Foreign Affairs

November/December 1998, Volume 77, Number 6

CATASTROPHIC TERRORISM: Tackling the New Danger

By Ashton Carter, John Deutch, and Philip Zelikow

IMAGINING THE TRANSFORMING EVENT

Terrorism is not a new phenomenon. But today's terrorists, be they international cults like Aum Shinrikyo or individual nihilists like the Unabomber, act on a greater variety of motives than ever before. More ominously, terrorists may gain access to weapons of mass destruction, including nuclear devices, germ dispensers, poison gas weapons, and even computer viruses. Also new is the world's dependence on a nearly invisible and fragile network for distributing energy and information. Long part of the Hollywood and Tom Clancy repertory of nightmarish scenarios, catastrophic terrorism has moved from far-fetched horror to a contingency that could happen next month. Although the United States still takes conventional terrorism seriously, as demonstrated by the response to the attacks on its embassies in Kenya and Tanzania in August, it is not yet prepared for the new threat of catastrophic terrorism.

American military superiority on the conventional battlefield pushes its adversaries toward unconventional alternatives. The United States has already destroyed one facility in Sudan in its attempt to target chemical weapons. Russia, storehouse of tens of thousands of weapons and material to make tens of thousands more, may be descending into turmoil. Meanwhile, the combination of new technology and lethal force has made biological weapons at least as deadly as chemical and nuclear alternatives. Technology is more accessible, and society is more vulnerable. Elaborate international networks have developed among organized criminals, drug traffickers, arms dealers, and money launderers, creating an infrastructure for catastrophic terrorism around the world.

The bombings in East Africa killed hundreds. A successful attack with weapons of mass destruction could certainly take thousands, or tens of thousands, of lives. If the device that exploded in 1993 under the World Trade Center had been nuclear, or had effectively dispersed a deadly pathogen, the resulting horror and chaos would have exceeded our ability to describe it. Such an act of catastrophic terrorism would be a watershed event in American history. It could involve loss of life and property unprecedented in peacetime and undermine America's fundamental sense of security, as did the Soviet atomic bomb test in 1949. Like Pearl Harbor, this event would divide our past and future into a before and after. The United States might respond with draconian measures, scaling back civil liberties, allowing wider surveillance of citizens, detention of suspects, and use of deadly force. More violence could follow, either further terrorist attacks or U.S. counterattacks. Belatedly, Americans would judge their leaders negligent for not addressing terrorism more urgently.

The danger of weapons of mass destruction being used against America and its allies is greater now than at any time since the Cuban missile crisis of 1962. It is a national security problem that deserves the kind of attention the Defense Department devotes to threats of military nuclear attack or regional aggression. The first obstacle to imagination is resignation. The prospects may seem so dreadful that some officials despair of doing anything useful. Some are fatalistic, as if contemplating the possibility of a supernova. Many thinkers reacted the same way at the dawn of the nuclear age, expecting doom to strike at any hour and disavowing any further interest in deterrence as a hopeless venture. But as with nuclear deterrence, the good news is that more can be done.

ORGANIZING FOR SUCCESS

The threat of catastrophic terrorism spans the globe, defying ready classification as solely foreign or domestic. As the 1993 World Trade Center incident demonstrated, a terrorist group can include U.S. citizens and foreign nationals, operating and moving materials in and out of American territory over long periods of time. The greatest danger may arise if the threat falls into one of the crevasses in the government's overlapping jurisdictions, such as the divide between "foreign" and "domestic" terrorism or "law enforcement" versus "national security."

The law enforcement/national security divide is especially significant, carved deeply into the topography of American government. The national security paradigm fosters aggressive, active intelligence gathering. It anticipates the threat before it arises and plans preventive action against suspected targets. In contrast, the law enforcement paradigm fosters reactions to information provided voluntarily, uses ex post facto arrests and trials governed by rules of evidence, and protects the rights of citizens.

President Bill Clinton appointed a national coordinator for security, infrastructure protection, and counterterrorism in May 1998 to "bring the full force of all our resources to bear swiftly and effectively." There is no harm in the designation of a White House aide, but one should not place faith in czars. Real power still resides in the executive departments that have people, equipment, money, and the capacity to get things done.

Because most of the government functions addressing the danger of catastrophic terrorism apply to other purposes as well, the people making decisions about these capabilities against terrorists should be the same people who consider the other missions and can reconcile competing demands. The U.S. government must create unglamorous but effective systems for accountable decision-making that combine civil, military, and intelligence expertise throughout the chain of command; integrate planning and operational activity; build up institutional capacities; and highlight defensive needs before an incident happens. This strategy has four elements: intelligence and warning; prevention and deterrence; crisis and consequence management; and coordinated acquisition of equipment and technology.

INTELLIGENCE AND WARNING

The intelligence role in preventing catastrophic terrorism is complicated by nonstate actors, concealed weapons development, and unconventional deployments, all of which

are hard to monitor and preempt. In cyberattacks, for example, the deployment of weapons can be entirely electronic. The U.S. government should therefore have the authority to monitor any group and its potential state sponsors that might have the motive and the means to use weapons of mass destruction. In order to detect such weapons anywhere in the world, the United States should utilize remote sensing technology and cultivate global sources of information. Necessary measures include clandestine collection of open sources, such as foreign newspapers and the Internet, as well as a full exchange of information with key allies.

Nearly a year before its attack on the Tokyo subway system the Aum Shinrikyo group had used the nerve gas Sarin in assaults on civilians. Although the Japanese media had reported the news, the U.S. government remained in the dark. Not only did Washington not hear what Japanese law enforcement agencies knew, but the Japanese agencies themselves were not aware of what other local organizations in Japan had uncovered. The parties involved did not share the expertise to prevent another attack. To this day, U.S. intelligence lacks a place to perform comprehensive planning for the collection of information, where the yields from overhead reconnaissance, electronic surveillance, clandestine agents, law enforcement databases and informants, and reports from foreign governments can be sifted and organized for maximum effect.

The intelligence job is hard but not impossible. The would-be terrorists have problems as well. If they are supported by a state, their organizations tend to be either large and leaky or small and feckless. If they are not backed by a state, the group may be small, feckless, and pathological, too. These realities form the opportunities for intelligence success. The national security agencies can seize the initiative. Domestic law enforcement officials, understandably, do not actively pursue intelligence collection but focus their efforts on informants or other evidence in investigating suspected criminal actions. Civil liberties properly discourage them from going out and looking for criminals before they have evidence of a crime. On the other hand, domestic law enforcement has many techniques for gathering data, including lawful wiretaps and grand jury investigations. Much of what these efforts yield, however, is closed off to the national security community by law or regulation to safeguard constitutional rights.

The United States needs a new institution to gather intelligence on catastrophic terrorism -- a National Terrorism Intelligence Center -- that would collect and analyze information so it could warn of suspected catastrophic terrorist acts ahead of time.

Since this center would have access to domestic law enforcement data, it should not be located at the Central Intelligence Agency. Instead, the National Center should incorporate the highly successful Director of Central Intelligence Counterterrorism Center, which has a narrower mandate than this proposal, and be located in the Federal Bureau of Investigation. However, the center would be run by an operating committee chaired by the director of central intelligence and including the director of the FBI, the deputy secretary of defense, the deputy attorney general, the deputy secretary of state, and the deputy national security adviser. The National Foreign Intelligence Program, which already provides support for the FBI's National Security Division, would cover the

center's budget, while the National Security Council would take up unresolved disputes. The director of the center would come alternately from the FBI and the CIA, and all intelligence organizations would provide a specified number of professionals exempt from agency personnel ceilings.

In short, the center would combine the active intelligence gathering approach of the national security agencies, which are not legally constrained in their foreign investigations, with the domestic authority and investigative resources of law enforcement agencies. This combination is consistent with public trust and respect for civil liberties: the center would have no powers of arrest and prosecution and would maintain a certain distance from the traditional defense and intelligence agencies. The center would also be subject to oversight from existing institutions, like the federal judiciary, the President's Foreign Intelligence Advisory Board, and the select intelligence committees of Congress. Such a plan reconciles the practices of foreign intelligence work with the restrictions that limit the reach of law enforcement.

PREVENTION AND DETERRENCE

at least three measures are needed to prevent and deter catastrophic terrorism: an international legal initiative outlawing the development or possession of weapons of mass destruction, a National Information Assurance Institute, and stronger federal support for strategic risk analysis.

Outlawing Terror Weapons. Prevention is intertwined with deterrence. The United States already has a firm and increasingly credible policy that criminalizes terrorist activity and supports sanctions, and even the use of force, to thwart or respond to an attack. Washington must now work with other countries to extend the prohibitions against development or possession of weapons of mass destruction. A Harvard biologist, Matthew Meselson, has suggested a convention making any individual involved in the production of biological weapons liable as an international criminal, prosecutable anywhere, as is already the case for pirates and airplane hijackers. This proposal would still permit countries to research and plan defensive work against biological warfare agents.

Governments have already promised to restrain their weapons development in other treaties, such as the Nuclear Nonproliferation Treaty, the Biological Weapons Convention, and the Chemical Weapons Convention. Governments that break such treaties violate international law. Our proposal is different and goes further. The development of prohibited weapons would become a universal crime, opening the way to prosecute and extradite individual offenders wherever they may be found around the world. Thus the power of national criminal law would be used against people, rather than the power of international law against governments. This builds on analogous developments in piracy law, airplane hijacking, crimes of maritime navigation, theft of nuclear materials, and crimes against diplomats.

Over time, the burden of proof on states to demonstrate compliance with international conventions must shift. International norms should adapt so that states are obliged to

reassure other states that are worried and to take reasonable measures to prove they are not secretly developing weapons of mass destruction. Failure to supply such proof or to prosecute the criminals living within their borders should entitle worried nations to take all necessary actions for their self-defense.

National Information Assurance Institute. Private-sector cooperation is vital but has proven elusive in the fight against cyberterrorism. The President's Commission on Critical Infrastructure Protection stressed that the private sector is reluctant to work with the government on this issue because of the high cost, unclear risk, and the prospect of heavy-handed government action. On the other hand, although the FBI has created a National Infrastructure Protection Center that can help identify weaknesses, it is too overburdened with other operational duties to work successfully with industry or harness the significant resources and expertise in the Pentagon on the cyberproblem.

Instead, a National Information Assurance Institute, based in the private, nonprofit sector, could become an industry laboratory for cyberprotection through a public-private partnership. The institute would serve as a nonprofit research organization composed of private companies, universities, and existing nonprofit laboratories, governed by a board of directors drawn from the private sector and academia. The institute staff could be supplemented from both industry and government. Industry affiliates would include not only manufacturers of information systems and service vendors but companies from the power, telecommunications, banking, transportation, oil and gas, water and sewer, and emergency service sectors. This institute could confidentially assess information assurance for industry and train industry representatives on state-of-the-art procedures ("technical best practices"), possible threats, and government policies while receiving contracts from government. In addition, it could conduct research on security assessment tools, intrusion detection, data recovery, and restoration. It would be hard for individual companies to invest in such research without claiming the proprietary right to profit from it, and difficult for any company to tell competitors about its vulnerabilities. But the government cannot do these jobs effectively on its own either. A neutral third party -- a nonprofit entity in the private sector -- is needed. As the institute develops industry standard best practices and evaluates the vulnerability of commercial products, it could rely on informal private-sector enforcement of these ideas in the marketplace -- through insurance rating, for example -- rather than government regulation. The institute could also perform incident evaluations, monitor information assurance, provide on-call assistance, and help industry develop contingency plans for failure.

Risk Analysis. This form of analysis is well known to engineers who look at a dangerous mechanical or electronic system to find key sequences of errors that can lead not just to failure, but to catastrophic failure. In this case, the role of such analysis would be to define risks, gather data to assess their relative seriousness, and subdivide the problems into components where resources can make the biggest impact. A systemic approach would include area surveillance, specific threat identification, targeted surveillance and warning, interdiction and covert action, postattack consequence management, forensic analysis, preventive and punitive action, and learning lessons.

Government agencies can do many things reasonably well, but strategic risk analysis is not one of them. A better alternative would be a nonprofit center for catastrophic terrorism risk analysis, under an FBI contract -- similar to the role of the rand Corporation early in the nuclear era. The Department of Defense has already created a good planning unit, but such a center must have a domestic, not just defense, focus. Meanwhile, the prevention of catastrophic terrorism depends on the interdiction of the people and materials involved. Guided by strategic risk analysis, a serious U.S. effort would include the development of remote sensing technology to detect nuclear, biological, and chemical weapons (and their components). Aided by international agreements among suppliers, the precursor materials that could be used to make such weapons should be chemically marked to enhance detection or ex post facto investigations.

Moreover, the United States should aspire as a long-term objective to identify every person and all freight entering the country. This goal cannot be attained soon, but even imperfect measures can raise the perceived risk to would-be terrorists that someone could intercept their weapons material. International border crossings are an important bottleneck. The United States should support a system to ensure that every country's passports are computer readable, with every country's passport control stations linked to a database that can verify the document or indicate the need for further inquiries. As with credit cards, third parties can perform this role using data supplied by participating clients -- in this case, governments. Terrorists could still use documents of nonparticipating countries, but those would attract just the suspicion they prefer to avoid.

CRISIS AND CONSEQUENCE MANAGEMENT

America bases its present system for handling terrorist emergencies on the FBI at home and the State Department or local military commanders abroad. If an acute threat emerges in the United States, local authorities must alert the FBI. In turn, the FBI's special agent in charge then organizes the intergovernmental response by activating a strategic intelligence center in Washington and a joint operations center and public affairs effort at the site of the attack. Following the East Africa bombings of U.S. embassies, for example, the State Department covered the diplomatic duties and most consequence management while the FBI took charge of the crime scene and criminal investigation.

If there were a threat of weapons of mass destruction, the FBI could call on its Weapons of Mass Destruction Operations Unit, which coordinates the response with other agencies, in particular the Pentagon. It also has the legal authority to seek military aid for a crisis on U.S. soil. Meanwhile, the Federal Emergency Management Agency (FEMA) would organize consequence management under the "Federal Response Plan." This present structure is adequate for ordinary terrorist threats or attacks, or even small scares involving weapons of mass destruction.

If the U.S. government learned that a large-scale attack of weapons of mass destruction was imminent, however, this usual structure would be pushed aside. The White House would immediately take charge and seek to use every bit of power at America's disposal to avert or contain the attack. The operational command structure would need to direct everything from CIA covert actions to air strikes; set up interdiction on ground, at sea,

and in air; mobilize thousands of soldiers; and move thousands of tons of freight. None of these actions can happen quickly unless plans have already been drawn up and units designated to carry them out, with repeated training and exercises that create the readiness to bring the plans to life. In this situation, the Defense Department would take the leading role. The FBI neither commands the resources nor plans to command them.

Crisis management for catastrophic terrorism should use appropriate force in any part of the world to minimize collateral damage while thwarting a possible attack. It would include urgent protective efforts; employ every resource of federal, state, and local governments; and launch a forensic investigation after an attack to collect evidence and track down the terrorists involved.

If an attack occurs, America must respond immediately to mitigate casualties and damage. Such a massive effort would include emergency medical care; distributions of protective gear, medications, and vaccines; and possible evacuations and area quarantines. It would also require extensive preparations in central locations, the capacity to mobilize its units on sudden notice, and cooperation of local authorities.

The United States needs a two-tier response structure: one for ordinary terrorist incidents that federal law enforcement can manage with interagency help, and another for truly catastrophic terrorist attacks. The government would require two new offices, one within the office of the defense secretary, and the other within the existing U.S. Atlantic Command, which already bears operational responsibility for the defense of the American homeland and the majority of the U.S. armed forces. These Catastrophic Terrorism Response Offices, or CTROS, would coordinate federal, state, and local authorities as well as the private sector to respond to major terrorist threats once they are activated by the president and the defense secretary.

The two CTROS should have the responsibility and accountability for U.S. readiness to handle catastrophic terrorist threats upon activation by the president. The defense secretary would serve as executive agent for both offices and their budget programs, so that they could be incorporated into the Department of Defense's program budgeting system, and he would submit a consolidated catastrophic terrorism response program for the president's budget proposal. Congress moved toward such a goal in the Defense against Weapons of Mass Destruction Act of 1996 (more commonly known as the Nunn-Lugar-Domenici Amendment, or Nunn-Lugar II), which mandated that the Pentagon train civilian emergency personnel at all levels of government and establish rapid terrorism response teams. This idea broadens the scope of the initiative and provides a stronger institutional base.

The Department of Defense would play a strong supporting role, but not the leading one. Its responsibilities would be contingent, not routine. It has the resources and capabilities to meet the challenge of biological and chemical weapons, but it should apply those resources either to crisis management or to postattack planning as part of a larger national effort.

Why two offices, rather than one? The CTRO in the Pentagon would concentrate on preparedness for preemptive and/or retaliatory strikes, through covert action or the armed forces. It would draw additional staff from a relatively narrow set of agencies: the Joint Chiefs of Staff, the CIA, and the FBI. This is a highly secret, delicate activity that currently only the CIA and the Joint Chiefs of Staff -- not the FBI -- cover in an ad hoc manner. The second office, in contrast, would handle a much broader range of activities that affect prevention, containment, and management of the postattack consequences. It would draw on the resources of the National Guard, FEMA, the Department of Health and Human Services, and other federal, state, and local agencies. This office would function like a large orchestra that an integrated structure like the U.S. Atlantic Command could activate in an emergency.

Neither of these new offices need be very large. Their jobs would involve planning, not day-to-day intelligence gathering, law enforcement, or combat operations. Yet their work will be invaluable should a crisis ever come.

ACQUISITION

Today the U.S. government is ordering everything from vaccines to new research, with nearly two dozen agencies issuing their own separate shopping lists. When these budget requests arrive in Congress, the lack of planning creates difficult choices for committees, which then argue with each other about how to divide the appropriations pie. The government should instead coordinate all budgets involving counterterrorism capabilities. The United States needs to acquire technology such as detectors of special materials (like radioactive substances), forensic investigation tools, automated tracking and analysis systems, and protective clothing and equipment. The Clinton administration has already started to acquire stockpiles of vaccines, antidotes, and antibiotics, adding to such a program already underway for the U.S. armed forces. But it still needs resources for storage and shipment of medications as well as research into defense against biological weapons. Laboratories around the country also need improved detection devices so they can rapidly analyze substances and check field identifications.

Attorney General Janet Reno has warned Congress of the extraordinary acquisition requirements of a serious policy addressing catastrophic terrorism. In April, she explained that "we may need to develop an approach which will permit the government to accelerate the normal procurement procedures to quickly identify and deploy new technologies and substances needed to thwart terrorist threats and respond to terrorist acts. These procedures would be used not only to purchase medications and other needed tools, but also in some instances, to borrow medications or tools from, or to enter in effective partnership with, academia and industry." This statement is a call for an interdepartmental acquisition program that draws on Pentagon expertise. Despite its limitations, the Defense Department still has the best track record in the government for successful sponsorship of technological development and rapid, large-scale procurement.

This proposed acquisition program for counterterrorism would be distinct from other programs for cooperative threat reduction (like the Nunn-Lugar programs for the former Soviet Union), the reducing of narcotics trafficking and organized crime, and

nonproliferation activities. The government requires an effective interdepartmental committee system -- a National Counterterrorism Acquisition Council -- chaired by the undersecretary of defense for acquisition and technology. The council should include representatives from other departments, including top subcabinet officials from the Departments of Justice, Energy, Treasury, State, and Health and Human Services, as well as the deputy director of the FBI, the deputy CIA director for science and technology, and the FEMA director.

This acquisition council would need to oversee the field testing and evaluation of new capabilities with the participation of several concerned agencies. Some agencies might worry about the Pentagon usurping the procurement decisions. But it is precisely these agencies that should want the national program. The Defense Department will already be acquiring vast quantities of equipment for its own needs. Suppliers will naturally configure themselves around this demand. Civilian agencies need a way to ensure that their particular requirements are taken into account as well. The acquisition council can also help agencies share technology, tactics, and materiel. Further, this council can provide a point of contact for international programs and technology-sharing with other nations. It can provide government-wide procedures, controlling access to especially sensitive projects within the national counterterrorism program. Although various departments would execute the program, the acquisition council would still be responsible for monitoring the progress of each program element and should be expected to report annually on progress to both the president and Congress.

OVERCOMING DISBELIEF

Catastrophic terrorism poses an eminent threat to America's future. But the United States can fight back only if it sets the right goals. In 1940 and 1941, the U.S. government pondered what kind of forces it would need to wage a global war. The answers went so far beyond the imagination that wry smiles and shaking heads in Washington offices greeted the planning papers as they made their rounds. The Cold War saw a similar pattern of disbelief. The notion of an intelligence system founded on photographic surveillance from the upper atmosphere or outer space seemed outrageously far-fetched in 1954, when the U-2 program was born. The films and cameras alone seemed an overwhelming hurdle. A few years later the U-2s were flying; six years later satellites were in place. Similar stories could be told about the remarkable history of intercontinental missile guidance or the fast deployment of more than a half-million troops and thousands of armored vehicles to the Persian Gulf in 1991 and 1992. America can meet new challenges, but it must first imagine success. Only then can it organize itself to attain it.

*This article is a distillation of the complete report of the Universities Study Group on Catastrophic Terrorism, published by Stanford University. A version of it will appear as a chapter in the forthcoming Preventive Defense: An American Security Strategy for the 21st Century, by Ashton Carter and William Perry. Members of the group, which was convened by the Kennedy School of Government's "Visions of Governance in the 21st Century" Project, are Graham Allison, Zoe Baird, Victor DeMarines, Robert Gates, Jamie Gorelick, Robert Hermann, Philip Heymann, Fred Ikl,, Elaine Kamarck, Matthew

Meselson, Joseph Nye, William Perry, Larry Potts, Fred Schauer, J. Terry Scott, Jack Sheehan, Malcolm Sparrow, Herbert Winokur, and Robert Zoellick. Though most members are sympathetic to our conclusions, none is responsible for this essay.

Ashton Carter is Ford Foundation Professor of Science and International Affairs at Harvard University's John F. Kennedy School of Government and a former Assistant Secretary of Defense. John Deutch is Institute Professor of Chemistry at the Massachusetts Institute of Technology and a former Director of Central Intelligence and Deputy Secretary of Defense. Philip Zelikow, a former member of the National Security Council staff, is White Burkett Miller Professor of History and Director of the Miller Center of Public Affairs at the University of Virginia.