TECHNOLOGY FOR PREVENTING TERRORISM

Introduction

Abraham D. Sofaer
Hoover Institution, Stanford University

The threat of terrorist attacks poses many challenges, but none as urgent and essential as prevention. The Hoover Institution is devoting its third National Security Forum to this subject. The Conference will examine, specifically, the role that technology might play in preventing terrorist acts. Panels have been formed to discuss several scientific, organizational, and legal topics central to a proper understanding of the potential contributions of technology, as well as the practical and legal difficulties in exploiting those opportunities.

To enhance consideration of the issues, background papers have been prepared on aspects of the subjects to be considered at the Conference. The papers are collected here, for the benefit of Conference participants; they will eventually serve, along with other papers and research, as the basis for a published report. The subjects covered are (1) sensors; (2) identification technologies; (3) data collection and analysis; (4) acquisition and enhancement of technological innovation; and (5) legal and ethical constraints.

The potential contribution of technology in preventing terrorism can only be judged with reference to the threats to which Americans are exposed. The threats include all sorts of violent acts ranging from murder to a missile attack

utilizing a nuclear warhead. The Conference will focus on those threats considered most likely to occur, and most likely to cause substantial human and economic damage. These include primarily the use of explosives, chemicals, and biological weapons, against important national infrastructure, military and diplomatic assets, or targets exposing large numbers of people. Threats can come from States directly, as well as from terrorist groups. The Conference will consider terrorist threats, irrespective of the extent to which they are initiated or supported by States.

Scope of the Terrorist Threat.

The threat posed to societies from terrorism has two dimensions: the weapons that may be used, and the targets that may be attacked. The weapons considered at the Conference will include conventional explosives, nuclear devices ("dirty" or normal), chemical weapons, biological materials, and methods for attacking cyber systems (worms, viruses, etc.). Targets to be considered include all critical infrastructures (air, sea, and land transport; power; communications; mail and other commercial systems, etc.), military and diplomatic installations within the US and abroad; key services related to the nation's capacity to respond to acts of terror, such as hospitals; and targets selected for their potentially adverse impact on morale, such as sports stadiums, schools, concert halls, and movie theaters.

A. Weapons.

Guns and conventional explosives still remain the principal weapons used by terrorists. But creative use of conventional means can create massive damage, as the September 11 attacks demonstrated. Airplanes, filled with jet fuel, were used as bombs, causing the deaths of some 3000 people, and economic loss of what has been calculated to be $150 billion, including the permanent loss of some 40,000 jobs in New York City alone. Other, analogous types of conventional attacks remain possible, including the use of trucks carrying fuel or hazardous materials, or attacks on nuclear power plants and other installations that could spread damaging substances. The National Commission on Terrorism concluded in its report of June 2000 that, while the number of international terrorist incidents has declined since 1980, the number of persons killed or injured in such attacks had increased by then from some 5,000 to almost 20,000.[1]

Explosives and conventional weapons range in the danger they pose. The use of mines and shaped-charges, for example, has been very limited. Yet, these devices are relatively easy to deploy and very difficult to detect in public roads and other public areas. Terrorists have also rarely used small mortars and rockets. But they could prove extremely damaging, and very difficult to prevent. For example, a terrorist armed with a small ground to air rocket could stand outside

[1] "Countering the Changing Threat," p.5.

the perimeter of an airport and shoot down, with relative ease, a commercial jet during takeoff or landing, while it is flying low and slow. The mortars being used against Israelis by Palestinians are small, with portable launchers, but can travel up to eight miles. As these weapons become more accurate, and their payloads more lethal, they will pose important challenges.

In addition to conventional explosives and weapons, terrorists can resort to unconventional weapons based on chemicals, biological substances, and nuclear materials. Putting together and delivering a chemical, biological, or nuclear weapon is more complicated and difficult than using a conventional explosive or gun. The damage these weapons can potentially inflict is so great, however, and the terror they can spread so horrible, that -- as former Secretary of State George P. Shultz predicted at the 1998 Hoover Conference concerning these weapons -- "it is not a question of 'if' but of 'when"' they will be used. A very small amount of refined anthrax, included in a few letters sent after the September 11 bombings, killed several people, and disrupted the postal service and the functioning of significant parts of the US government. That single, limited attack is estimated to have caused some $1 billion in economic damage. While it is highly unlikely that terrorists will be able to develop sophisticated, unconventional weapons on their own, it is very likely based on experience and current intelligence that several states that possess the capacity to develop such weapons will be prepared to assist terrorist groups in obtaining and delivering them. Such weapons need not be

highly sophisticated, moreover. The possibility of a terrorist group utilizing a "dirty" nuclear device, consisting of some plutonium and/or other nuclear materials, together with conventional explosives, is far more likely than the use of a sophisticated nuclear device, but little less chilling to contemplate. A successful program to prevent terrorist attacks must be designed to deal with the full range of anticipated weaponry.

B. Targets.

The US is extremely vulnerable to terrorist attack. Government studies of the critical infrastructures of the nation, mandated by Executive Order 13010 or undertaken for other reasons, all demonstrate how difficult it is to prevent attacks that are likely to have substantial consequences. In a recent summary focusing on transportation, Commander Stephen E. Flynn of the US Coast Guard concluded: "Most of the physical plan, telecommunications, power, water supply, and transportation infrastructure on U.S. territory lies unprotected or is equipped with security sufficient to deter only amateur vandals, thieves, or hackers."[2] A few examples of the most important vulnerabilities should suffice to illustrate the scope of the problem.

Borders. Border security poses a staggering problem for the US. The overall picture is suggested by the numbers of people and things that enter the nation through inspection checkpoints, where data are collected. In the year 2000,

[2] "The Unguarded Homeland," in How Did This Happen, p.186.

these points recorded the passage of 488.2 million people, 125.2 million passenger vehicles, 11.6 million maritime containers, 11.5 million trucks, 2.2 million railcars, 829,000 planes, and 211,000 vessels.[3] The US has some 95,000 miles of shoreline. Many major ports exist all around these shores. A single port can pose serious security problems. Long Beach, California, for example, has facilities to off-load some 408,000 barrels of oil per day, roughly 25% of the oil consumed in the State. Oil refineries in California operate at full capacity, so an attack on a tanker in the harbor could severely harm the State's economy. Despite its importance, the port is protected entirely by the companies that lease space there.[4] No effort is made to require any special level of security, and measures are almost entirely geared to preventing theft and vandalism. The Coast Guard has statutory responsibility for providing seaport security, but local port authorities have been happy with the low level of Coast Guard involvement that is possible, "since more security is widely perceived as undermining efforts to improve port efficiency and competitiveness."[5]

The US has neither the personnel nor the technology needed to screen effectively even a minute proportion of the people, vehicles, and containers entering the country every day. Inspectors are able to devote roughly 2 minutes to huge tractor-trailers entering at busy bridges, and even less time to individual

---

[3] _____

[4] A similarly serious problem is posed by the 257 aboveground oil tanks at Port Everglades, which serve as the exclusive source of oil imports for that region.

[5] Flynn, 187

containers. The Customs Service still uses paper-based systems, and has only recently been authorized to adopt primitive data-management tools. To the extent data are collected about vessels, vehicles, people, or cargoes, moreover, methods have not been devised for the data to be provided in a timely manner to all interested agencies.

The consequences of terrorist attacks go far beyond the immediate damage they cause. The transport infrastructure was devastated after the September 11 attacks, because all airline traffic and international commerce was stopped for several hours. This may have been the right thing to do, but it was costly. The American economy depends heavily on air traffic as well as on the timely delivery of goods from international manufacturers and fabricators. The profits realizable from US retail sales of $3.2 trillion per year depends significantly on the ability of industry to hold inventories to a minimum, which requires reliable deliveries. When borders are closed, losses include the very efficiency that is the hallmark of the US industrial system.

The sheer size of the problem confronting US security has led to the view that mechanisms are needed that separate lawful people and activities from suspect ones. The post-September 11 approach, which relied on massive freezes of commercial activity, "overlooks the fact that the overwhelming majority of international carriers, cargo, and travelers are indeed legitimate and their freedom of movement should not and must not be unduly restricted." The solution is "to

focus on building a regime that can reliably identify the people, goods, and conveyances that are legitimate, so their movements can be facilitated. Then regulators and inspectors could focus their energies on the smaller number of participants attempting to enter their jurisdiction about which they know little or have specific concerns."[6]

The Human Factor. Another, general problem to consider in evaluating the potential of technology in preventing terrorist acts is the failure of governments and individuals to exploit the benefits of available measures. This propensity is strong and so prevalent in all its forms that it must be taken into account. In some situations, government policies deliberately restrict the potential of specific technologies. This is most clearly and seriously evident in the restriction of access to information possessed by particular agencies of government. At least five of the nineteen hijackers on September 11 were on lookout lists of specific agencies; but this information was not provided to the airport or airline screeners, and was not shared among the agencies interested in preventing terrorism. Some restrictions are statutory, others based on regulation and/or practice.

In some instances, Congress has simply failed to provide the funds necessary for agencies to perform work clearly necessary to enable them to prevent acts of terrorism. Recommendations made soon after the 1983 bombing

[6] Flynn p.195.

of the U.S. Embassy in Beirut, Lebanon for a program to strengthen security at embassies were not implemented by the time of the attacks on the U.S. Embassies in Kenya and Tanzania in 1998 because of drastic cuts in State Department appropriations. Repeated requests for funds to upgrade Immigration & Naturalization Service capacity to screen and track aliens have been denied; the General Accounting Office determined in October 2001 that the INS was hopelessly unable to perform its tasks, so essential to secure U.S. borders.

In other cases, agencies or officials fail to abide by standards or policies established on the basis of expertise and experience. The bombing of the Khobar Towers military barracks in Saudi Arabia caused massive damages and the loss of 19 lives, most or all of which would have been avoided if the facility had been set back farther from a public road. The U.S. Embassy in Nairobi, Kenya was not in compliance with the State Department's required 100-foot setback/standoff zone. Similar failures to comply with guidelines concerning the use of new technologies should also be anticipated.

In part, the problem of human error must be dealt with by implementing technologies so as to reduce to a minimum reliance on variable decision-making. Beyond this, anti-terrorism policy must ultimately be based on the realization that, as Secretary of Defense Donald Rumsfeld has stated:

> . . . [D]efending the U.S. requires prevention, self-defense and sometimes preemption. It is not possible to defend against every conceivable kind of attack in every conceivable location at every minute of the day or night.

Defending against terrorism and other emerging 21st century threats may well require that we take the war to the enemy. The best, and in some cases, the only defense, is a good offense.[7]

[7] See "Secretary Rumsfeld Speaks on '21st Century Transformation' of U.S. Armed Forces," (remarks delivered at the National Defense University, Fort McNair, Washington, DC on Jan. 31, 2002), available at <http://www.defenselink.mil/speeches/2002/s20020131-secdef.html>.