al Qaeda began its efforts to acquire nuclear weapons–usable material in the early 1990s. While bin Laden was living in Sudan, his aides received word that a Sudanese military officer was offering to sell weapons-grade uranium. Bin Laden was willing to pay full price for the material: $1.5 million. After the purchase, however, the al Qaeda members realized that they had been scammed. This failure apparently did not discourage bin Laden—and his persistence highlights the seriousness of his interest. In the spring of 2001, bin Laden met with a Pakistani former nuclear scientist, Bashiruddin Mahmood, and discussed the development of nuclear and other weapons of mass destruction.

Today, all of this still points to intent but not capability. U.S. government officials and recognized experts have testified that al Qaeda probably does not currently have the nuclear materials or the technical expertise necessary to produce a nuclear weapon. However, they also recognize that the terrorists' ability to produce such a device could increase dramatically should they recruit just one or two individuals with access to nuclear materials or with knowledge of nuclear weapons designs.