Traditional terrorist tactics, including assassinations, hijackings, kidnappings, and bombings, are still the first choice of most terrorists. The September 11, 2001, attacks on the World Trade Center and the Pentagon demonstrated that these standard tactics can be used to inflict horrifying devastation. However, the availability of advanced technology and its ability to increase the harm caused by terrorists escalate the threat posed by contemporary terrorism. This chapter discusses two types of terrorist tactics that rely on advanced technology: CBRNE attacks and the use of the Internet to spread propaganda and destroy vital infrastructures.

CBRNE is the term used to describe chemical, biological, radiological, nuclear, and explosive weapons. Some of these weapons have always been available: for example, when the ancient Romans contaminated their enemies’ drinking water with dead horses, it was a form of biological assault. Chemical warfare, especially in the form of mustard gas, was well known to soldiers fighting in the foxholes and tunnels during World War I. However, although the threat is not new, advances in technology have made it more likely that the world will one day experience a CBRNE attack of greater magnitude than ever before.

The use of the Internet to spread propaganda, raise funds, incite violence, and plan attacks has been studied extensively (see, e.g., Colarik, 2006; Laqueur, 1997; Verton, 2003). A decentralized network of communications, which is the hallmark of the contemporary Internet, was initially created in the 1970s by the U.S. Department of Defense out of fear of a nuclear attack launched by the Soviet Union (Weimann, 2006b). Now, ironically, modern terrorists, who are perhaps the single greatest threat to the security of the United States, are making increasing use of the Internet to further their cause. The threat posed by digital terrorism, which includes both information warfare and cyberterrorism, has dramatically increased in recent years. Using the Internet to successfully attack critical infrastructure, such as water, power, and communication systems, increases the lethality of the weapons available to today’s terrorists.

As noted by David Rapoport in the first reading to accompany Chapter 2, technology does not cause terrorism: the Zealots-Sicarii, the Assassins, and the Thugs used whatever primitive technology available to them. It can be no surprise then that modern terrorists continue to employ extant technologies to achieve their goals.

Today’s terrorist can choose from a potent array of weapons capable of destroying large portions of our planet, causing hundreds of thousands and even millions of deaths and injuries. The
use of these weapons by terrorists could incite global panic and paralyze governments’ attempts to respond to the ensuing crisis. Worst-case scenarios paint horrific images of the potential destruction of the environment and all the flora and fauna on earth.

For more than a century, terrorists have fantasized about weapons that could obliterate large portions of the earth. Karl Heinzen, the mid-19th-century German radical philosopher who thought prizes should be given for inventing new poisons and explosives (Laqueur, 1977), fantasized about weapons like “rockets, poison gases, and land mines, that one day would destroy whole cities with 100,000 inhabitants” (Laqueur, 1999, p. 13). Imagining doomsday has long been a favorite preoccupation of science fiction writers. The mad scientists, bent on destroying the world, were well known in the late 19th and early 20th centuries to readers of H.G. Wells and other authors of the science fiction genre.

The difference between now and then is that today the raw materials for producing and dispersing CBRNE, manipulating the Internet, and engaging in digital terrorism are more readily available. The decline in the 1990s of left-wing terrorist groups, which flourished in the 1970s and 1980s, was accompanied by a rise in right-wing groups. Where left-wing terrorists focused primarily on economic and political causes, many of today’s right-wing terrorists, like those accused of the 9/11 attacks, are driven by religious zealotry (Laqueur, 1999). Thus, technological advances come at a time when right-wing fanatical terrorism is growing.

The destructive consequences of just one terrorist staging a CBRNE or Internet attack are extraordinarily high. Although some terrorists are deterred by the horrific consequences of such attacks, others want to maximize fatalities by using technologically sophisticated weaponry. Rogue governments may be afraid to use such weapons against more powerful enemies for fear of retaliation, but they may nevertheless be willing, either for profit or to further their political agendas, to supply terrorists with the raw materials to produce the weapons.

**CBRNE**

A variety of terms have been used to describe massively destructive weapons, and the terminology changes as new incidents occur. The terminology has evolved from WMD (weapons of mass destruction) to NBC (nuclear, biological, and chemical weapons) to CBW (chemical and biological weapons), to CBRN (chemical, biological, radiological, and nuclear weapons), and now to CBRNE (chemical, biological, radiological, nuclear, and explosive weapons; Ballard & Mullendore, 2003). One can only wonder what new term will be developed next to describe the horrifying future array of devices of devastation.

**Chemical Weapons**

Chemical agents can be gases or liquids. They include poisons, such as arsenic, Prussian acid, and strychnine. Choking agents, like chlorine and phosgene, can cause fluid to accumulate in the lungs and may lead to respiratory failure. Blistering agents, such as mustard gas, can also affect the lungs, as well as harming the eyes, respiratory system, and skin. Nerve gases, such as sarin and tabun, attack the body’s muscles and nervous systems (Laqueur, 1999).

In the 1870s, Irish nationals, referred to as the Fenians, were apparently the first group to try to use poison gas against their enemies; they hoped to spray it on the House of Commons in London (Laqueur, 1999, p. 242). Chemical gas attacks by the Germans in World War I killed thousands of Allied soldiers; the British and French retaliated, killing thousands of Germans. Chemical weapons subsequently were banned by international agreements, but that did not stop Adolf Hitler from using nerve gases against Jews in concentration camps. They were used more recently by Iraq in the war against Iran in the mid-1980s, by Libya against Chad in 1987, and by Saddam Hussein of Iraq against the Kurds in 1988 (Falkenrath, Newman, & Thayer, 2000).

Many chemical agents are used for legitimate medical, insecticide, and cleaning purposes and thus are readily available and often relatively cheap to purchase. In addition to the relative ease of their acquisition, the nerve gases manufactured today are more toxic than those of earlier eras.
Biological Weapons

A dead human body can be turned into a biological weapon. In the 14th century, the Tartars are believed to have catapulted plague-infected corpses over the walls of their enemies’ castles, initiating the Great Plague, also called the “Black Death," that eventually devastated much of Europe. Scientists confirmed that Japan used biological weapons against China and the Soviet Union during the early years of World War II (Falkenrath et al., 2000, p. 91).
In addition to spreading plagues, biological weapons can be used to spread smallpox, typhus, tuberculosis, Legionnaires’ disease, Ebola virus, and other infectious diseases. Biological weapons are relatively easy to produce and hide. By contaminating food and water, a small amount can wreak havoc.

The danger of bioterrorism became apparent for the first time to many people in the United States a few weeks after the 9/11 attacks when letters containing anthrax were sent through the U.S. mail: 5 people died from anthrax exposure and another 18 were known to be infected. More than a thousand people were tested for contact with anthrax, and about 30,000 people were given antibiotics to prevent infection.

Hundreds of other people reported exposure to substances that they feared were anthrax; most were false alarms. Health care professionals complained that the supply of antibiotics to counter anthrax was inadequate, and the Bush administration announced that it would buy antibiotics to treat up to 12 million people.

The ensuing investigation of the anthrax letters found no clear links to the September 11 attacks, and many officials speculated that homegrown bioterrorists were responsible. Subsequently, President Bush sent to Congress a proposed budget for fiscal year 2003 that sought an additional $11 billion over two years to protect the nation against biological terrorism; this amount quadrupled what was spent before the September 11 attacks to counter bioterrorism. Money also was earmarked for improving the nation's public health system and for pumping up budgets of federal agencies involved in biodefense. Funding was also provided to expand the national stockpile of vaccines and antibiotics, build anticontamination laboratories, research new drugs, and improve coordination among local, state, and federal emergency preparedness teams. The first reading that accompanies this chapter discusses the progress, or lack thereof, of many of these initiatives.

Views differ on the likelihood of bioweapons proliferation. Vogel (2006) has examined the development of the Soviet Union’s biological weapons programs and the subsequent threat of bioweapons proliferation. She argues that, with the fall of the Soviet Union and the adoption of U.S. nonproliferation assistance programs, more innovative studies are required to determine whether the knowledge possessed by former Soviet scientists might affect nonproliferation and counterterrorism policies in the future.

Radiological Weapons

A change in the nucleus of an unstable atom can result in the release of excess energy in the form of radiation. A radiological attack can kill and injure an untold number of people and animals and contaminate a large geographic area, perhaps for years or even centuries (Ballard & Mullendore, 2003). Terrorists can launch a radiological assault in two ways: attacking a nuclear facility or using a radiological device (Nuclear Threat Initiative, 2006).

When Abu Zubaydah, supposedly a high-level member of al-Qaeda, was captured in Pakistan in 2002, he told authorities about possible nuclear and radiological attacks. Many did not believe his claims until Jose Padilla was arrested later that year at Chicago’s O’Hare International Airport for “plotting to use a radiological bomb somewhere in the United States. The ‘dirty bomber,’ as he was labeled by the media, was now the person who the skeptics needed to believe that the threat was real” (Kushner, 2003, p. 1).

A “dirty bomb” uses common explosives, such as TNT, to spread radioactive material, but does not result in a nuclear explosion. Radioactive devices can come in many forms, including those that facilitate the transport of radioactive particles by air currents (Nuclear Threat Initiative, 2006).

Nuclear waste, from electric power generated at commercial nuclear plants and fissile materials at defense facilities, may take centuries to decay, posing major problems of waste disposal. The nation’s spent nuclear fuel and radioactive waste are currently stored in more than 120 sites around the country (U.S. Department of Energy, 2007). In 1982, Congress passed the Nuclear Waste Policy Act designed to establish a national policy on the disposal of nuclear waste and
subsequently approved the development of a long-term underground geologic repository on federal land at Yucca Mountain, in a remote area of Nevada. The current plans call for construction to start in 2009, with materials beginning to be received in 2017 (U.S. Department of Energy, 2007).

The Yucca Mountain project has received a great deal of negative attention over the years, in part from those who feared a terrorist attack while the spent nuclear fuel and radioactive wastes were being transported to the new facility. Ballard and Mullendore (2003, p. 772) describe the scope of the transportation problem in noting the following:

Local communities in more than 40 different states will be faced with an average of 3 to 6 shipments per day that are leaving the current storage facilities and traveling on the interstate highways, railways, and waterways of America toward Nevada and the Yucca facility. . . . [T]his level of activity will transpire every day, 365 days a year, and for at least 24 years. . . . The risk of a terrorist attack on nuclear waste shipments could be easily dismissed as someone else’s problem if it were not for the fact that these cargos will be in such easily identifiable vehicles and traveling set routes with such a frequency and duration that any potential saboteur or terrorist adversary would have no problem planning an attack against these materials.

Although the Department of Energy is still hoping to move forward with its timetable for Yucca Mountain, with the victory of Democrats in the 2006 Congressional elections, the future of the project is uncertain. The new Senate majority leader, Harry Reid of Nevada, has long opposed the project; in his new position of power, he has promised to prevent any pro-Yucca legislation, including funding, from being passed (Werner, 2006).
Nuclear Weapons

The world has witnessed two nuclear attacks: In 1945, the United States detonated nuclear bombs on the Japanese cities of Hiroshima and Nagasaki. The bombings brought a quick end to World War II, but at an awful cost to innocent Japanese civilians.

The ability to manufacture nuclear weapons depends on the availability of high-quality uranium and plutonium. These materials are frequently in transit from one nuclear reactor site to another, making them vulnerable to theft. Domestic pressures and international political differences make it difficult for the key nuclear states of Russia, China, France, India, and the United States to agree on methods of stopping the growth of nuclear weaponry (Barletta, 2001).

Pakistan has tested a nuclear device, and North Korea, Iran, and Iraq have developed or tried to develop nuclear capacity. When North Korea detonated a nuclear bomb in October 2006, all doubts were erased about the seriousness of the challenge facing Japan, South Korea, and ultimately the United States and its allies.

The United Nations Security Council imposed sanctions on Iran’s nuclear program at the end of 2006. In response, Iranian President Mahmoud Ahmadinejad asserted that the UN resolution designed to deprive his regime of nuclear materials was “invalid.” He opined that his country “is wise and will stick to its nuclear work and is ready to defend it completely” (“Ahmadinejad Says Iran’s Nuclear Plans Are Still On,” 2007).

Explosive Devices

Explosives are categorized as low or high depending on their rates of decomposition. Low explosives decompose rapidly, but do not usually explode on their own. High explosives decompose slowly and can explode on their own. High explosives can be divided further into primary explosives, like nitroglycerine, and secondary explosives, like TNT and dynamite. When Timothy McVeigh used a homemade truck bomb to blow up the Murrah Federal Building in Oklahoma City, he vividly demonstrated the harm that could be done by large-scale explosive devices.

The information necessary to construct explosive devices is readily available on the Internet. Such Web sites as “The Explosives and Weapons Forum” (http://www.roguesci.org/theforum) maintain bulletin boards that allow people to discuss their experiences with explosives and to assist others in their attempts to build better explosive devices.

How Real Is the Threat?

There have been many more hoaxes, pranks, and unconfirmed allegations reported than actual uses of CBRNE weapons. Most of the confirmed attacks have been made with simple “household” agents, which are unlikely to cause massive casualties. In addition, many CBRNE incidents have been criminally rather than politically motivated (Pate, Ackerman, & McCloud, 2001).

The Center for Nonproliferation Studies at the Monterey Institute of International Studies reported that the vast majority of CBRNE incidents were either failed attempts to acquire weapons of mass destruction, hoaxes, or pranks. Relatively few incidents resulted in death or serious injury (Monterey Institute for International Studies, 2001).

There are also many unconfirmed allegations of CBRNE attacks. For example, the United States has accused the Soviet Union of using toxic weapons against the Hmong tribesmen in Laos and against civilians and Khmer Rouge forces in Cambodia in the 1970s. South Africa was accused of using anthrax in the Rhodesian civil war of 1978–1980 and of releasing a deadly strain of malaria in Angola in the 1980s. Fidel Castro repeatedly has accused the United States of conducting biological attacks against Cuban crops (Falkenrath et al., 2000). In January 2000, a Russian general accused Chechen rebels of giving toxic wine and fruit to Russian soldiers in Chechnya (Pate et al., 2001).

In a report issued before the 9/11 attacks, the Henry L. Stimson Center, a nonprofit public policy research organizations, maintained that the United States was poorly prepared to react to
a significant attack using CBRNE weapons (Smithson & Levy, 2000). The Stimson Center’s study criticized the federal government for inadequately financing the disease surveillance and hospital systems that would likely be overwhelmed in a large-scale attack. According to the study, the government has funded training of emergency response teams of dubious value (Smithson & Levy, 2000). For example, more than $134.7 million was spent to prepare and train National Guard teams to help in the event of a germ or chemical terrorist attack, but the study found that the teams probably would not arrive in time to provide significant help to local populations because the germs and chemicals spread so quickly.

The Stimson Center study recommended that the United States stop funding emergency preparedness training programs and abolish the National Guard units responsible for responding to CBRNE attacks. Instead, it urged that funding be directed to outfit hospitals and fire stations with decontamination capabilities and to increase research and training. Further, the study criticized the lack of coordination of federal efforts, which resulted in the creation of about 90 terrorism training preparedness courses with different missions, resources, and requirements.

THE INTERNET AND TERRORISM

Terrorists have always cultivated technology to further their goals, and the use of computer networks to this end is no exception to the historical pattern. Cyberspace is appealing to extremists for numerous reasons, including its easy access and relative lack of regulations, its ability to reach a large audience, its anonymity, and its inexpensiveness.

According to Weimann (2006b), a search of terrorists’ presence on the Internet in 2006 revealed that more than 4,800 Web sites were maintained by terrorists or their supporters; this figure compares to a relative handful of terrorist sites only a decade ago. These sites may contain bulletin boards, chat rooms, publications, and videos. They may be official or unofficial Web sites of terrorist organizations, and they come in many languages and formats.

The Internet is used as a propaganda tool, of course, but that is just the tip of the iceberg (Weimann, 2006b). Terrorists also use it to contact colleagues, tap new sources of financial support, and plan attacks. They use the Internet to conduct debates and settle disputes. It also provides an abundance of detailed instruction for anyone interested in making bombs, rockets, flamethrowers, and dozens of other lethal weapons and poisons.

The Sri Lankan Tamils’ use of the Internet is a good example. Tamils living outside of Sri Lanka established a Web presence more than 10 years ago, posting to Usenet groups and launching several Web sites (Enteen, 2006). The goal of most of these Web sites is to advocate for national recognition for the Tamil people. The Tamil terrorist organization, the Liberation Tigers of Tamil Eelam, has likewise been a leader in the use of the Internet to get out its message and promote its long-range goals.

Digital Terrorism

The Internet has another, even more sinister potential: digital terrorism. Comprised of both information warfare and cyberterrorism, digital terrorism presents frightening possibilities for crippling vital economic, social, governmental, and other infrastructure.

Taylor, Caeti, Loper, Fritsch, and Liederbach (2006, p. 21) define six components of information warfare:

1. psychological operations: using information to influence the mental state of the adversary
2. electronic warfare: denying accurate information to an adversary
3. military deception: misleading foes about military capabilities or plans
4. physical destruction: destroying information systems
5. Security measures: protecting information systems from enemy infiltration

6. Information attacks: corrupting existing information without harming the physical structure where the information is located

A simpler definition is that “information warfare is any sort of strike or protective measure against an information system, whatever the means. Implanting a virus into a military computer is an information warfare tactic. On the other end of the spectrum, blowing up a cellular phone tower could also be considered information warfare” (Taylor et al., 2006, p. 21).

Cyberterrorism is the second component of digital terrorism. It is defined as a “premeditated, politically or ideologically motivated attack or threat of attack against information, computer systems, computer programs, and data that can result in violence against civilian targets” (Taylor et al., 2006, p. 23). A prolonged loss of water or power or serious disruption to the national economy, for example, could be socially destabilizing and deadly.

Whether a particular event should be categorized as information warfare or cyberterrorism may be difficult to determine, but taken together they demonstrate the threat posed by digital terrorism. For a legal and historical analysis of extremists’ use of computer networks, see Levin (2002).

Theoretically, it would take but one talented terrorist to devastate a country’s infrastructure and generate panic and death. Military bases, hospitals, airports, banks, power plants, and other critical components of daily life depend on computers. Boilers could be programmed to explode, national security data could be altered, air traffic control systems could be sabotaged, food and water sources could be poisoned through changes in computer-driven controls—the possibilities are limited only by terrorists’ skill and imagination.

How Real Is the Threat?

The Internet continues to evolve, as does its exploitation by terrorists. After the 9/11 assaults, Osama bin Laden issued a statement saying that “hundreds of young men had pledged to him that they were ready to die and that thousands of Muslim scientists were with him and who use their knowledge in chemistry, biology, and ranging from computers to electronics [sic] against the infidels” (Colarik, 2006, pp. 34–35).

Although the threat is real, thus far there have been no significant cyberattacks by terrorists on U.S. government information systems, transportation systems, power grids, nuclear power plants, or other key infrastructure components (Weimann, 2006a, p. 164). Cyberattacks are common, but they have been primarily conducted by nonterrorist hackers. A report issued by the IBM Global Security Analysis Lab in 2002 found that 90 percent of hackers were amateurs with limited skills, 9 percent had more skills, and only 1 percent were highly skilled (Weimann, 2006a, p. 165). D. Thomas (as cited in Weimann, 2006a) interviewed hundreds of hackers and reached the same conclusion: few hackers have the skills needed to launch a serious cyberattack. Thus, as with CBRNE attacks, the likelihood of a major digital terrorism attack is unknown.

Aum Shinrikyo: A Terrorist Cult

Only one large-scale attack with WMD by nonstate terrorists has been confirmed. The March 20, 1995, chemical weapons attack on Tokyo’s subways by the Aum Shinrikyo apocalyptic and millenarian cult was said to herald a new age of “catastrophic” terrorism (Smithson & Levy, 2000, p. xi).

Aum Shinrikyo was controlled by the messianic and highly eccentric Shoko Asahara. A large and wealthy cult, the members of which included several scientists, Aum Shinrikyo experimented with both chemical and biological weapons. It was able to obtain many of its raw materials from Russia and the United States.
Aum Shinrikyo was “a terrorist nightmare—a cult flush with money and technical skills led by a con-man guru with an apocalyptic vision, an obsession with chemical and biological weaponry, and no qualms about killings” (Smithson & Levy, 2000, p. xii). The group nevertheless could not overcome the technical and scientific difficulties in WMD production and dissemination, and the death toll from the attack fell far short of Aum Shinrikyo’s intent. Put another way, the attacks “were less deadly than some single-person shooting sprees, and required considerably more effort to prepare and carry out” (Falkenrath et al., 2000, p. 23).

Shoko Asahara: A Chaotic Leader

Shoko Asahara’s background seems bizarre for a terrorist leader (see, e.g., Cameron, 1999; Falkenrath et al., 2000; Laqueur, 1999; Mullins 1997; Walsh, 1995). Born Chizuo Matsumoto in 1955 on Kyushu, one of Japan’s major islands, he was blind in one eye and partly blind in the other. At the age of 5, he was sent to a special school for the blind, where his partial sight gave him a big advantage over the other students. He quickly turned this advantage into a position of power. With partial vision, Matsumoto helped his classmates, but in return he bullied and intimidated them into doing his bidding. After graduating from the school in 1977, Matsumoto moved to Tokyo. When he was refused entry into Tokyo University, he started studying acupuncture and herbal medicine. He married, and he and his wife opened a small shop selling traditional Chinese herbs and health tonics. The business went bankrupt after Matsumoto was arrested and fined for selling fake cures.

In 1984, Matsumoto opened a yoga school, began to gather disciples, and founded Aum Shinrikyo. Two years later, as his following grew, Matsumoto traveled to India, where he claimed to have become enlightened while alone in the Himalayan mountains. On returning to Japan, he changed his name to the “holy” Shoko Asahara. Aum in Sanskrit symbolizes the “powers of destruction and creation in the universe,” and shinrikyo means the “teaching of the supreme truth” (Reader, 2000, p. 15). As the name suggests, its leader’s mission was to teach his followers the truth about the universe.

As a religion, Aum was “a hodgepodge of ascetic disciplines and New Age occultism, focused on supposed threats from the U.S., which [Asahara] portrayed as a [conspiracy] of Freemasons and Jews bent on destroying Japan. The conspiracy’s weapons: sex and junk food” (Walsh, 1995). Asahara was demanding of his followers; for example, they were supposed to kiss his feet before addressing him.

From Bizarre to Dangerous

Aum was approved as a religious group under Japan’s Religious Corporations Law, which meant that it had tax benefits, the right to own property, and protection from government interference. It soon grew into a large organization with thousands of members. It also became rich with the money demanded from members: the group’s assets were estimated to be between $300 million and $1 billion (Senate Permanent Subcommittee, 1996). Aum owned many companies worldwide, including “a computer firm, a chain of restaurants and a fitness club in Japan; a Taiwanese import/export company; and a tea plantation in Sri Lanka” (Cameron, 1999, p. 284). It also had extensive land holdings in Japan and elsewhere. Many of Asahara’s followers were well educated, and several were doctors, engineers, and computer experts.

Why was Aum able to attract so many followers? One observer offers this explanation: “The time was ripe for gurus. Japan’s galloping economic miracle in the 1970s and ‘80s also spawned a boom in new religions offering spiritual refuge to Japanese alienated by materialism. Asahara’s messianic self-image expanded to help fill this void” (Walsh, 1995). Aum targeted people who were alienated from society, including lonely and emotionally needy people (Cameron, 1999, p. 284).

Asahara discouraged dissent and promoted his own unchallenged authority. To ensure obedience, he used brainwashing techniques, including sleep deprivation, poor diet, electric shock
treatments, and physical isolation. The cult also manufactured its own LSD and may have sold it to others (Sayle, 1996). Leaving the cult was not easy. Members were frightened, and some apparently were murdered for trying to escape. Outsiders who criticized the cult, including a lawyer, his wife, and their baby, were also murdered. That lawyer had been planning to sue Aum on behalf of some of the cult members’ parents (Kaplan & Marshall, 1996).

Aum continued to grow and expanded to Russia. Asahara once preached to a crowd of 15,000 in a Moscow sports stadium (Walsh, 1995). At its height, the cult was estimated to have 50,000 followers, of whom 10,000 were in Japan and up to 30,000 were in Russia (Cameron, 1999, p. 284).

In 1989, Asahara formed the Shinrito (”Supreme Truth”) political party in an effort to expand Aum’s base of support. In 1990, the party ran 25 candidates in the election for Japan’s Lower House Diet. All of them lost. Legal problems mounted when hundreds of the group’s
followers were accused of falsifying their legal residence so they could vote in Ashara’s district (Reader, 2000).

Stunned and humiliated by the defeat at the polls, Asahara became further alienated from the rest of Japanese society. His ambition switched from simply controlling Japan to destroying it (Cameron, 1999, p. 280). It is roughly around this time that Asahara became obsessed with the idea of the coming of Armageddon (Senate Permanent Subcommittee, 1996). He decided to fulfill this prophecy himself.

Aum apparently tried and failed several times to develop and disseminate biological weapons. The cult experimented with anthrax, Q fever, and botulinum, as well as trying to collect samples of the Ebola virus. In 1990, cult members drove around the area outside the Japanese parliament spraying a botulinum toxic aerosol. The Japanese Crown Prince’s wedding in 1993 was targeted for biological attack, but the group’s toxin was not ready in time; later that year, cult members again drove around the city spraying the toxin. In 1993, they tried to spray anthrax spores from the rooftop of their Tokyo headquarters (Cameron, 1999). None of these events caused any deaths (Kaplan & Marshall, 1996).

Aum had more success with developing chemical agents. The cult tested sarin gas on sheep at its farm in Australia (Cameron, 1999). Yet, the group again encountered numerous technical difficulties. For example, it had problems building electrolysis tanks and reactor vessels, and their Russian-made helicopters, which were to have been used to spray and disperse the gas, crashed (Cameron, 1999). In 1994, they nevertheless produced enough sarin gas to attack three judges who were presiding over a land fraud suit against the cult. The attack killed 4 and injured 150 people (Falkenrath et al., 2000, p. 20).

Not until 1995, however, did the Tokyo Metropolitan Police begin to seriously investigate Aum’s role in these assaults. Under Japan’s laws, religious organizations generally are exempt from official investigation. Its status as a recognized religion enabled Aum to keep its plans secret. Now, with the police investigating, Asahara felt pressured to quickly launch Armageddon, and he hatched a flimsy plan to release sarin gas in the Tokyo subway. The group did not wait to secure sufficiently pure sarin or to devise an effective dissemination strategy, dooming its plan for Armageddon.

The Attack

On the morning of March 20, 1995, five members of Aum Shinrikyo boarded subway trains at five different stations around Tokyo. Each member carried two sealed plastic pouches of sarin nerve gas and a sharpened umbrella. As the trains neared the center of the city, the terrorists put the plastic pouches on the floor and punctured them with the umbrellas. They then fled the subways as the liquids leaked quickly out of the bags. The effects were almost instantaneous: passengers began to sweat, their noses ran, they coughed and wheezed, some vomited, and others had seizure-like symptoms.

Twelve people died and more than 5,000 were injured (Senate Permanent Subcommittee, 1996). It could have been much worse. Had a more sophisticated approach been used, thousands could have been killed.

The Aftermath

After the attack, the police focused immediately on Aum Shinrikyo and raided the cult’s facilities. They seized large stockpiles of chemicals, including ingredients for nerve gases, such as sarin, VX, tabun, soman, and hydrogen cyanide (Cameron, 1999). On May 16, 1995, Asahara was arrested and charged with masterminding the subway attacks, as well as with 16 other crimes, including murders, attempted murders, manufacture of illegal drugs, and production of WMD. Japan’s so-called trial of the century began.

Asahara pled not guilty to most of the charges. He began his trial by firing his lawyer, and he refused to cooperate with any of his court-appointed attorneys. Often pictured wearing pajamas
and reported to be sleeping or mumbling to himself during the court proceedings, the bushy-bearded Asahara used his trial to reinforce his eccentric reputation.

Japan’s court system is complex, and it was not until February 2004 that he was sentenced to death. Several appeals ensued, but in September 2006, the Japanese Supreme Court rejected his final appeal, setting the stage for his eventual execution, provided the defense team does not apply for a retrial or an emergency appeal. It is unknown at this time when or if Asahara will be executed for his crimes.

After the attack, many members of Aum Shinrikyo tried to distance themselves from Asahara. The cult was reorganized, and its name was changed to Aleph, a name that symbolizes renewal. The cult apparently has renounced the belief that it is acceptable to commit murder to achieve its goals, but many Japanese still believe that Asahara controls the group.

**HIGHLIGHTS OF REPRINTED ARTICLES**

The first article selected to accompany this chapter extends the above discussion about Aum Shinrikyo by applying the lessons learned from the sarin gas attack on the Tokyo subway to the United States. The second article examines the likelihood of a nuclear attack and how the probabilities of nuclear occurrences are calculated.


This article examines lessons to be learned from the sarin gas attacks on the Tokyo subway system. The authors analyze the psychological barriers to interagency communications under disaster conditions. Using the 9/11 attacks as a point of comparison, the article examines the continuing problems of communication and coordination between Emergency Medical System (EMS) personnel at the attack site and area hospitals that received the injured victims.

In both Tokyo and the 9/11 attacks, many victims went on their own to the nearest treatment facility. This self-transport makes it difficult to determine which walk-in victims need the most help, hindering the allocation of resources during a disaster. Most hospitals in the United States lack enough beds, personnel, equipment, and isolation units to deal with a large-scale terrorist attack. Problems are also caused by the “worried well”; that is, people who fear they have been contaminated but have not been.


The second article selected to accompany this chapter discusses the process for arriving at the official estimates of the likelihood of nuclear terrorism. The research is based on declassified Central Intelligence Agency (CIA) National Intelligence Estimates (NIEs), as well as on unclassified CIA analyses, information on intelligence estimates leaked to the media, reports of government agencies and commissions, and comments by senior governmental officials. The reader is struck with the political, as opposed to purely scientific, nature of these estimates.

**EXPLORING TECHNOLOGY AND TERRORISTS FURTHER**

- Examine the Web site of the Center for Nonproliferation Studies at the Monterey Institute (http://cns.miis.edu/index.htm). What do their reports indicate about the possibility of CBRNE attacks?
・ The Carnegie Endowment for International Peace's Non-Proliferation Project (http://www.carnegieendowment.org/npp/) posts news and analysis on a variety of problems associated with CBRNE attacks. Its Web site posts critiques of the Bush administration's policies as well as threats and capabilities of nations around the globe.

・ Examine the United Nations Web site on weapons of mass destruction. Topics include treaties and conventions on unconventional weapons, as well as transcripts from the latest symposiums on terrorism and disarmament. The Web address is http://disarmament.un.org/wmd/.

・ The Henry L. Stimson Center (http://www.stimson.org/home.cfm), a nonprofit, nonpartisan organization, posts online publications such as “Iraq: Hard Choices, Real Consequences,” “Can the United States Contain Iran?” and “Next Steps on North Korea: Options Beyond Sanctions.”

・ Learn more about the underground geologic repository at the Yucca Mountain site from http://www.ocrwm.doe.gov/ym_repository/index.shtml.

・ The first reprint for this chapter, by Beaton et al., discusses the TopOff2 exercise of May 2003. Describe the exercise and the conclusions drawn from it.

・ According to Beaton et al., what types of problems can arise from victims transporting themselves to nearby medical centers? Who are the “worried well” and what types of problems do they pose?

・ Beaton et al. describe the Strategic National Stockpile (SNS). What is the SNS and what types of problems might hinder an effective emergency response to a terrorist attack of this sort?

・ Discuss the four major conclusions drawn by Zenko, the author of the second article reprinted in this chapter.

・ Explain Zenko's analysis of the NIEs of Iraq's weapons of mass destruction program. How did these estimates influence U.S. behavior?

・ According to Zenko, what is known about al-Qaeda's attempts to obtain nuclear materials?

**VIDEO NOTES**

Although weapons of mass destruction may seem like something from a movie plot, modern films contain few good studies of the threat of biological and chemical weapons. A celebrated drama about a global nuclear crisis spawned by terrorists is *Crimson Tide* (Hollywood Pictures, 1995, 115 min.).
This paper focuses on some of the lessons learned from the sarin gas attack on the Tokyo, Japan subway a decade ago. Members of a “doomsday” cult released sarin gas, a neurotoxic agent, in the Tokyo subway system, killing twelve people and causing more than five thousand people to seek medical care. The aim of this paper is to revisit the many lessons of the sarin gas attacks on the Tokyo subway system (especially the “psychosocial lessons”) and to compare and contrast present-day preparedness for a similar disaster and the ensuing psychosocial sequelae in the United States—10 years later. Lessons learned from the Tokyo subway sarin gas attacks were based not only on articles by Taneda (2005) and Kawana, et al. (2005) but also on a review of the published works of Okumura et al. (1998a, 1998b, 1998c), Matsui, Ohbu & Yamashina (1996) and Ohbu et al. (1997) among others.

COMMUNICATION OF VITAL INFORMATION

Although more than six years had elapsed since the sarin gas attacks on the Tokyo subway system, pre-hospital communication at the Pentagon terrorist disaster site on 9/11/2001 was suboptimal. According to the Arlington County after-action report prepared by Titan Systems, “Almost all aspects of communications continue to be problematic, from initial notification to tactical operation: In the first few hours following the attack on the Pentagon, foot messengers at times proved to be the most reliable means of..."
communication.” This report also noted that “communications and coordination were deficient between Emergency Medical System (EMS) control at the incident site and area hospitals receiving injured victims” (Department of Justice, 2002).

Since 9/11 there has been a concerted effort, including federal funding in the U.S., to provide emergency and rescue organizations with interoperable radios and communication protocols (FEMA, 2003). In King County, Washington (U.S.) the police, the State Department of Health, the county, the state, the Emergency Operation Centers (EOC’s) and all local hospitals use a common communication device with preset channels (Mariotti, Personal Communication, 2004).

Still, very little is known to date about the psychosocial barriers or impediments to interagency communication under disaster conditions. As recently as the second Top Officials (TopOff 2) exercise in May of 2003, interagency communication at all levels appeared to be problematic. In addition to infrastructure problems, communication was adversely affected by power differentials between local, state and federal authorities and a “cultural clash” between agencies. TopOff 2 was the largest and most comprehensive multi-agency terrorism exercise ever held in the U.S. It brought together top government officials from more than 100 federal, state and local agencies as well as the Canadian government to test the domestic response to mock terrorist attack(s) employing weapons of mass destruction. In the Illinois venue sixty-four hospitals responded to a simulated outbreak initiated by a bioterrorist attack. The TopOff 2 after-action report noted that “... the lack of a robust and efficient emergency communications infrastructure was apparent.” Most importantly, communication problems were the primary cause of flawed public policy decision making (DHS, 2003), as was the case in the original TopOff exercise in 2000 and in the case of the anthrax attacks in Florida in 2001.

In the event of a covert attack employing an imperceptible chemical or biologic agent, early communication and identification of the causative agent may well be crucial in initiating timely treatment designed to protect emergency workers and to initiate risk communication messages. While a chemical assay and confirmation of the sarin as the neurotoxic agent used in the Tokyo subway attack was not available until several hours after the attack (Taneda, 2005), there are now emerging technologies that may allow practically instantaneous point-of-service analysis of a chemical or bio-agent. The latter might include detection of a pathogen even before victims show signs or symptoms; e.g., BioWatch program (The White House, 2004). Thus, some recent advances in point-of-service technology under development in the U.S. might improve initial communication and timely diagnosis of victims of a covert bioterrorist or chemical attack. This would, in turn, guide initial treatment, prophylaxis, and improve the safety of rescue workers and hospital personnel alike.

A recently published series of articles on developing risk communication messages for terrorist events employing so-called Weapons of Mass Destruction (WMD) has the potential to improve the effectiveness of early post-event information for the general public. Based on findings from a series of focus groups with diverse community representation, Centers for Disease Control and Prevention (CDC) researchers learned how U.S. citizens and U.S. EMS personnel were likely to view a threat of or an actual WMD event, what kind of information they need to be able to respond appropriately and what communication channels they will likely rely upon (Vanderford, 2004; Becker, 2004, Wray & Jupka, 2004, Glik, Harrison, Davoudi & Riopelle, 2004). Timely and accurate risk communication could reduce unwarranted fear in the general populace and perhaps reduce, to some extent, demands on the health care system stemming from psychosocial factors, e.g., the “worried well” victims seeking treatment. Improved risk communication in the immediate aftermath of a terrorist attack employing a biological, chemical or radiologic agent could also improve the efficiency and safety of any ensuing emergency medical service response.

**Operational Logistics**

As with many, if not most, disasters, victims self-transported to nearby treatment facilities. For many victims of the Tokyo sarin gas attacks this was St. Luke’s Medical Center (Taneda, 2005). Similarly on September 11, 2001, at the Pentagon disaster site some surviving victims drove...
themselves or walked to nearby treatment facilities (DoJ, 2002). The problems arising from this self-transfer phenomenon are serious and complex. Without a pre-hospital triage system, such as Simple Triage and Rapid Transport (START), seriously injured victims who need immediate care might not get the timely and appropriate treatment (Hafen, Karren, & Mistrovich, 1992). Furthermore, the pre-hospital Incident Command System cannot accurately evaluate walk-in victim needs and appropriately meter the allocation of pre-hospital and area hospital resources (DoJ, 2002).

While there is ample evidence that disaster victims self-refer and self-transport to the nearest hospital, usually within minutes of a disaster, current Joint Committee on Accreditation of Healthcare Organizations (JCAHO) standards for emergency management hospital plans do not explicitly identify the problem of self-referral or self-transport (www.jcaho.org). Current JCAHO emergency management hospital standards also do not include plans for responding to surge capacity; that is, the influx of a massive number of disaster casualties and the need to treat them in a short period of time. The reality is that the casualty flow to nearby hospitals begins within minutes of a disaster with most casualties arriving at nearby hospitals on their own, in non-emergency vehicles within an hour and a half of the disaster impact (Auf der Heide, 1996). This is one of the operational lessons from the sarin gas attacks on the Tokyo subway system that we have yet to heed (Taneda, 2005).

Even if all available pre-hospital and hospital resources are allocated appropriately, surge capacity remains a problem for most EMS, Emergency Department and trauma hospital systems in the U.S. (AHRQ, 2004). Most hospitals in the U.S. lack adequate beds, equipment, isolation facilities and staff to respond to a large-scale terrorist attack. The Health Resources and Services Administration (HRSA) has set a critical surge capacity benchmark for all U.S. states, but converting from a current capacity system to a surge capacity system within a matter of hours still remains a daunting task in the U.S. (HRSA, 2004).

One federal program that predated 9/11 and which was developed to address at least one component of the problem of surge capacity is the Strategic National Stockpile (SNS). The SNS is a national repository of antibiotics, chemical antidotes, antitoxins and medical supplies needed in the event of a large scale mass casualty disaster or a bioterrorist event. It is managed, jointly by the Department of Homeland Security and the Department of Health and Human Services and is designed to augment state and local resources during a large-scale disaster or bioterrorism (Esbitt, 2003; Havlak, Gorman & Adams, 2002). The SNS is designed to supplement and resupply state and local efforts in the event of an emergency anywhere and at anytime within the U.S. or its territories, within 12 hours of approval of a request. The SNS maintains caches of medications and chemical antidotes that could be accessed in the event of a chemical or biodisaster regarding the latter, many hazardous materials teams and medic personnel in the U.S. have been trained in the pre-hospital administration of nerve gas antidotes such as pralidoxime chloride (2 PAM or 2 PAM chloride). In fact, the patient care protocols of Pierce County Washington recently authorized emergency medical technicians to administer the Mark I nerve agent antidote for the first time (Medical Program Director—Pierce County, 2005). A combination of pralidoxime chloride (2-PAM or 2-PAM Chloride) and atropine may be administered for nerve gas poisoning. The availability of drugs in the field is crucial, since the optimal time window for administration of nerve gas antidote is brief—in the case of a significant exposure to certain neurotoxic agents the time window for the administration of the antidote is only seconds to minutes (Holstege, Kirk & Sidell, 1997). The SNS represents an advance in our U.S. preparedness circa 2005 since nerve gas antidotes stocks were insufficient in the aftermath of the Tokyo sarin gas attack and no plan or system was in place to augment their stores (Okamura, Suzuki, Fukuda et al., 1998).

Unfortunately the 12-hour response time for SNS is inadequate for a nerve agent exposure, where treatment must be accomplished quickly in order to save as many lives as possible. As a result, the CDC established the CHEMPACK program for the "forward" placement of sustainable repositories of nerve agent antidotes in numerous locations throughout the U.S., so that they can be immediately accessible for the treatment of affected persons. Presently a pilot program, the CDC maintain ownership of the CHEMPACK stockpile (CDC, 2004), but in
conjunction with state and local officials, locate the antidotes in numerous strategically placed containers under controlled and monitored storage conditions for use in the event of an emergency involving nerve and other chemical agents.

We also need to consider surge capacity for mental health needs to provide care for victims, co-victims and communities following a terrorist attack with massive numbers of casualties (Hall, Norwood & Fullerton, 2002). Current JCAHO emergency management plans for U.S. hospitals do not include any mention of “worried well” nor other disaster mental health issues (www.jcaho.org). Just as medical care providers may be overwhelmed by a mass casualty incident, likewise the social work staff of medical centers may be overwhelmed. Communities need to have plans in place to recruit those trained in mental health support from a wide range of fields—crisis intervention call lines, clergy, chaplains, counselors, clinics, etc.

**SECONDARY CONTAMINATION OF EMERGENCY RESPONDERS AND HOSPITAL PERSONNEL**

Certainly EMS and hospital staffs in the U.S. are much more aware now of the potential for a terrorist attack in their communities employing nerve gas and other chemical agents. This awareness probably stems more from the events of 9/11 and anthrax attacks on the East Coast in this country in 2001 than from lessons learned from the Tokyo subway sarin gas attacks. Most urban fire departments and hospital personnel in the U.S. have, by now, been offered at least some awareness-level training and many now possess response teams with some Weapons of Mass Destruction (WMD) operational capabilities (Beaton & Johnson, 2002). Many U.S. public health workers and health providers have participated in WMD training and mass casualty drills, which have been documented to enhance knowledge and/or their perceived competency to respond to a WMD event in their communities (Beaton & Johnson, 2002; Beaton & Oberle et al., 2003; Beaton et al., 2004). An enhanced awareness of the signs and symptoms of a large-scale chemical attack could greatly limit, or even entirely prevent, secondary contamination of EMS and hospital staff, for instance, which was prevalent in the Tokyo sarin gas attacks (Taneda, 2005). Secondary transmission of sarin gas can occur since clothing and other belongings release sarin vapor for about 30 minutes after contact with sarin, leading to exposure of other people (i.e., secondary contamination). People may not be aware that they were exposed to sarin gas and other neurotoxic agents because they are odorless and colorless.

Another legacy of the Tokyo subway sarin gas attacks has been an increased appreciation of the importance of pre-hospital and hospital decontamination facilities (Jagninas & Erdman, 2004). Only limited decontamination of the Tokyo subway sarin gas attack victims was performed (Okamura, 1998). Pre-hospital or hospital decontamination could conceivably have reduced these victims’ symptoms arising from sarin gas exposures via absorption and inhalation routes as well as many, if not most, cases of secondary contamination of hospital personnel. A related psychosocial assumption is that primary victims of a chemical attack with few or mild symptoms that quickly resolve might be less likely to have lasting and/or severe psychosocial sequelae (DeWolfe, 2003).

Partnered with the decontamination, hospital and EMS directives in the U.S. regarding Personal Protective Equipment in response to identified or unidentified hazardous materials exposure could further reduce the likelihood of secondary contamination of First Responders and hospital personnel (OSHA, 2004 29CFR1910.120(g)). Some staff at receiving hospitals in Tokyo in the aftermath of the sarin gas attacks were not even wearing latex gloves or gauze masks, let alone hazardous material suits with respiratory protection which is the current U.S. standard to respond to a potential nerve gas agent. Of course, the Tokyo EMS and hospital personnel did not know what they were dealing with for several hours following the sarin gas attacks.

**THE “WORRIED WELL”**

One of the most challenging problems associated with a terrorist event are “worried well” who seek treatment out of fear or concern even though they have not been exposed to the chemical agent or pathogen (Bartholomew & Wessely, 2002). Following the terrorist attack on the Tokyo...
subway system “worried well” patients outnumbered patients with an exposure by a ratio of > 4:1. This response pattern is problematic since these “worried well” victims may consume scarce resources and may block access of critically-ill disaster victims who have experienced an actual exposure (Evans, Crutcher, Shadel, et al., 2002). These “worried well” patients, sometimes referred to as victims of “mass hysteria,” represent a problem for the disaster response, but they also should be considered patients who are “not well” and who, at the very least, need an initial medical evaluation, understanding, guidance and a plan (Stein et al., 2004; Pastel, 2004).

Obviously, some kind of definitive test or pathognomonic sign of exposure would be helpful in making a differential diagnosis but, lacking that, and complicating matters further, certain signs and symptoms of chemical and bio-exposure may overlap with cognitive and behavioral signs and symptoms of stress and anxiety (Beaton & Murphy, 2002). Therefore, it might be prudent to triage and hold presumably “worried well” patients for observation since more definite signs/symptoms of an actual exposure might emerge after some delay. Even if they have no direct exposure “worried well” victims would benefit from reassurance, some relevant information such as a fact sheet with guidance, a follow-up protocol, and available community resources. However, methodological sound research on such interventions for the “worried well” is still lacking (North & Pfefferbaum, 2002). At a pre-hospital WMD incident site such a triage protocol for “worried well” patients might also be possible (Copass, personal communication, 2001). However, given the large footprint of most disaster event sites and the perception by the public that definitive care is given at hospitals, medical centers must continue to expect and prepare for large numbers of self-referred victims with vague or mild complaints.

In a larger community context, timely and accurate risk communication might have reduced the number of worried well seeking medical treatment in the aftermath of a mass casualty event such as those seeking treatment in Tokyo two days or more following the attack. Effective risk communication might also have reduced the number of “white powder incidents” in the U.S. and calmed fears worldwide in the aftermath of the anthrax “attacks” on the Eastern seaboard of the U.S. in the fall of 2001 (ABC news, 2001). In these “attacks” anthrax powder was mailed in envelopes to several media and congressional authorities via the U.S. Postal system. As a result, a small number of individuals developed cutaneous or pulmonary anthrax and a large number of those potentially exposed received prophylactic antibiotics. For several months there were hundreds of reports of suspicious “white powder/possibly anthrax” that were investigated. Virtually all of these “white powder” substances after December of 2001 (or west of the Mississippi) tested negative for anthrax. A distinct improvement from past practice, current response plans in many U.S. communities incorporate formation of a Joint Information Center (JIC). JICs utilize local expertise and leadership to provide a single unified “voice” regarding important health risk communication information of the event, utilizing local media to distribute information broadly.

**Lack of Mental Health Preparedness for Rescue Workers**

Even though most samples of rescue and recovery workers show emotional resilience during and in the aftermath of disasters (Norris, Friedman, Watson, et al., 2002) at least some emergency responders such as firefighters do evidence secondary traumatic stress symptomatology (Beaton, Murphy, Johnson, Pike & Corneil, 1999). In certain cases their secondary traumatic stress reactions are transitory (Beaton, Murphy, Johnson & Nemuth, 2004), but some manifest chronic post traumatic stress disorder in the aftermath of disasters (McFarlane, 1989). Obviously any intervention that could prevent the onset and progression of post traumatic stress disorder in emergency workers would be well received. Critical incident stress debriefing (CISD) has been proffered as potentially therapeutic (Mitchell & Everly, 2001). There is and continues to be, however, an ongoing controversy regarding the clinical efficacy of CISD as a stand-alone intervention, or even within the context of a critical incident stress management program (CISM; McNally, Bryant & Ehlers, 2003). In fact, an NIH Consensus Conference Report on Mass Violence in 2002 noted the absence of methodologically sound data.
showing that debriefing actually deterred the onset or progression of PTSD and did not recommend its use for either rescue workers or for primary victims (NIMH, 2002). This same NIH Consensus Conference suggested that the term “debriefing” should no longer be used to describe this technique and also pointed to research evidence that it might actually cause psychological harm in some trauma victims. Likewise, “Psychological First Aid” for disaster workers (See Table 1) has been promulgated as potentially helpful (NIOSH, 2001) but this “intervention” has not been studied rigorously either.

### Table 1: Psychological First Aid

<table>
<thead>
<tr>
<th>What You Can Do On-Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Taking care of yourself will help you to stay focused on hazards at the site and to maintain the constant vigilance you need for your own safety. Often responders do not recognize the need to take care of themselves and to monitor their own emotional and physical health—especially when recovery efforts stretch into several weeks. The following guidelines contain simple methods for helping yourself. Read them while you are at the site and again after you return home.</td>
</tr>
<tr>
<td>• Pace yourself. Rescue and recovery efforts at the site may continue for days or weeks.</td>
</tr>
<tr>
<td>• Take frequent rest breaks. Rescue and recovery operations take place in extremely dangerous work environments. Mental fatigue over long shifts can place emergency workers at greatly increased risk for injury.</td>
</tr>
<tr>
<td>• Watch out for each other. Co-workers may be intently focused on a particular task and may not notice a hazard nearby or behind.</td>
</tr>
<tr>
<td>• Be conscious of those around you. Responders who are exhausted, feeling stressed, or even temporarily distracted may place themselves and others at risk.</td>
</tr>
<tr>
<td>• Maintain as normal a schedule as possible: <em>regular eating and sleeping are crucial.</em> Adhere to the team schedule and rotation.</td>
</tr>
<tr>
<td>• Make sure that you drink plenty of fluids such as water and juices.</td>
</tr>
<tr>
<td>• Try to eat a variety of foods and increase your intake of complex carbohydrates (for example, breads and muffins made with whole grains, granola bars).</td>
</tr>
<tr>
<td>• Whenever possible, take breaks away from the work area. Eat and drink in the cleanest area available.</td>
</tr>
<tr>
<td>• Recognize and accept what you cannot change—the chain of command, organizational structure, waiting, equipment failures, etc.</td>
</tr>
<tr>
<td>• Talk to people when YOU feel like it. You decide when you want to discuss your experience. Talking about an event may be reliving it. Choose your own comfort level.</td>
</tr>
<tr>
<td>• If your employer provides you with formal mental health support, use it!</td>
</tr>
<tr>
<td>• Give yourself permission to feel rotten: You are in a difficult situation.</td>
</tr>
<tr>
<td>• Recurring thoughts, dreams, or flashbacks are normal—do not try to fight them. They will decrease over time.</td>
</tr>
<tr>
<td>• Communicate with your loved ones at home as frequently as possible.</td>
</tr>
</tbody>
</table>

**SOURCE:** Excerpted from NIOSH fact sheet “Traumatic Incident Stress: Information for Emergency Response Workers.”

---

**Behavioral Health Preparedness and Treatment for Disaster Victims**

One arena in which we have made very little progress in our mass casualty planning has been that of behavioral or mental health preparedness. This has been on the “back burner” and not integrated into most U.S. or state disaster plans. In fact, as recently as 2003, a systematic review of 31 U.S. state and territory plans concluded the state mental health disaster plans were “both
variable and incomplete” and that “virtually all of the reviewed state (mental health) plans lacked key elements” (HHS, 2003). On a more positive note, this recent document observed that state mental health plans in process were now paying closer attention to terrorism and terrorist events (HHS, 2003). Most of the barriers to mental health disaster preparedness are well known and long standing. In addition to the persisting stigma of mental problems/disorders, many of the limitations and barriers to disaster mental health planning are noted in Table 2.

Best practice “early intervention” guidelines to assist disaster victims in the immediate aftermath of a disaster have been identified and represent a range of options including efforts to reduce immediate danger, provide safety, foster resilience and provide social support, all in an effort to reduce long-term psychological disorders and to treat acute psychiatric reactions (Ritchie et al., 2004). We also have a better appreciation of the short-term and longer-term impacts of disasters in general, and of terrorist-induced disasters in particular, on the emotional and behavioral health of primary victims and co-victims in surrounding communities (Shariat, et al., 1999; Okumura, et al., 1998a; DeWolfe, 2000; North, et al., 1999; Pfefferbaum, 2000; Schuster, et al., 2001; Schlenger et al., 2002). We also recognize that certain vulnerable populations, such as children, may have special psychological needs following a terrorist disaster (Pfefferbaum, et al., 1999; Pfefferbaum et al., 2002). (See Table 3 for a listing of other vulnerable populations based on disaster research and findings with combat veterans.)

One compelling lesson from the sarin gas attacks on the Tokyo subway is that some victims of terrorist events continue to have post trauma symptoms even with treatment. For many victims post trauma symptoms persist for years following the event (Kawana et al., 2005). However, while we may now more clearly recognize the short-term and long-term impact of a terrorist event on primary and secondary victims, we still do not have conclusive evidence that early interventions are effective. Furthermore, the available evidence suggests that the standard early and long-term interventions for trauma victims (Cognitive Behavioral Treatment (CBT), Eye Movement Desensitization and Reprocessing (EMDR) and Stress Management) are not helpful for all survivors. Dropout rates from studies of CBT in trauma samples are about 20% (Ballenger et al., 2000). Even in samples of PTSD patients who complete CBT, more than half may still meet the DSM-IV Criteria for PTSD at the post treatment assessment (Resick et al., 2002; Tarrier et al., 1999). Furthermore, even if PTSD symptoms are partially ameliorated, not all PTSD patients receiving CBT rate their post-treatment functioning as “good” (Marks et al., 1998).

Another lesson of the sarin gas attacks on the Tokyo subway system, also supported by other empirical findings and theoretical perspectives, is that trauma victims may manifest their symptoms cognitively, socially, behaviorally, emotionally, as well as physically (Van der Kolk, 1988; Van der Kolk, 1994; Krystal, et al., 1989). The assessment of post trauma symptomatology reported by Kawana, et al. (2005) purposely included physical symptoms in an effort to detect and measure “masked PTSD” in sarin gas

<table>
<thead>
<tr>
<th>Table 2</th>
<th>Barriers to Disaster Mental Health Planning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of human and financial resources to do the work</td>
<td></td>
</tr>
<tr>
<td>Little political will to focus on disaster mental health over many years, once a disaster passes</td>
<td></td>
</tr>
<tr>
<td>Mental health being overlooked in favor of safety and security concerns</td>
<td></td>
</tr>
<tr>
<td>The lack of collaboration and consistency among federal departments and agencies including SAMHSA/CMHS, the Department of Justice, the Centers for Disease Control and Prevention, and the Health Resources and Services Administration and corresponding state departments and agencies receiving disaster and terrorism funding</td>
<td></td>
</tr>
<tr>
<td>The lack of well-defined, “proven” and easily implemented programs in disaster mental health that can be adopted widely</td>
<td></td>
</tr>
</tbody>
</table>

attack survivors. Too, there may be some conceptual overlap between “masked PTSD” and “multiple unexplained physical symptoms” not infrequently observed in the aftermath of chemical, biological and/or radiological incidents (Pastel, 2004). A chronic bioneuroendocrine dysfunction has been hypothesized that may, in part, account for these physical symptoms in trauma survivors (Yehuda, et al., 1991)

**CONCLUSIONS AND FUTURE DIRECTIONS**

Compared to the 1995 Tokyo subway sarin gas disaster, there are no doubt both an increased awareness and improved, although still imperfect, communication and logistical capabilities to respond to a similar mass casualty event in the U.S. in 2005. However, most U.S. hospitals have yet to adopt realistic policies to triage and decontaminate and treat large numbers of victims of such a chemical attack who may self-transfer to the nearest available health care facility. There are also no current U.S. hospital standards nor widely adopted health care protocols to respond to the needs of the “worried well,” co-victims of a covert or overt chemical or biological attack. The basis for effective health risk communication in the immediate aftermath of a WMD terrorist event has improved, at least in theory. Yet we still have a paucity of evidence-based treatments designed to ameliorate the distress of victims of a terrorist attack employing chemical weapons or to prevent the onset and progression of post traumatic stress disorders and other adverse psychological outcomes in rescue workers and in hospital personnel. In most U.S. hospitals, states and jurisdictions there is still no mental health response component integrated into existing all-hazards disaster plans (HHS, 2003).

Use of psychotropic medications to ameliorate symptoms and sequelae of Acute Stress Disorder (ASD) and PTSD is a promising new area of treatment. Much has been learned from managing military combat-related PTSD, resulting in new approaches (Morgan, Krystal & Southwick, 2003). Propranolol, a beta-blocker, has benefited acutely traumatized burn victims (Pittman, et al., 2002), and stimulated further research. An important recent finding is the significant reduction in hyper-vigilance, flashbacks, intrusive memories, nightmares and insomnia in post-trauma patients given Prazosin, and alpha-1 antagonist (Raskind, et al., 2003). A “morning after” pill designed to mitigate psychic damage from acute trauma may not be too far off.

Chronic PTSD now has a range of FDA approved medication treatments including SSRI antidepressants (Sertraline, Fluoxetine, Paroxetine) and combination therapies with low dose mood stabilizers (Asnis et al., 2004) and/or low dose atypical antipsychotics (Stanovic, James & Vandevere, 2001). Carefully employed psychotropic medication combined with behaviorally oriented goal-directed therapy has the potential to offer disaster trauma victims better outcomes.

In terms of future directions, we still have not applied many of the psychosocial lessons learned from the sarin gas attack on the Tokyo subway system a decade ago. There may be special features of a deliberate, man-made covert terrorist attack, such as “uncertainty” that are particularly distressing and anxiety provoking and increase the risk of long-term mental health sequelae (Stein, et al, 2004). We are challenged to develop new interventions and to modify current standard trauma interventions to better treat victims of “the next” sarin gas attack.

### Table 3: Vulnerable Populations to Post-Disaster and Combat Distress

- Pre-existing mental illness ([Yehuda, 2002](#)
- Prior mental illness ([McFarlane, 1989](#)
- Females (more short-term distress in U.S. sample post 9/11) and more long-term post-trauma symptoms in Japanese sarin gas attack victims ([Kawana, et al., 2005; Silver, 2002](#)
- Those with intense and/or prolonged trauma exposures ([Goldberg, et al., 1990](#)
- Hispanic and other immigrant populations, including refugees ([Galea, et al., 2002](#)
- Weak or deteriorating psychosocial resources ([Norris, et al., 2002](#)
- Pre-existing chronic medical illness ([Bromet et al., 1998](#)
NOTES

1. Randal Beaton, PhD, EMT, Andy Stergachis, PhD, RPh, Mark Oberle, MD, MPH, and Elizabeth Bridges, RN, PhD are affiliated with the University of Washington. Correspondence should be addressed to: Randal D. Beaton, PhD, EMT, Research Professor, University of Washington, Department of Psychosocial & Community Health, Box 3257263, Seattle, WA 98195-7263/(206) 543-8551/e-mail: randyb@u.washington.edu

2. Marcus Nemuth, MD is affiliated with the Veterans Affairs Administration of Puget Sound.

3. Tamlyn Thomas, STAT RN is affiliated with the University of Washington Medical Center.

4. Acknowledgements: This article was made possible by grant number 1 T01HP01412–01–00 from the Health Resources and Service Administration, DHHS, Public Health Training Center Program and was also supported, in part, by a cooperative agreement from the Center for Disease Control and Prevention (CDC) through the Association of Schools of Public Health (ASPH), Grant Number U36/CCU300430–21. The contents of this article are solely the responsibility of the author and do not necessarily represent the official views of CDC or ASPH.

REFERENCES


Copass. (2002). Personal communication from director of Harborview Medical Center Trauma Unit.


Joint Committee on Accreditation of Healthcare Organizations (JCAHO) available at www.jcaho.org, accessed 12/30/04.


Pfefferbaum, B., North, C.S., Flynn, B.W., et al. (2002). Disaster mental health services following the 1995 Oklahoma City bombing: Modifying approaches to address terrorism. *International Journal of Neuropsychiatric Medicine, 7*(8), 575–579.


This article represents the first comprehensive analysis of publicly available intelligence assessments regarding the threat of nuclear terrorism to the United States. It draws primarily on declassified Central Intelligence Agency (CIA) National Intelligence Estimates (NIEs) but also on unclassified CIA analyses, intelligence estimates leaked to the media, the findings of relevant government agencies and commissions, and statements made by senior intelligence and political officials. Since nuclear terrorism lies at the nexus of three arenas that the U.S. government treats with supreme secrecy—intelligence, nuclear weapons, and terrorism—this discussion will necessarily remain unfinished until all of the relevant information is declassified. Nevertheless, given the past, present, and future threat posed by nuclear terrorism, it is essential to understand the collective judgments of the U.S. Intelligence Community (IC) on the subject—not only during the past five years, but over the past fifty.

I proceed in five sections. I begin with a discussion of the purpose, production, and inherent limitations of community-wide intelligence estimates. Turning to the evidence, I first review intelligence estimates on the possibility of Soviet or Chinese clandestine nuclear attacks on the United States, the first manifestation of nuclear terrorism during the 1950s and 1960s. Next, I explore the era of modern international terrorism that emerged in the late 1960s, along with concerns about U.S. civilian nuclear safeguards and unsecured American nuclear storage depots abroad. I then address the breakup of the Soviet Union, including the subsequent insecurity of its nuclear arsenal and the arrival of the international jihadist groups with nuclear ambitions, most notably al-Qaeda. Finally, I analyze the key themes that stand out upon examining more than a half-century of declassified intelligence estimates of the nuclear terror threat. A careful review of the available evidence reveals four key findings: (1) nuclear weapons or materials can be stolen or diverted with relative ease; (2) terrorist groups are obsessed with obtaining a nuclear weapon; (3) a bomb could be smuggled into America without detection; and (4) the U.S. government has been, and remains, insufficiently prepared to counter these threats.

WHAT ARE INTELLIGENCE ESTIMATES?

Intelligence estimates are analytical products developed by the IC to establish both the state of knowledge of an important issue and clear gaps in understanding.1 Government agencies,
businesses, and large organizations produce versions of intelligence estimates to better comprehend their operating environments and to develop long-range action plans. Because competitors and adversaries continuously hide their true intentions through denial and deception, intelligence estimates naturally suffer from a lack of information. In the U.S. government, the crown jewel of intelligence estimates is the NIE. According to the CIA,

A National Intelligence Estimate (NIE) is the most authoritative written judgment concerning a national security issue prepared by the Director of Central Intelligence. Unlike "current intelligence" products, which describe the present, most NIEs forecast future developments and many address their implications for the United States. NIEs cover a wide range of issues—from military to technological to economic to political trends. NIEs are addressed to the highest level of policymakers—up to and including the President. They are often drafted in response to a specific request from a policymaker. Estimates are designed not just to provide information but to help policymakers think through issues.2

The process of writing an NIE begins either when the director of national intelligence (DNI) chooses to produce one, or when the executive branch, the Joint Chiefs of Staff, or, more rarely, Congress, requests one. Once the request is approved, Terms of Reference are drafted to outline "issues and key questions to be covered in the Estimate."3 Next, a national intelligence officer in the National Intelligence Council (NIC), or an outside expert, drafts the Estimate based on all of the available information on the subject. The author then distributes it for approval to the fifteen intelligence agencies that comprise the wider IC, which are allowed to include dissenting opinions in footnotes on key issues of disagreement. The NIE is then forwarded to the National Intelligence Board—a group chaired by the DNI and composed of senior IC officials—for its prompt approval. Finally, the NIE is disseminated as a classified document to policymakers under the signature of the DNI.4

The NIE arrived with infamy onto the national scene after an October 2002 Estimate, "Iraq's Continuing Programs for Weapons of Mass Destruction," concluded that Iraq had chemical and biological weapons and would have a nuclear weapon within eight years’ time. Charles Duelfer, director of the CIA's Iraq Survey Group, later acknowledged that in estimating Saddam Hussein's weapons of mass destruction (WMD) programs, "we were almost all wrong."5 According to the various bodies that investigated the October 2002 NIE, the ninety-three page estimate of Iraq’s WMD capabilities suffered from an assortment of intelligence tradecraft errors. The Senate Select Committee on Intelligence found it was compiled hurriedly and approved in twenty days, whereas the IC ideally prefers three months. The CIA's after-action assessment noted that "[the NIE] was the product of three separate drafters, each responsible for independent sections, drawing from a mixed bag of analytic product." The Commission on the Intelligence Capabilities of the United States regarding Weapons of Mass Destruction listed as "a central flaw of the NIE" that it took "defensible assumptions (of Saddam Hussein's prior behavior) and swathed them in the mystique of intelligence, providing secret information that seemed to support them but was in fact nearly worthless, if not misleading."6 A key difference between this flawed NIE and those presented below is that the Iraq Estimate was an action-forcing document written to influence a congressional vote to approve the Iraq war, while most NIEs are stand-alone products that inform the ongoing process of national security policy making.

1950S AND 1960S: THE CLANDESTINE PROBLEM

The United States lost its short-lived nuclear monopoly when, on August 29, 1949, the Soviet Union conducted its first successful atomic test at Semipalatinsk, Kazakhstan.7 In its first NIE after the Soviet test, the CIA warned that "the continental U.S. will be for the first time liable to devastating attack."8 Before the advent of the first Soviet intercontinental ballistic missiles (ICBMs) in 1957 and nuclear-armed submarines in 1960, bombers were judged to be Moscow’s most likely means of nuclear attack on the United States. Nevertheless, a November 1950 NIE warned that "the Soviet Union has the capability for clandestine atomic explosions in ports and in selected inland areas."9

In 1951, the CIA updated that estimate and produced its first complete analysis of the issue
with an NIE titled “Soviet Capabilities for Clandestine Attack against the U.S. with Weapons of Mass Destruction and the Vulnerability of the U.S. to Such Attack.” This fascinating document demonstrates that, within two years of Soviet acquisition, the CIA had mapped out many of the pathways that a state—or nonstate—actor could use to discretely deliver a bomb into the United States to this day. This NIE found that the Soviet Union, from the least to greatest probability, could

- “Smuggle an atomic bomb through customs as a commercial shipment.”
- Conduct a “clandestine attack with civilian aircraft of a type used by U.S. or foreign transoceanic airlines.”
- “(Utilize) a merchant ship for delivering an atomic weapon into a key U.S. harbor.”
- “[Smuggle] ... an atomic bomb, especially if disassembled, from a Soviet port into an isolated section of the U.S.”

This final method was deemed the most likely means of a Soviet clandestine atomic attack on the United States. “The USSR,” the NIE concluded, “will have no scruples about employing any weapon or tactic which promises success in terms of over-all Soviet objectives.” Given this assessment, one would hope that the U.S. government would have been sufficiently alarmed to act on such an analysis. Unfortunately, the Estimate included a troubling assessment as relevant today as it was fifty-five years ago:

No coordinated over-all plan has yet been complete for the detection and prevention of the smuggling of atomic weapons into the U.S. at secluded points. Until such a plan is complete and put into effective operation, the U.S. will remain vulnerable to this threat.

Throughout the 1950s, the CIA periodically updated its estimate of the clandestine threat to reflect how such an attack corresponded with the Soviet Union’s growing strategic capabilities for striking the United States. One such NIE, written in 1955, explores the possibility of “Clandestine Introduction of Nuclear Weapons under Diplomatic Immunity.” This Estimate noted that weapons ranging “from one kiloton to one megaton in yield . . . could be designed to break down into components weighing from a few pounds up to 25 pounds in the case of small-yield weapons and up to approximately 200 pounds in the case of large yield weapons.” By using the shield of diplomatic immunity, it was envisioned that Moscow could place nuclear weapons at Soviet diplomatic establishments, such as at its Washington embassy, or in its United Nations delegation offices in New York City. According to the Estimate, “In this way [the Soviet Union] could virtually ensure successful attack on two major targets without using a large number of personnel and without incurring the risks involved in transporting nuclear weapons to areas which do not enjoy diplomatic immunity.” The NIE ultimately estimated that “the chances are now slightly better than even that the USSR would not undertake” an attack using diplomatic immunity. In an interesting dissenting footnote, the assistant director of the FBI contended—and the director of naval intelligence concurred—that “it is impossible to predict whether the USSR would or would not attempt to utilize the diplomatic pouch to clandestinely introduce nuclear weapons into the U.S.” Given that, to this day, there are no limitations to the size of a diplomatic pouch, there was no technical constraint precluding the FBI’s concerns.

The Cuban Missile Crisis in 1962 rekindled interest in protecting the United States from a clandestine nuclear attack. In the collective cold war memory, the crisis is remembered as an “eye-ball to eyeball” confrontation between Khrushchev and Kennedy in which the Soviets blinked first. This triumphalist attitude, however, should have been tempered by the fact that, despite persistent intelligence collection on Cuba and Soviet freight shipping to the island, Moscow succeeded in covertly dispatching approximately 130 nuclear warheads—with an explosive power of more than fifty megatons—ninety miles from the U.S. coastline. An NIE approved six months prior to the Soviet shipment concluded erroneously that it was “unlikely that the [Soviet] Bloc will provide Cuba with strategic weapon systems.” After Moscow and Washington negotiated an end to the crisis, 98 tactical nuclear warheads remained in Cuba, unbeknownst to the United States. Fidel Castro requested that the warheads stay on the island to deter an American invasion, but Moscow refused, and on Christmas Day, the remaining Soviet nuclear arsenal was removed from Cuba.

After the Cuban Missile Crisis, President John F. Kennedy became concerned that nuclear
weapons or other WMD could be smuggled into the United States. The CIA thus reexamined the threat of clandestine nuclear attacks, and a March 1963 NIE reconfirmed that such an attempt would be easy. “Nuclear weapons yielding up to 300 [kilotons],” the NIE stated, “could be brought into the United States by a variety of means such as by ground or air transport across land borders or at points along U.S. seacoasts.”

Even in the ballistic missile age, clandestine attacks retained the comparative advantage of “extreme accuracy or the desire to deny warning time.” But, given the “growing number and dispersal of U.S. delivery vehicles,” and subsequent “limited advantages of this course of action,” it was ultimately deemed unlikely that the Soviets would introduce nuclear weapons clandestinely. In January 1968, the Joint Chiefs of Staff requested that the 1963 NIE be updated to reflect the proliferation of nuclear weapons capabilities, and more specifically the threat from China, which tested its first bomb in October 1964.

From its allies, this NIE confidently concluded that “we can foresee no changes in the world situation so radical as to motivate the UK, France, or any of the other potential nuclear powers to attempt to clandestinely introduce nuclear weapons into the U.S.” From China, however, the Estimate noted that, “because the Chinese have no other means of attacking the U.S. with nuclear weapons, they might consider a clandestine emplacement effort with the object of deterring the U.S. from launch a devastating nuclear attack on China.” Beijing was believed to have faced greater difficulties in smuggling a bomb than Moscow. First, “Chinese weapons are probably fairly large and would probably require more detailed assembly and check out after being brought in than would Soviet designs”; and second, “there are no Chinese Communist diplomatic establishments in the U.S. Canada, or Mexico. The absence of such bases precludes the use of diplomatic pouches for the clandestine introduction of nuclear weapons or their components.” Although Beijing could have overcome these disadvantages, it was deemed unlikely they would do so because a detonated smuggled bomb would not deter the U.S. from launching a devastating nuclear attack on China.

These early NIEs make clear that a clandestine nuclear attack from Russia or China was alarmingly achievable and a constant possibility. The CIA, however, never considered such an attack by either country to be likely, and to date no available evidence shows that Moscow or Beijing ever considered such an attack during the cold war. The NIEs envisioned that a smuggled bomb would be detonated only after either state decided to commence a general war with the United States and only as a subsidiary component of an all-out attack. None of the declassified NIEs ever concluded that an all-out war with China or the Soviet Union was likely in the foreseeable future during the time period in which they were published.

Interestingly, although the CIA quickly dismissed the clandestine threat from Great Britain or France, no NIEs mention how—or even if—the U.S. government could attribute the source of the fissile material used in a bomb through forensic attribution if no state claimed responsibility. A 1970 NIE even found it “conceivable that the Chinese Communists might seek to introduce into the U.S. a nuclear device with the intention of detonating it under certain circumstances... in hope that it would lead U.S. authorities to conclude that the action had been perpetrated by the Soviets” or, alternatively, “introduce into the U.S. a nuclear device so constructed as to appear to be of Soviet origin, and intended not to be detonated but to be discovered by U.S. authorities.”

**Modern Terrorism**

International terrorism was only a distant concern to the U.S. national security community prior to the late 1960s. Reflecting on his time in the Pentagon, former secretary of defense Robert McNamara later noted, “I don’t think we used the term terrorist.” Influenced by the tactics of the Vietcong in the Vietnam War, government documents termed acts of terrorism as conducted by “insurgents,” “guerrillas,” “extremists,” or “dissident groups.” In March 1967, the JASONs—a group of some forty scientists who conducted secret research projects for the Pentagon—studied the likely consequences of the American use of tactical nuclear weapons (TNWs) in Vietnam. Under the leadership of physicist Freeman Dyson, the JASON study found that the U.S. military would see few battlefield advantages from using TNWs because the Vietcong moved in small groups under the cover of the jungle and could quickly rebuild
diagnosed transportation routes. Crossing the nuclear threshold in Southeast Asia, however, could lead the Soviets or Chinese to provide the Vietcong TNWs—in the form of atomic demolition devices, nuclear mortars, or recoilless rifles—which would have had devastating effects on the Saigon airport, densely populated U.S. bases, and Army and Air Force logistics facilities. Furthermore, if the Vietcong attacks succeeded, “insurgent groups everywhere in the world would take note and would try by all available means to acquire TNWs by themselves. . . . It is therefore of tremendous long-range importance to avoid setting a precedent for the use of TNW by guerrilla forces.”26

International terrorism in its modern connotation exploded onto the world stage when the Palestinian Liberation Organization conducted a series of airline hijackings, embassy attacks, and the massacre of eleven Israeli athletes at the 1972 Munich Olympics. In the wake of Munich, the CIA’s Directorate of Intelligence created its first analytical team to systematically collect data on significant terrorist events and terror groups, and published the results in Weekly Situation Reports.27 It was not until April 1976 that the CIA produced its first comprehensive analysis of international terrorism, “International and Transnational Terrorism: Diagnosis and Prognosis.”28 The study concluded that “there has been a marked and enduring upsurge in transnational terrorism since 1967.” The emergent phenomenon was characterized by five factors: (1) “a substantial increase in the number of terrorist groups;” (2) “a trend toward greater international contact and cooperation among terrorist groups;” (3) “a trend toward bolder and more dramatic actions;” (4) “the general popularity of American targets;” and (5) “significant regional differences in the intensity and nature of such violence.” Exacerbating these factors was “the diffusion of terrorist-adaptable technological know-how,” which led the CIA to estimate that

the prospect of nuclear-armed terrorists can, in fact, no longer be dismissed. But because of the major problems that would be involved in the acquisition, storage, transport, and employment of a nuclear device, a more likely scenario—at least in the short term—would be a terrorist seizure of a nuclear weapons storage facility or a nuclear power plant to exploit the publicity and the bargaining power in the attendant threat of radiological pollution.29

Since the late 1960s, officials in the Atomic Energy Commission (AEC) had been scrutinizing the relative insecurity of nuclear reactor facilities in the United States. In 1965, six bombs’ worth of highly enriched uranium (HEU) from the Nuclear Materials and Equipment Corporation in Apollo, Pennsylvania, were found to have gone missing.30 In 1966, twenty low-enriched uranium (LEU) fuel canisters were stolen—and later recovered—from the Bradwell Nuclear Power Station in Essex, England.31 Spurred by these incidences of nuclear loss or theft, the AEC directed seven outside nuclear industry experts, lawyers, and accountants to study the issue of U.S. nuclear safeguards. In March 1967, the panel recommended that the AEC require nuclear power operators to improve and upgrade existing safeguards—specifically, physical protection, accounting, and oversight—to prevent the diversion of nuclear material.32 The panel also warned, for the first time in a U.S. government publication, that “safeguards programs should also be designed in recognition of the problem of the terrorist or criminal groups clandestinely acquiring nuclear weapons or materials useful therein.”33

Though the AEC succeeded in implementing some of the panel’s recommendations, a “perfect storm”—a combination of more lethal terrorist attacks, nuclear terror hoaxes, and a constellation of dedicated physicists and academics warning about the relative ease of stealing fissile material and making a crude nuclear device—led the U.S. government to further study the issue.34 In 1974, the AEC directed five independent experts to evaluate the safeguards in place in America’s civilian nuclear facilities.35 Led by technology consultant David Rosenbaum, the Special Safeguards Study warned that the U.S. system was “entirely out of proportion to the danger to the public” because of the contemporary nature of terrorism:

Terrorists groups have increased their professional skills, intelligence networks, finances, and levels of armaments throughout the world. International terrorist organizations, particularly those of the Arabs, probably have the ability to infiltrate highly trained teams of 10 to 15 men into this country without detection. . . . Because of the widespread dissemination of instructions for processing special nuclear materials and for making simple nuclear weapons, acquisition of special nuclear material remains the only substantial problem facing groups which desire to have such weapons.”36
Senator Abraham Ribicoff, causing an uproar over the issue, leaked a draft copy of the *Special Safeguards Study* to the press. According to the AEC, “due to the amount of public attention being given to the safeguards area and the resulting flood of information in the media, and the increase of terrorism,” the federal agency subsequently revised its rules, adopting most of the recommendations that emanated from the *Study*.37

During the 1970s, the U.S. government also became worried about the security of its nuclear weapons arsenal, which was deployed in twenty-seven countries and territories during the cold war.38 Spurred by the gang-bombing of the Fifth Army Corps Headquarters in Frankfurt, Germany, in 1972, and the assassination of the CIA station chief in Athens, Greece, in 1975, concern arose about the potential nuclear terror threat from Western European terrorist groups.39

In 1978, a leaked CIA estimate identified the more than six thousand warheads stored in NATO nuclear depots in Western Europe as “the most vulnerable and therefore most likely targets for future terrorist activity.”40 One year earlier, the Pentagon’s Studies, Analysis and Gaming Agency conducted a week-long hypothetical exercise with thirty-five members of the national security community to consider how they would react if terrorists obtained a bomb and used it to blackmail the United States.41 Although the exercise results were never declassified, participants reported that the seized weapon ended up in the hands of an unpredictable third-world leader.42


If a terrorist group does acquire nuclear explosives, it can rely upon unconventional delivery methods which would be inappropriate for any but the most desperate or irrational state. Any form of transport—airplane, boat, truck, or train—could conceivably be employed. Unlike a state, terrorists with a mobile base of operations need not be concerned with the threat of counter-attack, hence they are not subject to the deterrence of defense systems that constrains states.43

On a positive note, the study observed that there were “sufficient systemic constraints against nuclearly-armed [sic] terrorists that non-state actors seem more likely to be an aberration than a characteristic of nuclear proliferation.” Among these constraints: a nuclear terrorist group would have to be “well-established and well-financed,” the bomb might be too large for nonmissile or nonplane delivery, and the group would be “the most sensitive to adverse public reactions.”44

**LOOSE NUKES AND THE JIHADIST TERROR THREAT**

When the Soviet Union disbanded on December 25, 1991, the IC was deeply troubled about the Red Army’s command and control of its nuclear arsenal.45 The Soviet arsenal, consisting of more than thirty thousand nuclear warheads, was dispersed throughout eleven time zones in Russia, in all fifteen former Soviet republics, as well as in East Germany, Hungary, Poland, Bulgaria, and Czechoslovakia.46 A June 1991 NIE, titled “Implications of Alternative Soviet Futures,” warned that the worst-case scenario would be a fragmentation of the Soviet Union in which Moscow lost any effective central control over its former republics. According to the NIE,

This scenario is potentially the most dangerous for the West because of the chaos and unpredictability of events. Although the USSR would disappear as a cohesive military power, the prospects of nuclear and other weapons of mass destruction falling into the hands of some republics, mutinous troops, or radical groups would pose a new set of risks. . . . There would also be a greater chance for nuclear materials and expertise finding their way to foreign states seeking to develop nuclear weapons.47

Another NIE on the topic, written three months later, warned of the potential threats from fragmentation in more stark terms: “The disappearance of reliable central control over nuclear weapons in some republics, as well as uncertainty over their disposition, would increase the prospect of nuclear weapons falling into terrorist hands.”48

As far as is known, the dissolution of the Soviet Union did not lead to the worst-case scenario—loose nukes in the hands of terrorists. But the loss
of a nuclear warhead or fissile material from the 221 nuclear facilities in the former Soviet Union remained, in the words of FBI Director Louis Freeh, “the greatest long-term threat to the security of the United States.”49 In late 1994, the DCI’s Joint Atomic Energy Intelligence Committee (JAEIC, pronounced “Jake”)—an interagency group that meets bimonthly to discuss items related to nuclear intelligence—conducted a comprehensive examination that came to the chilling conclusion that “none of these facilities in Russia or other newly independent states had adequate safeguards or security measures by international standards for weapons-useable materials.”50 Although there are no known instances in which nuclear material leaked from Russia into terrorist hands, the CIA’s National Intelligence Council later concluded that “weapons-grade and weapons-usable nuclear materials have been stolen from some Russian institutes. We assess that undetected smuggling has occurred.” Although the report goes on to say that “we do not know the extent or magnitude of such thefts,” it then lists four specific instances of smuggling between 1992 and 1999.51

Despite the U.S. Cooperative Threat Reduction program, which has advanced the goal of dismantling and securing the former Soviet nuclear arsenal since 1991, a September 1996 leaked CIA report demonstrated how persistent and challenging the problem of protecting Russia’s nuclear weapons remained. The top secret report, “Prospects for Unsanctioned Use of Russian Nuclear Weapons,” warned that “the Russian nuclear command and control system is being subjected to stresses it was not designed to withstand as a result of wrenching social change, economic hardship, and malaise within the armed forces.” The report further noted that Russia’s twenty-thousand-plus tactical nuclear weapons “appear to be the weapons most at risk”—a daunting assertion considering that some of these could have been carried by one person, weighing as little as sixty-five pounds.52 Finally, the report shattered the false sense of security that Russia’s weapons would ultimately be protected from unauthorized use by permissive action links, stating that “all technical [security] measures can be circumvented—probably within weeks or days depending on the weapons involved.”53

Along with the threat of loose nuclear material, the decline of the Soviet Union assisted in creating the second significant modern nuclear terror threat. In February 1989, Moscow withdrew the last Red Army soldiers from Afghanistan, in effect conceding victory to the Islamic mujahideen. The Arab and Afghan jihadi.s, under the leadership of Osama Bin Laden and others, renamed their successful resistance organization al-Qaeda. As early as 1993, U.S. intelligence officials learned of Bin Laden’s efforts to acquire nuclear materials or warheads from former Soviet republics.54 These attempts failed as al-Qaeda brokers were conned into buying low-grade reactor fuel and radioactive waste.55 In 1993, Jamal al-Fadl, a senior al-Qaeda operative, purchased a three-foot cylinder of weapons-grade uranium for $1.5 million from a former Sudanese military officer.56 According to Michael Scheuer, former chief of the Bin Laden Unit in the CIA’s Counterterrorism Center (CTC), by mid-to late 1996, the “Bin Laden unit acquired detailed information about the careful, professional manner in which al-Qaeda was seeking to acquire nuclear weapons . . . there could be no doubt after this date that al-Qaeda was in deadly earnest in seeking nuclear weapons.”57

In 1993, the Pentagon’s Office on Special Operations and Low Intensity Conflict convened a panel of forty-one retired intelligence analysts and counterterrorist experts to brainstorm about the evolution of international terrorism. Their still-classified report, Terror 2000: The Future Face of Terrorism, was a departure from other government-sponsored studies that catalogued the post–cold war terrorist groups and warned of their capabilities and intentions. The Terror 2000 report predicted that terrorists would use chemical or biological agents on a major subway system; conduct multiple, simultaneous attacks to strain government response capabilities; strike a major financial center in the United States; and hijack civilian airliners to strike American landmarks. The report noted that “horrified civilians will get to watch every step in a terrorist plot. CNN and other networks will certainly air the footage.”58 This prescient report also concluded that easy access to biological, chemical and nuclear technologies will bring many new players to the game of mass destruction. They may not even be limited to states and traditional terrorist groups. Organized crime, fanatical single-issue groups and even individuals all will be able to acquire weapons once limited to regional and world powers . . . [A WMD attack on the U.S.] is
increasingly probable, perhaps within the next five years.59

The Terror 2000 report was reprinted and circulated within the Pentagon, Justice Department, and Federal Emergency Management Agency. A sanitized version was also prepared in book form for public consumption. The federal government, however, never released the report in declassified form because of concerns that it would inspire terrorists, that the scenarios were too far-fetched, and, in the words of report’s manager, that it was “a little too scary for the times.”60

September 11, 2001, demonstrated that the United States was both a host to, and victim of, attacks that former DCI George Tenet aptly described as “professionally conceived and executed.”61 Two facets of 9/11 caused the IC to reevaluate the threat of nuclear terrorism. First, the use of conventional means—civilian airliners—led the December 2001 NIE to conclude that “the Intelligence Community judges that U.S. territory is more likely to be attacked with WMD using non-missile means—most likely from terrorists—than by missiles, primarily because non-missile delivery means are less costly, easier to acquire, and more reliable and accurate.”62 It had been the opinion of the IC for decades that the political prestige and deterrence strength of missiles made them the weapon of choice for WMD attacks on the United States.63

Second, the avalanche of media and government investigations into 9/11, and documents recovered from al-Qaeda safe houses in Afghanistan, revealed that Osama bin Laden meant it when he declared in 1998 that obtaining a weapon of mass destruction was “a religious duty.” A biannual CIA report to Congress on the “Acquisition of Technology Relating to Weapons of Mass Destruction and Advanced Conventional Munitions” said of the documents, “We have uncovered rudimentary diagrams of nuclear weapons inside a suspected al-Qa’ida safehouse in Kabul. These diagrams, while crude, describe essential components—uranium and high explosives—common to nuclear weapons.”64 The fall of the Taliban also revealed that Bin Laden had met with scientists from the Pakistani nuclear weapons program on several occasions before 9/11, leading the CIA’s Weapons Intelligence, Nonproliferation, and Arms Control unit to determine that al-Qaeda “probably had access to nuclear expertise and facilities and that there was a real possibility of the group developing a crude nuclear device.”65

The Commission on the Intelligence Capabilities of the United States regarding Weapons of Mass Destruction later revealed that “[intelligence] analysts were largely unaware of the extent of al-Qa’ida’s weapons of mass destruction research and development.”66

In the past few years, the IC has focused on the threat of nuclear terrorism to an unprecedented extent. The NIC’s 2020 Project report, Mapping the Global Future, aptly summarizes the IC’s current consensus opinion on the subject:

With advances in the design of simplified nuclear weapons, terrorists will continue to seek to acquire fissile material in order to construct a nuclear weapon. Concurrently, they can be expected to continue to purchase or steal a weapon, particularly in Russia or Pakistan. Given the possibility that terrorists could acquire nuclear weapons, the use of such weapons by extremists before 2020 cannot be ruled out.67

CONCLUSION

American intelligence estimates about the development of nuclear weapons by other states and their intentions for their use have been a mixed bag of quiet successes and notable failures. Knowing the capabilities and intentions of nonstate groups interested in obtaining nuclear weapons is undoubtedly a much more difficult proposition. Nevertheless, in reviewing the history of known intelligence estimates of the threat of nuclear terrorism, several important themes emerge: the proliferation of interest among nonstate actors in obtaining a bomb, the acknowledged ease with which terrorists could assemble a crude nuclear device, the ease with which any malicious actor could smuggle it into the United States, and the continued surprise of the U.S. government that this threat has persisted over a half century. The intelligence estimates presented above demonstrate beyond any doubt that the United States has been sufficiently warned about the very real possibility of a nuclear terror attack. If a terrorists’ bomb were detonated on American soil tomorrow, given the sustained strategic warning that the IC has provided to policy makers, it would be a “bolt from the blue” only to the indifferent, but not the unaware.
NOTES

1. Scholars interested in further studying National Intelligence Estimates (NIEs) can visit the CIA’s “Electronic Reading Room” Web site: http://www.foia.cia.gov/nic_collection.asp. There are more than one thousand declassified NIEs posted, searchable by title, geographic area, and function.
4. Ibid.
5. Testimony before the Senate Armed Services Committee, October 6, 2004.
7. Highlighting the inherent difficulty of uncovering the nuclear intentions and capabilities of other states, three weeks after the first Soviet test, on September 20, 1949, the CIA issued Intelligence Memorandum no. 225, “Estimate of Status of Atomic Warfare in the USSR,” which stated, “The current estimate of the Joint Nuclear Energy Intelligence Committee is that the earliest possible date by which the USSR might be expected to produce an atomic bomb is mid-1950 and that the most probable date is mid-1953.”
12. Ibid., 2.
13. Customs agents were reportedly trained to search the luggage of some Soviet citizens traveling to the United States, but this would not have included diplomatic pouches. See “Customs Hunting Atom Smugglers,” New York Times, February 16, 1954, p. 2.
14. The quote is attributed to the secretary of state, Dean Rusk, who stated, “We are eyeball to eyeball, and I think the other fellow just blinked.” McGeorge Bundy, Danger and Survival: Choices about the Bomb in the First Fifty Years (New York: Random House, 1988), 405.
27. These reports were not actually published weekly. See Naftali, Blind Spot, 55.
29. Ibid., 4–5.
32. Walker, Containing the Atom, 229.
37. Walker, “Regulating against Nuclear Terrorism,” 120.
42. Ibid., 10.
44. Ibid., 30–31.
55. Ibid., 32.
63. One month after 9/11, a CIA agent, code-named DRAGONFIRE, reported that terrorists had obtained a ten-kiloton nuclear weapon from Russia and planned to smuggle it into New York City. After weeks of investigating, intelligence officials determined DRAGONFIRE’s information was false. See Massimo Calabresi and Romesh Ratnesar, “Can We Stop the Next Attack?” Time, March 11, 2002, p. 24.
64. CIA, Unclassified Report to Congress on the Acquisition of Technology Relating to Weapons of Mass Destruction and Advanced Conventional Munitions, 1

65. The WINPAC report was produced on November 23, 2001. As quoted in WMD Commission, pp. 271, 277, fn. 66.
