Counterterrorism

Terrorism is as old as history, but the twenty-first century has brought a new form of terrorism. Terrorists now have access to technical skills that multiply their ability to wreak havoc far beyond the efforts of those in the past. However, the democracies that are most vulnerable to terrorist attack also have much greater technical resources with which to make the terrorist's task more difficult and less damaging. To understand how technical knowledge might be used to counter terrorism, one must evaluate the nature of the threat, the vulnerability of targets in civil society, and the availability of technical solutions to reduce these vulnerabilities.

Despite their small numbers, terrorists possess some advantages. Their actions (particularly those of ideological terrorists) are unpredictable, they may have cells hiding in the society they plan to attack, and they have the initiative in choosing the target and deciding when to attack. As a result, those defending against terrorism must always be alert; the terrorists need be prepared only when they choose to strike. Finally, terrorists may enjoy the technical and financial support of a nation state.

However, modern industrial societies have available a range of options in combating terrorist threats. These include the application of new technologies that can make targets less vulnerable and thus less attractive. These technologies can also limit the damage that may result from an attack, increase the speed of recovery, and provide forensic tools to identify the perpetrators. This is the main focus of a study by the National Academies of Science and of Engineering and the Institute of Medicine, released June 25, 2002. This study found that science and technology can contribute substantially to making the nation safer but cannot assure that catastrophic attacks will not take place.

Terrorist targets and weapons. Terrorists may seek to kill large numbers of people, to destroy national symbols of capitalism or of democracy, or to cripple elements of the industrial infrastructure on which normal economic and social life depend. If terrorists can obtain weapons of mass destruction—nuclear, biological, and chemical weapons—they may be expected to use them. More probably, they may use elements of the very economy they seek to attack. They may use elements of the transportation system as a weapon, as they did in the September 11, 2001, attacks. A rental truck filled with commercial fertilizer (ammonium nitrate) and fuel oil was used to blow up the Murrah Building in Oklahoma City in 1995. Terrorists might cause the release of toxic chemicals (such as railroad tank cars full of chlorine destined for municipal water supplies). They might use computers to interfere with electronic messages used to control critical industrial processes or needed by first responders to communicate when the attack occurs. This list of targets and tools to attack them is very long.

The vulnerability of civil society arises from the very efficiency of its competitive economic system. The competitive drive for commercial efficiency creates linkages and vulnerabilities in critical infrastructure industries—energy, transportation, communications, food production and distribution, public health, and financial transactions. The concentration of food packaging in a few firms, and of power production in ever bigger plants, and the production of ever larger aircraft and ships create targets that terrorists can exploit. The economy is not designed with the threat of catastrophic terrorism in mind.

Technical activities. Examples will be discussed of how technical activities might reduce either the threat of terrorism or its consequences in the areas of nuclear and radiological threats, biological threats to people and their food supply, toxic chemicals, explosive and flammable materials, energy systems, communications and information systems, transportation and borders, and cities and fixed infrastructure.

Nuclear and radiological threats. If terrorists can acquire enough highly enriched uranium, they may be able to assemble a crude but effective nuclear weapon which could kill hundreds of thousands of people. Governments with stocks of highly enriched uranium can blend them with natural uranium, leaving the material useful for power generation but not for bombs. Even more dangerous is the possible availability to terrorists of finished nuclear weapons provided by states with nuclear weapons capability. Clearly, it is extremely important to detect fissile materials entering the United States from foreign sources. The radioactivity of plutonium might be sensed, but highly enriched uranium can easily be shielded with moderate amounts of lead. Scientists are exploring the use of beams of neutrons that can penetrate steel containers and produce telltale signals from any uranium inside. Another alternative is the use of gamma rays to detect any very heavy element, including all the fissile elements.

Biological threats. Research might enable the detection of a bioterrorist attack before symptoms appear in infected people. This would also be a huge step forward in public health protection against natural agents such as SARS. Since terrorists might acquire the skill to modify deadly diseases genetically to make them resistant to known treatments and vaccines, a vigorous research effort to detect and respond is needed. Even more important is new means for detecting toxic materials or pathogens that might be inserted into the nation's food supply. While quick diagnosis and isolation of patients, as was done to quench the SARS epidemic, is the best defense today, biologists are working on networks of sensors, based on genomics and proteomics (study of the entire DNA sequences and of the entire range of proteins produced by pathogenic organisms) to detect pathogens that might be released in the air before they have time to make people ill. Since it takes years to develop vaccines for new diseases, biologists are also exploring new ways to create broad-spectrum antibiotics and antivirals for defense against a biological attack.

Toxic chemicals and dangerous materials. Dangerous chemicals in transit, such as tank cars filled with chlorine for protection of water supplies, could be blown up by terrorists with catastrophic results. These rail cars could be tracked by transponders that would report their positions using signals from the Global Positioning System and would be identified to responding fire fighters using encrypted radio messages only they can read. Sensor networks established in transportation nodes might allow attacks to be prevented, and sensors in crowded places, such as subways, theaters, and athletic facilities, could provide instant warning of dangerous chemicals that might be released there. Self-analyzing filter systems for ventilating modern office buildings might not only protect the inhabitants but detect and report the presence of dangerous materials that may be trapped in the filters. Basic research might lead to discovery of biosensors that could duplicate the ability of dogs, whose sense of smell exceeds that of humans by about 10,000 times, to smell minute traces of explosives, and perhaps toxic chemicals as well. *See* NETWORKED MICROCONTROLLERS.

Energy systems. The hazards associated with fossil fuel storage and shipment are well known. Perhaps less apparent are the vulnerabilities of a modern electric power grid. Critical points of vulnerability are the extremely high voltage, one-of-a-kind transformers that form the heart of a power distribution facility. They are hugely expensive, are imported, and have no backup. Engineers need to design reconfigurable midsized transformers, stored in a safe place off site, that could be assembled in configurations that would mimic one of these very high voltage transformers. *See* ELECTRIC POWER SUBSTATION DESIGN.

The computers that control power distribution control rooms are sensitive to cyber attack. Research to develop rigorously secure computer systems with encrypted communications might prevent attacks on these system control and data acquisition (SCADA) computers, which form the brains of the distribution system. From the perspective of a longer time frame, adaptive power grids should be developed which can automatically detect a loss of part of the system and restructure it before irreparable damage is done to the entire network.

Communications and information systems. In the United States, the most urgent issue is to provide secure communications to police, fire, and medical personnel so that they can communicate with one another and with emergency operations centers. Failure of fire fighters to hear the warnings of police to evacuate the towers greatly aggravated loss of life in the World Trade Center attack. Research is needed not only to ensure interoperability among a broad range of diverse responders to emergency but to manage priority access to the network and ensure its security against denial of service. But the main worry about cyber attacks is how to prevent terrorists from using a cyber attack to amplify the destructive effect of a conventional physical or biological attack. Greatly increased technical protection of computer communications is an urgent but difficult technical challenge. No computer operating system today is fully secure against an expert penetration effort. While the Internet and many telecommunications systems are soft targets against a cyber attack, they can be brought back into service in a matter of hours or days. But research is needed to reduce this recovery time dramatically so that information services can be available to emergency officials during an attack. *See* TELECOMMUNICATION NETWORK SECURITY.

Transportation and borders. Sensor networks for inspection of goods and passengers crossing the nation's borders will be a research priority. Off-line sensors are already used in airports to inspect trace chemicals that might indicate the presence of explosives. What is needed is a detector network that allows detection when persons or packages pass nearby. The primary technical challenge will be melding sensor networks together with data fusion and decision support software, so that false positive signals and failures to detect can be identified and unambiguous advice given to security officials for action. Biometric technology, such as devices that scan the unique patterns of each person's retina or iris, can provide more secure identification of individuals. The range of threats to the transportation networks of a modern state is very great, and careful systems analysis to identify the weak points and find the most effective and economical means for protecting them is essential.

Cities and fixed infrastructure. Much research is underway to analyze the structural characteristics of high-rise buildings that make them much more vulnerable than necessary. Buildings like the Murrah Building in Oklahoma City depend on each pillar on the ground floor remaining intact. Modifications to buildings that allow adjacent pillars to share the load and prevent catastrophic collapse are being explored. Air intakes for large buildings need to be less accessible, and equipped with better air filters and toxic chemical detectors. Instrumentation to allow first responders to detect toxic chemicals and hazardous materials, and robots to go where humans cannot, are also needed. Special provisions for protecting harbors, bridges, dams, tunnels, dikes, and urban water supplies are urgent.

Public response to terrorist threats. Public panic as a result of lack of credible public information is a serious threat, especially in the event of a radiological weapon ("dirty bomb") or bioterrorist attack. Loss of public confidence in those responsible for protecting the public can make a bad attack much more destructive. Government officials must introduce to the public well in advance of any attack a number of trusted and technically knowledgeable experts able to provide accurate and trustworthy information quickly and authoritatively.

Systems issues. Reducing vulnerabilities in critical infrastructure is possible but is a highly complex systems problem, requiring a tested strategy. A unique degree of cooperation between industry, cities, and federal government is required. Policies

for understanding who will pay to harden the critical infrastructure industry are needed. Investments to make the country harder to attack will be much cheaper and easier to sustain if technical strategies are of dual benefit, to the counterterrorism effort and to the civil economy. There are many examples of this possibility, from improved public health services to safer, more reliable transportation and reduced vulnerability to natural disasters.

For background information *see* ACTIVATION ANALYSIS; COMPUTER SECURITY; ELECTRIC POWER SYSTEMS; GENETIC MAPPING; MEDICAL BACTERIOLOGY; POISON; STRUCTURAL DESIGN; TOXICOLOGY; TOXIN in the McGraw-Hill Encyclopedia of Science & Technology.

Lewis M. Branscomb

Bibliography. G. Bugliarello (ed.), *Urban Security: Engineering the Protection of Our Cities*, vol. 1, Polytechnic University, Brooklyn, 2003; Committee on Microbial Threats to Health in the 21st Century, Institute of Medicine, *Microbial Threats to Health: Emergence, Detection, and Response*, National Academies Press, Washington, DC, 2003; Committee on Science and Technology for Countering Terrorism, National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, National Academy Press, Washington, DC, 2002; Computer Science and Telecommunications Board, *Information Technology for Counterterrorism: Immediate Actions and Future Possibilities*, National Academies Press, Washington, DC, 2003; U.S. Commission on National Security—21st Century (Hart-Rudman Commission, Phase III), *Roadmap for National Security: Imperative for Change*, February 15, 2001.