

## *Are We Ready for Terror?*

The Latest Hart-Rudman Report and What It Missed

America remains dangerously unprepared to prevent and respond to a catastrophic terrorist attack on U.S. soil.” That’s the verdict of a task force set up by the Council on Foreign Relations to study the country’s readiness for an attack involving weapons of mass destruction.

The task force was led by Gary Hart and Warren Rudman, the two former Senators who had previously worked together as co-chairmen of a commission on national security. In its final report—released a half-year before the September 11 attacks—that previous commission called for the creation of a homeland security agency. Now, more than a year after the attacks, the new Hart-Rudman task force has made a series of recommendations on how, among other things, to use technology to prepare for future acts of terrorism.

One of the most urgent recommendations in the task force’s report is to put new equipment in the hands of the emergency personnel who would be the first responders in case of a terrorist attack. In

addition to the protective gear normally used by firefighters, emergency personnel need specialized equipment to protect against chemical and biological attacks—as well as training in how to use and maintain the equipment. Only a fraction of the country’s 9 million first responders have had any hands-on training with live chemical agents and other weapons of mass destruction. Such training is essential if emergency personnel are to respond effectively to future attacks, especially in the critical early hours before better-trained and better-equipped federal personnel arrive on the scene.

The task force also made recommendations regarding the use of information and communication technologies. The report calls for a “twenty-four-hour operations center in each state” that would monitor federal and international databases to determine whether suspects held by police should be kept in custody. It recommends replacing the conventional radio equipment used by police and firefighters with new technolo-

---

gies “that can integrate multiple radio platforms to support interoperable communications, including the ability to coordinate the flow of voice, image, and electronic information among responding agencies.”

The country’s critical infrastructure is also badly protected, according to the task force. Many unmanned oil pumping stations have no intrusion-detection devices. There are few spare parts for key components of the power grid. The nation’s food and water supplies are vulnerable to attack, as are the few bridges and tunnels that act as major conduits of trade with Canada.

The Hart-Rudman task force also called for improvements to America’s public health system, though for the most part it didn’t make recommendations about the role of medical technology in responding to terror, choosing instead to recommend better training and greater readiness.

Indeed, this lack of detailed suggestions about improving medical technology is one of the Hart-Rudman report’s chief weaknesses. Shortly after the report was released, another panel studying the same subject—the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, better known as the Gilmore Commission—released its fourth annual report. That report pointedly recommends several technological steps that should be taken to shore up America’s public health system, including the development of “an electronic, continuously updated handbook” for response personnel; a “national strategy for vaccine development for bioterrorism”; an incremental smallpox vaccination plan (which President Bush has since initiated); and stronger programs focusing on “the application of new technologies or devices in public health.”

Another weakness of the Hart-Rudman

report is its failure to endorse new technologies for detecting dangerous contents in the cargo containers shipped into America’s seaports. The report acknowledges the woeful vulnerability of America’s insecure ports, and includes recommendations for improving the system for tracking and monitoring the thousands of containers shipped into the country every day.

But these recommendations don’t go far enough. It’s not sufficient simply to track containers; customs officials should be better equipped to make sure the containers aren’t used to sneak bombs or other dangerous materials into the country. As things stand now, the materials for building weapons of mass destruction could easily slip through America’s insecure ports undetected and be used to threaten major population centers. This is not just a hypothetical weakness: In a report that somehow failed to cause an uproar, ABC News last year shipped 15 pounds of depleted uranium into a New York port—where the Customs Service failed to detect the radioactive material and just admitted the container into the country. This appalling lapse—caused by a combination of insufficient technology and bureaucratic arthritis—should be a wake-up call.

This shortcoming in the Hart-Rudman report is made all the more perplexing by the fact that the task force wisely recommended the use of new high-tech sensors to address other kinds of threats. According to the report, the national research labs should “develop, field test, and widely distribute new portable and hand-held sensor equipment” for detecting “highly explosive, chemical, biological, and radiological materials” in urban areas. A parallel research program should be started to provide similar advanced detection equipment to the country’s ports.

---

Finally, the Hart-Rudman report recommends careful deliberation before adopting proposed high-tech remedies to bolster homeland security: “Technology can often serve as an enabler, but it must belong to a layered and dynamic system of defense that incorporates the contribution of human intuition and judgment. Any proposed technological ‘solution’ must be evaluated against the costs and consequences if it should be compromised.”

This is a reasonable approach, since many of the challenges to homeland security are not technological in nature, and some technological solutions can lull us into a false sense of security. As the report rightly puts it: “After a year without a new attack, there are already signs that Americans are lapsing back into complacency.” Unfortunately, complacency is a problem for which technology can offer no solution.