



Combating Chemical,  
Biological, Radiological and  
Nuclear Terrorism:  
A Comprehensive Strategy

Frank J. Cilluffo  
Sharon L. Cardash  
Gordon N. Lederman

December 2000

**Center for Strategic and International Studies**  
**Washington, D.C.**

## About CSIS

The Center for Strategic and International Studies (CSIS), established in 1962, is a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary.

CSIS is dedicated to policy impact. It seeks to inform and shape selected policy decisions in government and the private sector to meet the increasingly complex and difficult global challenges that leaders will confront in the next century. It achieves this mission in four ways: by generating strategic analysis that is anticipatory and interdisciplinary; by convening policymakers and other influential parties to assess key issues; by building structures for policy action; and by developing leaders.

CSIS does not take specific public policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

President and Chief Executive Officer: John J. Hamre  
Senior Vice President and Director of Studies: Erik R. Peterson  
Director of Publications: James R. Dunton

© 2000 by the Center for Strategic and International Studies.  
All rights reserved.

Center for Strategic and International Studies  
1800 K Street, N.W., Washington, D.C. 20006  
Telephone: (202) 887-0200  
Fax: (202) 775-3199  
E-mail: [books@csis.org](mailto:books@csis.org)  
Web site: <http://www.csis.org/>

## **CSIS CBRN TERRORISM TASK FORCE REPORT**

### **EXECUTIVE SUMMARY**

The United States currently lacks a comprehensive strategy for countering the threat of terrorism involving nuclear, radiological, chemical, and – most glaringly – biological weapons. Although federal, state, and local governments have made impressive strides to prepare for terrorism using these weapons – the whole remains less than the sum of the parts. As a result, the U.S. is now at a crossroads. While credit must be given where it is due, the time has come for cold-eyed assessment and evaluation based on program reviews and other measures of effectiveness.

This report offers a roadmap of near-term and long-term priorities for senior federal officials to marshal federal, state, local, private sector, and nongovernmental resources for defending the U.S. homeland against CBRN (chemical, biological, radiological, and nuclear) terrorism.

#### **I. The Threat**

There is no way to predict the nature of the CBRN threat to the U.S. homeland in the near or long term. Some things, however, are clear. Due to unparalleled U.S. power (cultural, diplomatic, economic, and military), U.S. adversaries are likely to favor “asymmetric” attacks against undefended targets as opposed to direct conventional military confrontations. Witness the 1993 attack on the World Trade Center. The threat of CBRN terrorism against the U.S. homeland is serious enough for President Clinton to have stated that there is a 100 percent likelihood of a biological or chemical terrorist

attack on U.S. soil in the next 10 years.<sup>1</sup> As a result, U.S. military superiority in itself is no longer sufficient to ensure the safety of the United States. Consequently, the entire concept of U.S. national security planning must be broadened to encompass CBRN counterterrorism.

## II. The Challenge

CBRN terrorism by states and non-state actors presents unprecedented planning challenges to American government and society. No single federal agency owns this strategic mission completely. Many agencies are acting independently in what needs to be a coherent response:

- \* Federal government agencies that have previously worked little together – such as the Intelligence Community and the Departments of Defense, Justice, Health and Human Services, Agriculture, and Energy – must develop smooth real-time channels of inter- and intra-agency coordination and cooperation.
- \* State and local governments must continue to develop and expand their capabilities to respond to a CBRN terrorist attack. More resources must reach the state and local level for management and execution. State and local assets will be first on the scene, and time is of the essence.
- \* Federal, state, and local governments must allocate – between and amongst themselves – responsibilities and resources for domestic preparedness and ensure harmonization of equipment and operating procedures.
- \* The biomedical community, the public health and human services infrastructure, and pharmaceutical companies must mobilize amongst themselves and work in coordination with the national security community.
- \* The American public must come to grips with the reality of the threat and the need to defend against CBRN terrorism.

Impressive strides have been made by federal, state and local governments.

However, progress has been uneven after several years of activity in this arena. Only

---

<sup>1</sup> Statement of Richard Clarke, National Coordinator for Security, Counterterrorism, and Infrastructure Protection, on 60 Minutes, October 22, 2000.

now does the U.S. know enough to ascertain the contours of a comprehensive strategy and a future year program and budget to implement the strategy. Such a comprehensive strategy would address the full spectrum of activities, from prevention and deterrence, to retribution and prosecution, to domestic response preparedness. It must incorporate both the marshaling of domestic resources and the engagement of international allies and assets. And it requires monitoring and measuring the effectiveness of the many programs that implement this strategy so as to lead to common standards, practices, and procedures.

If federal, state, and local agencies fail to coordinate effectively and judiciously, the gravity and nature of mass casualties following a CBRN attack, when combined with a lack of confidence in government's ability to respond, could produce civil disorder and damage the fabric of American society.

### III. A Comprehensive Strategy for CBRN Counterterrorism: At Home and Abroad

A complete CBRN counterterrorism strategy involves both (1) preventing an attack from occurring, which includes deterrence, non- and counter-proliferation, and preemption, and (2) preparing federal, state, local, private sector, and nongovernmental capabilities to respond to an actual attack. U.S. CBRN counterterrorism capabilities and organizations must be strengthened, streamlined, and then synergized so that effective prevention will enhance domestic response preparedness, and vice versa.

#### A. Prevention

A strategy for preventing CBRN terrorist attacks from occurring is multifaceted: *Deterrence* involves dissuading states and non-state actors from launching an attack out of fear of forceful U.S. political, economic, and/or military response. *Nonproliferation* entails using and adapting traditional arms control techniques to stop the spread of CBRN

weapons, technology, and know-how. *Counter-proliferation* focuses on more aggressive activities – such as covert action and military strikes – to stop the proliferation of CBRN materiel. Finally, *preemption* is designed to disrupt an imminent terrorist attack from actually taking place.

1. The U.S. Intelligence Capability

Linking all four elements of prevention is the need for a first-rate intelligence capability. The breadth, depth, and uncertainty of CBRN threats demands significant investment, coordination, and retooling of the intelligence process across the board, for the pre-attack (warning), trans-attack (preemption), and post-attack (“whodunit”) phases. Moreover, since current intelligence needs exceed available dollars, investments in intelligence must be prioritized.

CBRN counterterrorism poses unique challenges to the U.S. Intelligence Community (IC) due to the fact that terrorist groups are hard to penetrate and have become less susceptible to technological collection techniques. Several steps to strengthen the IC need urgent examination and may require significant changes to intelligence programs and budgets:

- Invest in all-source intelligence capabilities. Multi-disciplinary intelligence collection is crucial to provide indications and warning of a possible attack (including insights into the cultures and mindsets of terrorist organizations) and to illuminate key vulnerabilities that can be exploited and leveraged to disrupt terrorist activities before they occur. To date, signals intelligence has provided decision makers with the lionshare of operational counterterrorism intelligence. National technical means cannot be allowed to atrophy further. While a robust technical intelligence capability is crucial, our human intelligence capability must also be enhanced – especially needed against low-tech terrorists who are also less susceptible to non-human forms of intelligence collection.

- Invest in intelligence analytical capabilities. The intelligence community, including the FBI, must invest in expertise – linguists, CBRN weapons experts, and regional specialists – to buttress its analytical ability to track terrorists considering using CBRN weapons. Moreover, the intelligence community must structure its analytic capabilities and methodologies creatively to track the CBRN terrorist threat.
- Invest in detection and attribution capabilities. A credible retribution capability, essential for effective deterrence, depends upon a strong attribution capability to identify the perpetrators and their supporters. These capabilities include laboratory facilities and personnel necessary for attributing a CBRN attack to its perpetrators.
- Strengthen the U.S. warning capability. Conduct a lessons-learned study of U.S. government warning across the entire intelligence cycle (collection, processing, analysis and dissemination), with an eye towards improving the signal-to-noise ratio to facilitate preventive measures.
- Develop Annual Net Threat Assessments of the Foreign and Domestic Threat of CBRN Terrorism. Provide federal planners with the basis for assessing the emerging risk of such attacks and develop an integrated analysis structure for planning U.S. programs and response.
- Conduct Regular Net Assessments of Counterterrorist Intelligence Capabilities. Develop a comprehensive net assessment of current and projected U.S. intelligence capabilities with respect to warning, detection, defense, targeting, and damage assessment. This assessment must also focus on the current and future capabilities of specific agencies such as the National Security Agency (NSA) and the National Reconnaissance Office (NRO) and agencies with human intelligence responsibilities.
- Foster an environment amenable to recruiting and cultivating sources. The CIA guidelines governing the recruitment of assets who have committed human rights violations may dissuade CIA case officers from recruiting terrorist informants. Standard procedures for evaluating the credibility, reliability, and operational viability of a potential asset should guide terrorist recruitment efforts. The CIA Director should make it clear to field officers that a request to recruit a terrorist will not be automatically denied under these guidelines. The President and Congressional leadership should also encourage such collection efforts by publicly acknowledging the risks involved and by supporting officers in the field.
- Tighten coordination among the non-proliferation, counter-proliferation and counterterrorism communities. Rotational assignments at the analyst level should be encouraged.

- Tap the scientific and biomedical research communities. Develop relationships between the IC and the scientific and biomedical research communities, whose knowledge of emerging capabilities and of other information gleaned from the open scientific literature, international scientific collaborations, and conferences could prove invaluable to the IC – particularly with respect to the bioterrorism threat. Indeed, some of the most critical intelligence related to bioterrorism may be derived through the ongoing and open-source practice of international public health and surveillance activities, such as those run by the World Health Organization.

## 2. Arms Control and Counter-Proliferation

Traditional arms control assumes large state efforts with detectable weapons production programs. But traditional arms control measures are less effective in monitoring and controlling smaller proliferation efforts, and might not detect the rapid development of a biological weapons or chemical weapons manufacturing capability using only commercial supplies and equipment. Nevertheless, traditional arms control measures may influence behavior, though they will be more effective vis-à-vis state-sponsors of terrorism than non-state actors. However, by focusing on state actors, we may also capture non-state actors swimming in their wake. Several measures, including non-traditional counter-proliferation methods, merit immediate consideration:

- Build international consensus against CBRN weapons proliferators. Developing a consensus of leading nations that CBRN terrorism is a problem critical to each state's security, and causing the international community to close ranks in isolating states that do develop such weapons, should be one of the President's most important diplomatic initiatives.
- Strengthen the Biological Warfare Convention (BWC) while finding a reasonable balance with industry's main concerns. Though an imperfect instrument (verification being difficult and enforcement even more so), the BWC is valuable because it strengthens the international norm against development of biological weapons and helps discourage nations bent on acquiring biological warfare capabilities.
- Exploit back channels to warn states and non-state actors who are contemplating the development of CBRN weapons that the U.S. reserves

the right to conduct counter-proliferation activities (overt or covert), including military operations.. This message, designed to deter, would put potential perpetrators on notice.

B. Domestic Response Preparedness

The traditional distinction underlying current response preparedness, namely crisis management versus consequence management, is unworkable in practice. Crisis management and consequence management will occur simultaneously, and there will be no hand-off of the baton from the crisis managers (responsible for immediate response, and apprehension of perpetrators), to the consequence managers (responsible for treating mass casualties and restoring essential services). This artificial distinction distracts us from the more important underlying question of whether we are properly organized in terms of domestic response preparedness.

1. Effective Federal Organization

Effective CBRN counterterrorism requires the coordinated participation of many federal agencies:

- Create a Senate-confirmed Assistant to the President or Vice-President for Combating Counterterrorism. Grant certification and passback authority. The span of departments and agencies involved in combating CBRN terrorism requires that policy be coordinated by the Executive Office of the President. The only way to ensure that the Assistant has sway over the departments' and agencies' policies is to give the Assistant direction over their budgets. This direction is achieved by granting the Assistant authority to certify departments' and agencies' future year plans, program budgets, and annual budgets. Given this budgetary role, the Assistant should be Senate-confirmed.
- Develop future year plans and coordinated program budgets. Each federal department and agency with a CBRN counterterrorism mission should develop five year plans, and long-term research, development, testing, and evaluation (RDT&E) plans. These would then be coordinated by the Assistant to the President or Vice President for Combating Terrorism, who should support a holistic effort to use technology to improve domestic response preparedness and tie RDT&E efforts to practical deployment plans.

- Empower FEMA to assume the lead role in domestic response preparedness. Capitalize FEMA with personnel as well as administrative and logistical support, and assign FEMA the training mission for consequence management. It makes little sense to hive off training for consequence management from the very organization that would handle consequence management. Moreover, FEMA is already well-integrated into state- and local-level activity in the context of natural disasters.
- Resolve potential FBI/FEMA conflicts. The FBI and FEMA will be operating simultaneously in their respective crisis and consequence management roles. The goal is to save lives while also preserving criminal evidence. Exercises should be devised to encourage the dovetailing of these two missions.
- Fortify our own defense by strengthening the consequence management capabilities of our partners worldwide. This should occur through the Department of State's Coordinator for Counterterrorism, who manages the Foreign Emergency Support Team (FEST). The United States Army Medical Research Institute of Infectious Diseases (USAMRIID) and the Centers for Disease Control and Prevention (CDC) should be operationally linked to this capacity in the case of bioterrorism and infectious disease emergencies.
- Establish a Congressional counterterrorism working group. This group should be chaired and vice-chaired by Members of the majority and minority parties, respectively, and include senior staff from the various authorizing and appropriations committees with jurisdiction over federal agencies concerned with terrorism, crisis and consequence management, and homeland defense. By means of a monthly report, the working group would keep these authorizing and appropriations committees apprised of ongoing legislative initiatives and funding issues in Congress.

2. Effective State and Local Organization and the Federal Interface

State and local emergency response personnel will be the initial responders to a CBRN terrorist attack. Federal, state, and local exercises have revealed serious deficiencies in preparedness including severe lack of coordination.

- Increase training and exercising of state and local emergency responders. Expand Nunn-Lugar-Domenici training and exercising for additional state and local jurisdictions, broaden the range of participants (e.g., public health, environmental health and human services personnel), and provide funding for purchase of equipment – all with an eye toward standardizing training and equipment for interoperability across jurisdictions. Develop matrices for judging the effectiveness of training. State and local

jurisdictions should be prepared to participate in cost sharing for maintenance and sustainability of equipment provided.

- Make CBRN exercises more realistic, robust and useful. Training exercises are an indispensable part of efforts to improve domestic response preparedness. For enhanced value, there is a need for additional “no-notice” exercises, as well as more exercises involving bioterrorism scenarios and psychosocial effects (e.g., large numbers of concerned people and people with stress-induced symptoms self-reporting to medical facilities).
  - Create a central clearinghouse to synthesize lessons learned from exercises. Doing so would permit better allocation/appropriation of resources, and would facilitate the emergence of (common) best practices. Also organize a series of conferences, as well as a private Internet site, to facilitate the sharing of ideas and lessons-learned among emergency responders throughout the U.S.
  - Share the expertise and capabilities of the Department of Defense. Sharing DOD’s expertise and capabilities can be a vital contribution to the development and deployment of countermeasures against CBRN weapons. Traditionally, the DOD has provided assistance to federal, state, and local officials in neutralizing, dismantling, and disposing of explosive ordinance, as well as radiological, biological, and chemical materials.
  - Identify and remedy legal ambiguities or inadequate authority. An interagency task force, with state and local representation, should immediately begin efforts to identify legal issues raised by a CBRN threat or attack and work to resolve those issues, whether through proposing new laws or simply clarifying the application of existing laws and authorities.
  - Foster greater organizational collaboration between the health sector and emergency management officials. Such collaboration is critical at the county and city level during an epidemic. Either (a) Nunn-Lugar-Domenici programs should be broadened to focus on the training of medical and public health first responders, or (b) a separate national training strategy for bioterrorism should be developed by HHS and FEMA.
3. Effective Organization of the Medical, Public Health, and Human Services Communities

Since bioterrorism is primarily a medical/public health issue, effective organization of these communities – which are relative newcomers to the national security arena – is critical. The biomedical, public health, and human services

communities are underequipped vis-a-vis a biological attack and for infectious disease in general. The core capacity for public health and medical care needs to be greatly enhanced with respect to detection and treatment of infectious disease. The biomedical, public health, and human services communities should be working in greater partnership with each other and should be coordinating more effectively with the larger national security community. The expertise of the commercial pharmaceutical and biotechnology sectors must also be leveraged and integrated into the effort.

- Capitalize the public health structure. Core functions of public health (*e.g.*, disease surveillance and laboratory capability) will form the foundation of detection, investigation, and response for bioterrorist threats. Development of these core functions requires investing in communications facilities, administrative support, and surge personnel capabilities so that public health offices are capable of leading the effort to contain and eradicate epidemics.
- Develop a national bioterrorism surveillance capacity. Surveillance is the touchstone of public health and organizes the other capacities within the public health sector. A national bioterrorism surveillance system should allow public health and emergency managers to monitor the general health status of their populations (human, livestock and crops); track outbreaks; monitor health service utilization; and serve as an alerting vehicle for a bioterrorist attack. There should be linkage between: public health and clinical medicine; hospitals and health departments; local health officers, and local, state, and federal health authorities.
- Develop rapid and more reliable diagnostic capabilities and systems. Build suitable regional diagnostic centers and upgrade hospital diagnostic laboratories. Create a “library” of strains of diseases which is linked – in real-time and via a safe intranet – to public health and medical systems worldwide. “Gold standard” diagnostic capabilities are critical to recognizing and confirming a biological attack in time to mitigate mass casualties.
- Expand CDC’s national bioterrorism laboratory response network and laboratory standardization efforts. This multi-department (DOD, DOE, FBI, USDA) initiative should fully cover the nation for a coordinated laboratory network for bioterrorism. CDC’s rapid response and technology transfer laboratory activities in support of this network should be expanded, as should the development of standardized assays.

- Direct FEMA and CDC to develop a national response capacity for rapid assessment of a bioterrorist emergency occurring anywhere in the U.S. These agencies should develop a Biological Emergency Support Team (BEST) that can rapidly assess and set priorities following a bioterrorist event. This will ensure that FEMA can rapidly galvanize other federal departments around a common assessment and set of response priorities during a national emergency. Furthermore, this arrangement links state and local infectious disease control agencies through CDC to the disaster management skills of FEMA.
- Expand the provisions on biological terrorism in the Terrorism Annex of the Federal Response Plan and designate FEMA as the lead federal agency to coordinate the National Disaster Medical System (NDMS). The current U.S. plan for an organized response must be updated to include preparedness for a biological attack, which presents a host of unique and complicated challenges and requires re-examining lead agency roles and missions. The National Disaster Medical System, which is composed of FEMA, DOD, HHS, and the VA, has no strategy to augment rapidly medical resources at the state and local level in the event of a biological attack. NDMS has never been resourced properly, nor has it been properly focused on the issue of bioterrorism response.
- Develop a comprehensive strategy for assuring surge capacity for healthcare. Through both regional and national planning efforts, identify all existing assets and how they would be mobilized to address mass casualty care. In addition, develop working strategies for how rapid expansion of care can occur as needed, including potential mobilization of field hospitals or establishment of auxiliary care facilities (*e.g.*, in school gymnasiums, armories, or hotels). Strategies for rapid mobilization of critical equipment needs (*e.g.*, ventilators or respiratory isolation capacity), on a regional basis, must also be formulated.
- Focus national pharmaceutical stockpiling efforts. Developing a national pharmaceutical stockpile of vaccines, drugs, and equipment is administratively complex and costs billions. To streamline this process and spend effectively, a Board which reports to the President should be created. Board members should include state and local emergency planning officials, federal government officials, academic research scientists, and senior pharmaceutical industry representatives.
- Engage the pharmaceutical industry and the private sector as a whole. Explore new funding strategies to “incentivize” broader participation of the private sector, including ways to encourage greater engagement of hospitals/medical care providers in preparedness planning and capability building, and ways to engage more fully the pharmaceutical industry in developing and supplying new diagnostics, antibiotics, antivirals, and vaccines.

- Increase R&D for new pharmaceuticals, vaccines, and antidotes. Harness the power of the U.S. academic and medical communities, and the pharmaceutical industry to research and develop: (a) better understanding of basic pathogens and immunology; (b) new vaccines and antidotes, especially for unknown or “designer” toxins; (c) ways to lengthen the shelf-life of existing vaccines and antidotes; and (d) improved biological detection capability. Provide incentives to, utilize contracts with, and adopt an In-Q-Tel style format vis-à-vis universities and companies. Strengthen applied R&D programs and ensure that R&D is not concentrated solely on military needs.
- Develop an integrated plan for biomedical research conducted under the auspices of both the Departments of Defense and Health and Human Services. Civilian and military research efforts should dovetail, and applied research should not be forsaken in favor of long-term bench research projects.
- Increase physician awareness of the symptoms which could be an indicator of biological terrorism. Physicians are the tripwire for recognizing a biological attack and must be trained to spot symptoms of exotic diseases and rapidly report unusual manifestations or clusters of disease to the appropriate public health authorities. HHS should work with pertinent infectious disease professional societies and medical specialists to further this goal.
- Increase training for other key health and human services personnel. Far too few health department, hospital, mental health, and social services personnel with crucial roles to play after a CBRN attack have received appropriate training. An inadequately prepared health and human service system could easily be overwhelmed. In such a situation, survivors might not receive needed care and suffering might be prolonged.
- Legislate emergency supplemental funding authority (akin to FEMA natural disaster supplemental) for reimbursement for CBRN response activities. This funding should be applied to both domestic and international U.S. response activities.
- Prepare a communications and information strategy. Information packages concerning infectious disease and bioterrorism should be predeveloped in various languages. Public health officials and other governmental personnel who will liaise with the media during a biological attack should train for that role, for instance, through simulated tabletop exercises. These sorts of outreach activities in advance of an event may help to foster trust between key officials and the media.

\* \* \*

Embargoed until 12:01 AM, December 14, 2000

A comprehensive strategy for CBRN counterterrorism must marshal and harmonize federal, state and local resources. Newcomers to the national security arena, such as the biomedical and public health communities, will be critical to this effort. Developing, implementing, and sustaining such a strategy should be one of the highest priorities for U.S. national security in the 21<sup>st</sup> century.

*WE THE PEOPLE of the United States, in Order to form a more perfect Union, establish justice, insure domestic Tranquility, provide for the common defence....*  
– Preamble, United States Constitution

*The means of security can only be regulated by the means and danger of attack. They will, in fact, be ever determined by these rules and by no others.*  
– Federalist No. 41

## I. INTRODUCTION

The United States currently lacks a comprehensive national strategy for combating terrorism against the American homeland involving nuclear, radiological, chemical, and – most glaringly – biological weapons. Countering this threat requires both (1) preventing an attack from occurring, which includes deterrence, non- and counter-proliferation, and preemption, and (2) preparing federal, state, local, private sector, and nongovernmental capabilities to respond to an actual attack. Among chemical, biological, radiological and nuclear (CBRN) threats, bioterrorism gives rise to the most pressing need for new strategic thinking on preparedness and response. This is because our public health emergency infrastructure is relatively underdeveloped in comparison to our traditional national security architecture.

Current thinking and efforts with respect to homeland defense, while impressive, concentrate merely on elements of prevention (e.g., arms control), or on domestic response preparedness (e.g., training emergency responders, or managing the consequences of an attack). As such, the synergies offered by a comprehensive national strategy – namely, how effective prevention will strengthen domestic response preparedness, and vice versa – are lost. In contrast, this report offers decision-makers an integrated strategy covering both prevention and domestic response preparedness, and

presents specific recommendations, for both the near-term and long-term, to translate that strategy into action.

The United States currently fields the most powerful armed forces in the world. Yet military superiority alone is no longer sufficient to ensure America's safety. It is now widely accepted that U.S. adversaries will avoid conventional military confrontation in favor of "asymmetric" attacks against lightly protected targets. Several trends indicate that future attacks may target the U.S. homeland and involve CBRN weapons:

- \* Dramatic changes in the global geopolitical environment and the nature of transnational terrorism: The end of the Cold War spawned new terrorist groups less dependent on states for support. These substate groups are independently funded (e.g., through narco-trafficking and smuggling), and resent pre-eminent U.S. power and/or disdain the West. At the same time, nations no longer restrained by the Cold War/Soviet Union, may be tempted to sponsor a CBRN attack against the U.S., using a terrorist group as cover.
- \* Growth of domestic terrorism: The U.S. faces a domestic terrorist threat composed of "lone wolves," ideological and religious zealots, apocalyptic cults, and anti-government groups. However, to date, these domestic elements have not generally been technically adept.
- \* Increased proliferation of CBRN weaponry: The Soviet Union's collapse left exposed its stockpile of CBRN weaponry and left unemployed its CBRN scientists. Moreover, dozens of nations, including the majority of those designated by the Department of State as state-sponsors of terrorism, possess a chemical or biological weapons capability.
- \* Rapid and continuous technological advances: Advances in science and biotechnology hold both promise and peril. Scientific advancement, especially in the chemical industry, means that a greater variety of inflammable and highly toxic chemicals are commonplace in factories throughout the world. Likewise, new insights into the nature of infectious diseases and the organisms that cause them could easily be redirected to nefarious ends. New technologies will make it increasingly easy to manipulate and deliver pathogens in new ways. Moreover, by facilitating both cross-border communication and access to information, the Internet enables small groups of dedicated terrorists to operate globally.

The fact that the U.S. homeland now faces the threat of CBRN terrorism alters the entire concept of U.S. national security. The current focus on both forward-deployed (or deployable) conventional forces and on nuclear forces aimed at other nuclear powers is insufficient. But the traditional U.S. national security establishment – composed of the military, the intelligence community, the diplomatic corps, and key defense contractors – cannot accomplish the new mission alone. To the contrary, the potential for CBRN attacks presents unprecedented challenges to government and society:

- \* Federal, state, and local governments must allocate responsibilities and resources for domestic response preparedness based on a threat that may materialize simultaneously at both the national and local levels.
- \* Federal government agencies that traditionally have not been part of the national security establishment (such as the Departments of Health and Human Services, and Agriculture), must be brought into the fold, and smooth channels of coordination among all “the players” must be developed.
- \* The biomedical community, the public health and human services infrastructure, and pharmaceutical companies must mobilize and develop improved strategies for partnering among themselves, as well as with others such as the law enforcement and intelligence communities.
- \* More generally, the U.S. government must cooperate with the private sector, aside from traditional defense contractors, to obtain the latest technology and other assets that the government needs for combating CBRN terrorism.
- \* All levels of government must plan now for communicating effectively with the public in the event of a CBRN attack and in the context of 24-hour news media.
- \* The American public must come to grips with the reality of the threat, the resource requirements of CBRN preparedness, and the inconveniences necessary now in order to prevent – or at least cope effectively with following – a major CBRN incident in future.

Given the potential consequences of a CBRN event, developing, implementing and sustaining a comprehensive strategy to combat CBRN terrorism should be one of the highest priorities for U.S. national security in the 21<sup>st</sup> century.

IV. Four Very Bad Days: A Taxonomy of CBRN Terrorism Scenarios

“One Very Bad Day” was how the Smithsonian exhibit on dinosaurs referred to the day on which meteors rendered dinosaurs extinct. Exploring how the U.S. should structure a CBRN counterterrorism program should begin with an understanding of what a “very bad day” caused by a CBRN terrorist attack could look like.

A. CBRN Terrorism Scenarios

1. Very Bad Day No. 1: A Nuclear Terrorist Attack

A high-level Russian source under CIA control reveals details of a missing tactical nuclear weapon from the stockpile at a Siberian storage site. The weapon is believed to be headed to a suspected terrorist organization operating in Iraq. Subsequent communications intercepts between Iraqi and Syrian officials and unnamed persons in the United States reveal plans to smuggle a “special” device into the Land of Satan. Overhead reconnaissance satellites detect a suspicious convoy en route from Iraq to Syria. Information sharing among U.S. intelligence organizations is muddled, as the Central Intelligence Agency (CIA), the National Security Agency (NSA), and the Air Force lack smooth pathways for exchanging data. And information-sharing between the intelligence community and federal law enforcement is obstructed due to the presence of sensitive source materials and legal restrictions associated with domestic collection activities. Western allies are contacted, but the U.S. refuses to divulge the source of the information. Several western allies, believing this to be a ruse by the United States to

strengthen international resolve with respect to sanctions against Iraq, refuse to give the U.S. warning any credibility.

Given the magnitude of the response required, along with the disruption of normal functioning for many state and local organizations and entities, the ability of the Federal Emergency Management Agency (FEMA) to mobilize resources (both human and basic supplies) is rapidly overwhelmed. The President orders Department of Defense (DOD) to provide Military Support to Civil Authorities in accord with the Federal Response Plan. However, defense medical assistance and other disaster relief measures are not forthcoming due to transportation blockages and inability to sustain operations in a radiological environment.

2. Very Bad Day No. 2: A Radiological Terrorist Attack

Building on the first very bad day, a Russian organized crime syndicate steals radioactive isotopes from various unprotected nuclear and medical research laboratories in Russia. The material is sold to a radical Serbian group opposed to U.S. policy in the Balkans. The isotopes as well as plastique are smuggled into Canada and, from there, into the U.S. via an unprotected border-crossing. Once in the U.S., the smuggler heads for Rich Stadium in Buffalo. Sitting among a crowd of 80,000, he detonates the weapon, creating a small explosion but spreading radiological material throughout the stadium.

Buffalo firefighters race to the site but cannot enter due to fleeing fans. However, Buffalo riot police are subsequently able to enter the stadium and restore order. Without radiation detectors, the police are exposed to radiological fallout. Firefighters and hazardous materials (HAZMAT) teams – now able to access the premises – detect the radiation, and set up decontamination equipment. However, the equipment can

decontaminate only 500 people per hour. A near-riot situation ensues. Area hospitals are quickly overrun by real and sympathetic victims suffering, respectively, from radiation exposure and other psychosomatic or stress-related symptoms. Population dislocation also results – on both sides of the border – as people flee what they think is a “contaminated” area.

3. Very Bad Day No. 3: A Chemical Terrorist Attack

With the Utah-based vinyl processing plant shutting down in a matter of weeks and relocating to Mexico, the enraged employee decided to “take action” against the federal government that had supported the North American Free Trade Agreement - and what better symbol of government could there be than the IRS, he thought to himself. After stealing a 50-gallon drum of chlorine, the disgruntled and disenfranchised worker drove to the IRS Processing Center in Ogden, located just two hours away. Parking his stolen vehicle upwind of the Center, the distraught worker remotely detonated the poisonous cargo – purposely selected because of chlorine’s high reactivity with human lungs. The ensuing gas cloud engulfed the building, choking scores of victims instantly and incapacitating hundreds more in the community downwind. Police responded first, but refused to enter the disaster zone without personal protective equipment. As a result, a valuable opportunity to collect criminal evidence was missed. Minutes later, county HAZMAT teams arrived on the scene – but to little avail, as they were overwhelmed by the scale of the incident.

4. Very Bad Day No. 4: A Biological Terrorist Attack

No signs or symptoms of an attack manifested themselves during the incubation period following the covert release of a biological agent. The first cases of the illness

occurred among the portion of the population with the weakest immune systems: children, the elderly, AIDS patients, and patients undergoing chemotherapy. These individuals visited their primary care physicians with complaints akin to the flu. Primary care physicians, seeing nothing unusual in either the symptoms or the numbers of complaints, sent the initial victims home to rest and prescribed over-the-counter medicine. As the biological weapon produced person-to-person disease contagion, the victims infected their family and friends.

As cases mounted in numbers and seriousness, and as odd symptoms manifested themselves, physicians began to contact fellow physicians and the local public health department. Samples were flown to the nearest laboratory and subsequently, to the Centers for Disease Control and Prevention (CDC) laboratory in Atlanta, for diagnostic tests. CDC determined the sample to be a genetically-altered strain of smallpox.

The time lag between testing the first patients and diagnosing the cause of their illness allowed the disease to spread further. Victims – and people believing themselves to be ill – crowded the hospitals. This depleted the supply of beds and equipment. Hoarding of medication by medical staffs across the country increased sharply. Antivirals were flown into the region but, without a distribution mechanism in place, failed to reach the public. The spread of the disease exponentially complicated the efforts of CDC and public health officials to trace the origin of the disease. And the use of experimental antiviral agents introduced a host of complicated and novel issues – such as how to obtain informed consent (for use) from recipients and how to administer the agent to large numbers (particularly intravenously).

Containment of the epidemic was the top priority. Yet, the public health and healthcare communities were unable to work together. Public health officials' antiquated communications facilities broke down under the strain. And, despite pre-existing policies such as the Federal Response Plan and Presidential Decision Directive 39, relationships "on the ground" between the FBI, the public health community, or the governor, and emergency responders, were ad hoc.

Widespread illness in the community resulted in significant shortages of personnel, thereby disrupting critical services including telecommunications, electric power and air traffic control. The rapid spread of the disease caused officials to consider containment and community isolation as the first line of defense. Command, control and communications proved inadequate. And it was not clear who was in charge.

In the end, a quarantine was instituted – but it was too late. Public health, law enforcement, and emergency response personnel were ill prepared to implement such an untested measure. Public health officials mishandled the announcement of the quarantine, sparking panic in outlying communities and causing thousands to flee. Pressured by their own fearful populations, governors of the surrounding states deployed the National Guard to prevent citizens from the infected state from entering. Unable to enter surrounding states, while unwilling to return to their homes, thousands of citizens became refugees. Civil order collapsed.

5. As If Four Bad Days Were Not Enough: A Terrorist Attack Involving a Large Explosive

Conventional explosives could, of course, produce results similar in magnitude to those that would flow from a CBRN attack. Consider, for example, what would have

happened if the bombing of the World Trade Center had indeed collapsed one tower onto the other. In that scenario, 50,000 people could have been killed. Though conventional explosives are beyond the scope of this report, it bears emphasizing that the comprehensive strategy for combating CBRN terrorism outlined herein is equally applicable to terrorist attacks involving these weapons as well. In short, the U.S. must act to prevent terrorist attacks (by whatever means), through deterrence, non- and counter-proliferation, preemption and retribution. The U.S. must also develop the domestic response capability to provide medical care for large numbers of casualties.

B. Reflection on the Four Bad Days

In all instances, emergency responders such as firefighters and police play a critical initial role. In the case of chemical, radiological, and nuclear attacks, the priority is to provide medical treatment to the injured, restore essential services, and ascertain who perpetrated the attack. Biological terrorism, however, is different – and, in its worse case scenario, much more ominous. The process of detecting whether an attack has occurred is more difficult, as there would likely be no detonation. Medical professionals – primary care physicians, emergency room physicians, and pharmacists – will be the first to treat symptoms resulting from an attack. Public health professionals will play a key role in any medical response. Yet, the national emergency infrastructure related to surveillance and alert, and the capacity to expand clinical services, are much weaker than our capabilities vis-à-vis chemical and radiological attacks.

Biological terrorism also presents decision-makers with a different and more difficult calculus. While medical emergency response generally requires some sort of triage of patients, a highly contagious biological agent will force policymakers to adopt

measures to which the American people are unaccustomed – such as isolation, detention, travel restrictions, forced treatment, and possibly full quarantine. Triage will still be required, however – and in its starkest form. Given limited healthcare and pharmaceutical resources, nothing short of who lives and who dies will be at stake.

V. The Constituent Components of a Comprehensive Strategy for CBRN Counterterrorism

No single tenet of CBRN counterterrorist strategy is sufficient in and of itself. Moreover, distinct advantages and particular limitations inhere in each individual element:

- A. Prevention is a coordinated campaign to stop a CBRN terrorist attack before it is perpetrated. There are four types of prevention:
  1. Deterrence
    - a. Definition: Convincing terrorists and states that a CBRN attack on the U.S. will result in massive retribution, dissuading them from launching attacks in the first place. A robust response capability also serves to deter by reducing the possibility that terrorist objectives will be met.
    - b. Limitations: Deterrence requires a convincing ability to attribute an attack to a particular individual, group or state, which may prove quite difficult. Also, while states are more susceptible to deterrence than nonstate actors, states may gamble that state sponsorship of an attack is difficult to ascertain or prove. Finally, certain terrorist groups (such as the suicidal and the apocalyptic) may not be deterred.
  2. Non-proliferation
    - a. Definition: Employing arms control and other international diplomatic or regulatory regimes to prevent the spread of CBRN weapons, agents, technology, and know-how.
    - b. Limitations: Arms control regimes are often not verifiable, and U.S. industry may resist practical verification procedures in order to protect trade secrets.

3. Counter-proliferation
    - a. Definition: Acting aggressively to stop the spread of CBRN weapons, agents, technology, and know-how.
    - b. Limitations: Requires good intelligence and may involve unilateral U.S. action.
  4. Preemption
    - a. Definition: Blocking an actual CBRN attack, whether by disrupting the perpetrators' financial and logistical support on a long-term basis, or by intervening decisively during the advent of an attack.
    - b. Limitations: Requires very good, if not excellent, intelligence; may require either cooperation with other states or unilateral U.S. action.
- B. Response Preparedness consists of managing a CBRN crisis, as well as the consequences of such an event. It includes efforts to apprehend and prosecute terrorists, to administer emergency and long-term medical treatment, to reconstitute critical services, and to preserve or restore civic normalcy.
1. Crisis Management
    - a. Definition: Executing measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism. (Adapted from "The Federal Response Plan").
    - b. Limitations: Requires detailed intelligence to detect an attack immediately, to deploy trained and equipped assets on-scene quickly, and to identify the perpetrator(s).
  2. Consequence Management
    - a. Definition: Instituting measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism. (Adapted from "The Federal Response Plan").
    - b. Limitations: Requires effective coordination between all levels of government, relies upon stockpiles of supplies or the ability to produce such caches quickly, and necessitates

an effective strategy for restoring and maintaining public confidence and trust.

If pursued simultaneously, however, the various tenets of the CBRN counterterrorist strategy discussed above will reinforce each other:

- enhancing deterrence and/or preemption decreases the likelihood of an attack, making other aspects of prevention and all aspects of response less necessary;
- increasing the effectiveness of non-proliferation and counter-proliferation would, correspondingly, provide good intelligence to allow us to focus our deterrent and preemptive efforts;
- pursuing non-proliferation strengthens the international norm against CBRN terrorism, thereby: (1) making U.S. and allied retribution more defensible in the court of world opinion, (2) increasing the credibility of the U.S. deterrent, and (3) decreasing the likelihood of a terrorist attack; and
- improving domestic CBRN terrorism response capabilities – and publicizing them – may disincline potential perpetrators from attempting such attacks.

A comprehensive strategy for combating CBRN terrorism is, therefore, greater than the sum of its parts – and, as such, constitutes a more effective means of countering CBRN terrorism than does current U.S. practice and doctrine.

#### VI. Recommendations for a Comprehensive Strategy for CBRN Counterterrorism

In an ideal world, the safety of every American could be assured. The reality, however, is that resources – both human and financial – are limited, and that some level of risk – even in the context of a comprehensive CBRN counterterrorism strategy – must be absorbed. In order to assist the policymakers facing these difficult challenges, this Report sorts its recommendations into three classes, ordered by level of importance:

Priority 1: The recommendation is of the highest priority and should be implemented immediately (within 180 days) regardless of effort or cost required.

Priority 2: The recommendation is important and should be implemented by January 2003.

Priority 3: The recommendation is desirable but its implementation not critical in the near-term.

A. Prevention

Preventing a CBRN terrorist attack from occurring is our first priority. Each element of prevention – deterrence, non-proliferation, counter-proliferation, and preemption – is discussed below.

1. Deterrence

a. Discussion

Effective deterrence requires a credible U.S. commitment to respond forcefully, in political, economic, and/or military terms, in the event of a CBRN terrorist attack. The objective is to dissuade potential perpetrators – which, in turn, requires robust intelligence and an adversary susceptible to the threat of retribution.

i. Who to Dissuade: Attribution

A robust intelligence capability is a prerequisite of effective deterrence. Without robust intelligence, the source of a CBRN terrorist attack will not be identified (“attribution”) – nor will targeting for retribution be possible. And without attribution and retribution, there can be no credible commitment to forceful response in the wake of a CBRN terrorist attack.

A solid attribution capability is founded on good intelligence about terrorists’ aims, modus operandi, logistics, and CBRN weaponry. Yet, intelligence collection against hard targets of this sort is more challenging today than it was during the Cold War. The explanation for this is four-fold. First, current chemical and biological manufacturing technology is increasingly dual-use in character and widespread. It is

therefore more difficult to determine which manufacturing facilities to monitor – assuming that the location of such facilities can even be ascertained. Moreover, biological equipment is particularly small and thus, easily concealed. Accordingly, whether such equipment is being used to support a covert weapons program<sup>2</sup> will turn on the question of intent.

Second, establishing intent generally requires human intelligence (HUMINT) gleaned either through source recruitment or (terrorist) group penetration – but, until recently, the favored discipline was technical intelligence (signals intelligence, satellite reconnaissance, and the like). Augmenting and honing our HUMINT collection capabilities in the wake of the Cold War is far easier to suggest than do, however. Many terrorist groups are homogenous in composition and small in size, and the smaller groups are assembled into networks of networks – all of which makes penetration difficult. Likewise, the membership of terrorist groups does not frequent the diplomatic cocktail circuit, which would facilitate source recruitment by CIA case officers stationed at embassies overseas. To the contrary, key informants are likely to be thoroughly unsavory characters – if not actual terrorists themselves.

Third, the proliferation of CBRN technology has shortened the span between weapons development and possible deployment, thereby taxing – more than ever before – the capability of the intelligence community (IC) to detect and monitor the emergence of new CBRN threats. And finally, the proliferation of weapons has been accompanied by a

---

<sup>2</sup> The intelligence community has already identified 120 biological agents and 30 chemical agents on which to focus their collection efforts. There is also concern about the creation of “fourth generation” chemical weapons designed to defeat standard detection and countermeasures.

proliferation of intelligence consumers – which has deepened the challenge of dissemination. During the Cold War, the IC focused on a more limited set of customers (including the NSC, Congress, and the Department of Defense, Energy and State). By contrast, today’s array of intelligence consumers is broader – and may vary in composition depending upon the phase of the CBRN attack (be it pre-, trans- or post-).<sup>3</sup>

Against this backdrop, the complexities of attributing a CBRN attack are all the more apparent. Since HUMINT provides unique insights into the answer to “whodunit” (and to who may be considering a CBRN attack), HUMINT collection tradecraft bears greater consideration. Specifically, the CIA, which provides the lion-share of HUMINT, currently operates under guidelines issued in 1995 governing the recruitment of sources that may have been involved in human rights violations. While the guidelines themselves do not prohibit recruitment of such sources, the practical effect of these guidelines has been to discourage CIA case officers from recruiting the types of sources necessary for effective collection efforts (see the Report of the National Commission on Terrorism, also known as “the Bremer Commission”).

Because the stakes involved with CBRN counterterrorism are so high, case officers should be encouraged to recruit and cultivate potential sources, notwithstanding the existence of the 1995 guidelines. If officers in the field are not receiving this message, the Director of CIA should consider the symbolic power of an explicit statement that the guidelines do not apply to the recruitment of terrorists. The CIA has

---

<sup>3</sup> Pre-attack phase: Intelligence should focus on *preventing* an attack or *warning* of its imminence. Trans-attack phase: Intelligence should focus on *detecting* whether an attack is occurring, *preempting* an attack as it is taking place, and *mitigating* an attack if possible. Post-attack phase: Intelligence should focus on providing information useful for *identifying* and then *retaliating* against or *prosecuting* the perpetrators.

said no request to recruit a terrorist has ever been denied, and it is unlikely one ever would be denied. Thus, it is not clear what harm would result from removing the chilling effect the guidelines might have on recruitment efforts by making it clear they do not apply in this particular context. Such a statement could have the added benefit of re-affirming the importance of the guidelines in other contexts, where the need to obtain information from human rights violators is less compelling.

This is not to say that the guidelines present the greatest barrier to the recruitment of terrorist informants, or that their removal would result in a sudden increase in such recruitments. Penetration of a terrorist organization is inherently extremely difficult. Moreover, even without the guidelines, case officers in the field may continue to question the willingness of those in Washington, whether at CIA headquarters, the White House, or on Capitol Hill, to stand behind them when the consequences of this kind of risk-taking manifest themselves. We say we want CIA to recruit more terrorists, but this is a highly risky venture. The risks can and should be managed, but they cannot be eliminated. In the past, risk-takers have often been hung out to dry when inevitable problems arose. If we are going to ask the young men and women risking their lives overseas to gather information on terrorists, we should be prepared to back them up when, despite their best efforts, things fall apart or go awry. Political leaders at both ends of Pennsylvania Avenue should acknowledge to the American people the high risks involved in these intelligence efforts. They should also stand up and share responsibility when things go wrong.

In addition to problems collecting information, the IC lacks the technological capability and analytical structure to decipher the vast volumes of information it does

collect, particularly when the threat itself is so diffuse. With the advent of CBRN terrorism, both state-sponsored and non-state, the range of possible targets for collection has increased, making decisions with respect to focusing collection resources and analyzing data much more complicated. The IC must increase its effectiveness in handling the vast amount of information it does acquire. This includes both classified and open source material. The IC currently has a dearth of properly cleared linguists, leading to lag times in translating collected information. Many members of the IC lack training in chemical and biological science and/or weapons, leaving them ill-suited to recognize the tell-tale signs of such armaments among the mountains of collected intelligence. The IC must make efforts to recruit or liaise with biologists, chemists, and other individuals who have the expertise necessary to provide technical support for U.S. CBRN counterterrorism.

Part and parcel of the analysis issue is the fact that, as the amount of information collected grows exponentially, the IC is unable to access and assimilate advances in information technology (IT) into its operation. Reasons for this include the Agency's long procurement cycles that are inconsonant with "Internet time"; a pay scale that pales in comparison to Silicon Valley's; and a cultural gap between the IC and IT communities. With these problems in mind, the CIA created In-Q-Tel, a non-profit corporation intended to bridge the gap between the Agency and Silicon Valley. In-Q-Tel partners the private sector with the CIA to develop information technology to address some of the Agency's most pressing problems, while at the same time providing commercial opportunities to the private sector. With In-Q-Tel being only one year old, it remains to be seen whether it will prove successful over the long term. In the interim, however, the

NSA and other elements of the IC should consider creating “In-Q-Tel-type” organizations in order to develop and acquire the latest information technology for analyzing raw intelligence and disseminating analyses.

Innovative technology might also assist the IC in thinking through how to disseminate information to its diverse customer base, which ranges from federal agencies, to state and local governments, to the biomedical and public health communities. But the challenge of dissemination is not exclusively technological in nature. Consider, for example, the FBI, which is an increasingly important collector of terrorist-related information, through both the Bureau’s intelligence and law enforcement functions. It is the FBI, for instance, that conducts electronic surveillance under the Foreign Intelligence Surveillance Act. This surveillance is undertaken for intelligence purposes, but most of the information collected never reaches analysts outside the Bureau. The FBI’s primary mission is investigating crimes and supporting the prosecution of criminals. FBI Director Louis Freeh has significantly strengthened the emphasis on prevention of terrorist attacks, with some clear indications of success. However, the Bureau has never embraced the dissemination mission. This is in part cultural, but it also reflects a lack of resources. The National Commission on Terrorism recommended that the FBI develop analysts who could not only assist the FBI in its traditional mission but could also be tasked with ensuring appropriate dissemination of information to analysts and policymakers. This recommendation deserves careful consideration.

Before closing this section, it bears emphasizing up front that combating CBRN terrorism may involve acting jointly with our international allies. A terrorist attack on a U.S. installation overseas, for instance, would require close cooperation with the law

enforcement and security apparatus of the host country. The activities of the Department of State, Office of the Coordinator for Counterterrorism (S/CT), would be – indeed, are – critical to this effort. The Coordinator’s mission is to organize all U.S. government efforts, with foreign governments, to improve counterterrorism and to manage the interagency Foreign Emergency Support Team (FEST). The Coordinator also plays a leading role in the Department of State’s Antiterrorism Assistance Program, which has trained more than 20,000 representatives from over 100 nations. The Coordinator should ensure that the training includes a CBRN terrorism preparedness program, which should include policy engagement with host nation officials and response to a CBRN incident at the operational and emergency responder levels. Additionally, the program should integrate a detailed component on the importance of forensics and on forensic capabilities and techniques.

ii. How to Dissuade: Retribution

Effective deterrence requires the potential perpetrator(s) to be susceptible to the threat of retribution. Few state leaders would be willing to incur the destruction of their own regime as the price for striking at the U.S. However, certain terrorist groups – such as those motivated by the desire to cause Armageddon or by the desire to enter paradise – may be less concerned about the effects of retribution and thus, may be more difficult to dissuade. Moreover, it may be difficult to pin a terrorist group or state activity to a particular location that can be targeted for attack. And even if identified, such a location may lie in a state that may not be acting as that group’s state sponsor (though tolerating that group’s presence on its soil).

Current U.S. policy is based on the concept of “calculated ambiguity,” pursuant to which the U.S. has not specifically stated, but rather has hinted at, whether it will use nuclear weaponry in retribution for a CBRN terrorist attack. As Secretary of Defense William Cohen was quoted as saying in November 1998, “We think the ambiguity involved in the issue of nuclear weapons contributes to our own security, keeping any potential adversary who might use chemical or biological [weapons] unsure of what our response would be.”<sup>4</sup> And, as then Secretary of Defense William Perry testified before Congress in March 1998, “[I]f any country were foolish enough to use chemical weapons against the United States, the response would be ‘absolutely overwhelming’ and ‘devastating’.”<sup>5</sup> The crux of “calculated ambiguity” is that the U.S. will retaliate, although the exact manner of retribution involves a case-by-case decision.

The U.S. currently possesses the capability for conventional surgical strikes against terrorist infrastructure, as demonstrated by the U.S. attack on targets linked to Osama bin Laden in Afghanistan and a purported chemical weapons facility in Sudan. Accordingly, terrorists will likely hide themselves ever more among civilians (whether sympathetic or unwitting), making a surgical (retributory) strike much more difficult. The U.S. must therefore invest continuously in smart-weapons technology in order to enhance America’s ability to conduct such surgical strikes.

Aside from the technical aspects of a military response, any major political, economic, or military response also entails a significant diplomatic element as well. All

---

<sup>4</sup> Dana Priest and Walter Pincus, “US Rejects ‘No First Use’ Atomic Policy: NATO Needs Strategic Option, Germany Told,” The Washington Post (Nov. 24, 1998), p. A24.

<sup>5</sup> The Honorable William Perry, testimony before the Senate Foreign Relations Committee (Mar. 28, 1996).

such actions will be judged by the court of world opinion, but the U.S. is hampered from introducing its most convincing evidence of the target's terrorist activities in order to protect intelligence sources and methods. Moreover, some countries argue that retribution has an uncertain basis in international law. Indeed, the U.S. justified its strikes against Afghanistan and, to a lesser extent, Sudan as being necessary to avert future terrorist attacks rather than as response for the 1998 embassy attacks.

Due to the practical difficulties of military response, the U.S. should pursue other means of retribution against terrorists, including covert action and special operations. Alternatively, the U.S. government may move to strangle a particular group's finances or logistics. This would involve a multi-department effort within the U.S. government – including the IC and the Treasury Department – as well as cooperation by foreign governments due to the fact that terrorists will likely use foreign financial institutions. It should be noted, though, that several established terrorist groups have substantial fundraising mechanisms within the U.S. Accordingly, the U.S. should ratify the United Nations' International Convention for the Suppression of the Financing of Terrorism in order to foster a global effort to squelch terrorists' sources of fundraising.

The role of law enforcement as a retaliatory mechanism against international terrorists should not be discounted. The FBI has played a major role in investigating terrorist attacks overseas such as the Khobar Towers and USS Cole bombings. Certainly the FBI's attribution and investigatory capacity will be useful in determining the perpetrators of an attack so that the U.S. can retaliate through military or other means as appropriate. Yet prosecution of the perpetrators in U.S. courts, or in foreign courts, is also possible. Indeed, the whole question of whether a terrorist attack is treated as an act

of war or a crime meriting prosecution is a strategic decision facing senior U.S. policymakers; prosecution may take a long time to come to fruition, while retribution may cause collateral damage and cause political fallout. In any event, the choice of which strategy to pursue will dictate how the FBI, IC, military, and other governmental agencies will cooperate “on the ground.” As a result of these dual tracks, care must be taken that FBI investigatory actions are coordinated with the IC, the military, the State Department, and other U.S. governmental agencies with respect to terrorist attacks against overseas U.S. diplomatic/military installations, and senior U.S. policymakers must be the ones to decide how the U.S. wishes to respond to the attack and thus whether an attack should be treated as an act of war or as a crime.

Finally, part of making the threat of retribution credible is publicizing the fact that the U.S. will retaliate, even if the exact nature of the retribution is ambiguous. As reviewed above, senior U.S. officials have already made statements concerning massive retribution against states in the event of a CBRN terrorist attack. With respect to non-state actors, the U.S. government’s intent to retaliate has been demonstrated by the Sudan and Afghanistan attacks. To avoid having these incidents be viewed as a one-time affair, the U.S. government should broadcast through backchannels, that the U.S. will respond by any means available, such as covert operations and attacking the group’s logistical base and funding, if the U.S. possesses sufficient evidence linking an attack to a particular terrorist group.

One final point with respect to retribution and thus deterrence: One aspect of the ongoing change in terrorist mentalities is that State sponsorship of terrorism is carefully concealed and terrorist groups now tend to operate in small cells, amalgamated into

networks of networks, thus making them more difficult to track. The diffuse structure also gives leaders of terrorist movements a semblance of plausible deniability with respect to the ultimate actions of their followers. In order to remove any doubt as to a terrorist leader's responsibility for the actions of his or her followers, however far removed, the U.S. should quietly spread the word through back-channels that it will hold military and operational planners personally responsible for the organization's actions. Such a policy would involve a sliding scale, meaning the more removed the leader is from the follower, the less the leader will be targeted for some sort of retribution. Indeed, publicizing such a threat should be part of a larger effort to employ psychological operations against terrorists, convincing them that they are being hunted.

It should be noted that, for domestic terrorist groups, the "retribution" for a terrorist attack is the investigation of the attack by law enforcement and ultimately the prosecution and incarceration of the perpetrators for engaging in criminal activity. If U.S. law enforcement is better able to discover who perpetrated a terrorist attack and prosecute such terrorists effectively, the criminal justice system will be better able to deter such attacks *ab initio*. Thus, the attribution ability called for above with respect to international terrorism aimed at the U.S. homeland will also prove useful in the context of domestic terrorism.

b. Recommendations

Priority 1:

- (1) Invest in all-source intelligence capabilities. Multi-disciplinary intelligence collection is crucial to provide indications and warning of a possible attack (including insights into the cultures and mindsets of terrorist organizations) and to illuminate key vulnerabilities that can be exploited and leveraged to disrupt terrorist activities before they occur. To

date, signals intelligence has provided decision makers with the lionshare of operational counterterrorism intelligence. National technical means cannot be allowed to atrophy further. While a robust technical intelligence capability is crucial, our human intelligence capability must also be enhanced – especially needed against low-tech terrorists who are also less susceptible to non-human forms of intelligence collection.

- (2) Invest in detection and attribution capabilities. A credible retribution capability, essential for effective deterrence, depends upon a strong attribution capability to identify the perpetrators and their supporters. These capabilities include laboratory facilities and personnel necessary for attributing a CBRN attack to its perpetrators.
- (3) Develop Annual Net Threat Assessments of the Foreign and Domestic Threat of CBRN Terrorism. Provide federal planners with the basis for assessing the emerging risk of such attacks and develop an integrated analysis structure for planning U.S. programs and response.
- (4) Conduct Regular Net Assessments of Counterterrorist Intelligence Capabilities. Develop a comprehensive net assessment of current and projected U.S. intelligence capabilities with respect to warning, detection, defense, targeting, and damage assessment. This assessment must also focus on the current and future capabilities of specific agencies such as the National Security Agency (NSA) and the National Reconnaissance Office (NRO) and agencies with human intelligence responsibilities.
- (5) Foster an environment amenable to recruiting and cultivating sources. The CIA guidelines governing the recruitment of assets who have committed human rights violations may dissuade CIA case officers from recruiting terrorist informants. Standard procedures for evaluating the credibility, reliability, and operational viability of a potential asset should guide terrorist recruitment efforts. The CIA Director should make it clear to field officers that a request to recruit a terrorist will not be automatically denied under these guidelines. The President and Congressional leadership should also encourage such collection efforts by publicly acknowledging the risks involved and by supporting officers in the field.
- (6) Tighten coordination among the non-proliferation, counter-proliferation and counterterrorism communities. Rotational assignments at the analyst level should be encouraged.
- (7) Impede terrorist logistics and fundraising. U.S. government departments and the National Security Council staff should further advance strategies and mechanisms to disrupt terrorist fundraising in the U.S. The U.S. should ratify the U.N.'s International Convention for the Suppression of the Financing of Terrorism.

- (8) Establish an information strategy for convincing terrorists that they will not achieve their objectives. Deterrence also requires that the terrorists believe that they will not achieve their end goals, i.e. destruction of our national will, disruption of our everyday way of life, and making us curtail our individual freedom to avoid his attacks. This is a very difficult and challenging undertaking and should be handled with the utmost care employing trained behavioral scientists working with the communications profession.
- (9) Tap the scientific and biomedical research communities. Develop relationships between the IC and the scientific and biomedical research communities, whose knowledge of emerging capabilities and of other information gleaned from the open scientific literature, international scientific collaborations, and conferences could prove invaluable to the IC – particularly with respect to the bioterrorism threat. Indeed, some of the most critical intelligence related to bioterrorism may be derived through the ongoing and open-source practice of international public health and surveillance activities, such as those run by the World Health Organization.

#### Priority 2

- (1) Foster harmonization of allies' policies with respect to retribution. Encourage U.S. allies to adopt policies for retribution similar to the U.S., allowing the U.S. and its allies to present a unified front against states and non-state actors contemplating a terrorist attack. U.S. allies would be less likely to criticize the U.S. in the event of U.S. retribution for a CBRN terrorist attack.
- (2) Increase the IC's ability to tap the most advanced information technology. Strengthen In-Q-Tel and create additional organizations like it to allow the IC to benefit from the latest advances in information technology to collect, analyze, process, and disseminate intelligence information.
- (3) Establish new methodologies and technologies for collection and dissemination of intelligence. Develop pathways and mechanisms for the dissemination of intelligence information, including information collected by the FBI, to the diverse set of players in CBRN counterterrorism (including the Departments of Agriculture and Health and Human Services, state and local governments, and the biomedical and public health communities). Develop methods and technology to allow sharing of certain classified information with uncleared individuals without compromising sensitive sources and methods and for law enforcement information to be shared without violating statutory restrictions. FBI's dissemination function overall should be reviewed and additional resources made available if needed.

- (4) Strengthen U.S. law enforcement capability to prosecute domestic terrorist groups. Deterrence of domestic groups requires a robust law enforcement capability. Law enforcement should be trained to recognize suspicious signs pointing to CBRN terrorism and should have the resources to investigate and prosecute such cases quickly and successfully.

Priority 3

- (1) Explore development of means to obscure sources and methods. Being able to reveal information evidencing guilt would assist the U.S. in justifying retribution in the court of global public opinion. Perhaps means can be developed to obscure the sources and methods involved. For example, if U.S. satellite imagery shows terrorists camps in a particular area, the U.S. could arrange for commercial satellite photographs of that area and release the commercial photographs to the public.
- (2) Continue investing in smart-weapons capability. Retribution against terrorists will require a surgical strike capability. The U.S. already possesses a strong capability, namely B-2 Stealth bombers and cruise missiles, but continued new investments are needed. A corresponding investment will have to be made in intelligence to support these weapons. A significant lesson of the smart weapons age is that precision weapons require precision intelligence.

2. Non-proliferation

- a. Discussion

Non-proliferation involves employing arms control and other international diplomatic or regulatory regimes to control the spread of CBRN weapons, agents, technology, and know-how. More specifically, non-proliferation includes arms control, disarmament programs, and export and domestic controls.

- i. Arms Control

The general purpose of an arms control regime is to develop an agreement, binding under international law upon signatory countries, to ban or limit the procurement or maintenance of certain armaments and production capabilities by the signatories. Arms control regimes exist for nuclear, chemical, and biological weapons. A host of agreements already govern nuclear weapons as well the transfer of fissionable material

and are outside the purview of this study, which instead focuses on arms control regimes for chemical and biological weapons.

Negotiations on the Chemical Weapons Convention (CWC) began in 1968, and the CWC finally entered into force on April 29, 1997. The CWC bans the production, acquisition, stockpiling, transfer, and use of chemical weapons. Under the CWC, states agreed to destroy their chemical weapons and to destroy any chemical weapon production facilities.

The CWC was the first arms control treaty to affect the private sector directly and widely because of its impact on dual-use chemicals and because the CWC included a verification mechanism. The Organisation for the Prohibition of Chemical Weapons (OPCW) is the CWC's monitoring and verification organization. Based in The Hague, it is responsible for implementing a verification infrastructure designed to operationalize the CWC.

The CWC verification mechanism has three major components: First, the *declaration of dual-capacities* is intended to make a state's potential capability for producing chemical weapons transparent. Declaration of dual-capacities involves an accounting by facilities containing dual-use chemical equipment with respect to the actual commercial uses of such equipment. Second, *challenge inspections* involve inspections following elucidation of evidence suggesting non-compliance with the CWC. Third, *routine inspections* involve routine visits to confirm the accuracy of declarations and clarify unresolved questions about declarations.

The verification program is intended to balance the goal of ensuring confidence in states' compliance with the CWC with the need to protect national security interests and

confidential industry information. For example, the CWC enunciated the principle of “managed access,” which allows national security or business confidential information to be protected during on-site inspections by devising alternative methods to answer any questions posed by inspection teams of the OPCW. The CWC verification regime is a carefully crafted tradeoff between the intrusiveness needed to obtain a reasonable level of confidence in treaty compliance and the need to protect trade secrets and unrelated national security information. In fact, the Chemical Manufacturers Association (CMA, since renamed the American Chemistry Council) participated extensively in the CWC negotiations and exerted a strong influence on the U.S. delegation to make sure that industry trade secrets would be protected, including by means of a Treaty Annex on Confidentiality. A strong indication that the U.S. chemical industry’s concerns were largely addressed in the final treaty text is that the CMA was a key supporter of the CWC during the ratification debate in the U.S. Senate in 1997. Indeed, the CWC would not have been ratified by the Republican-led Senate without strong industry support.

The CWC’s companion, the Biological and Toxin Weapons Convention of 1972 (BWC), which entered into force in 1975, condemned germ warfare as “repugnant to the conscience of mankind”, as did the Geneva Protocol of 1925. The BWC prohibits the development, stockpiling, and use of biological weapons – but has no verification or compliance provisions. Instead, the signatory states convene a Review Conference every five years to assess compliance with the Convention. At the 1986 Review Conference, the signatory states agreed that each state should submit annually a series of non-binding declarations about certain biologically-related activities in their country. The purpose of

the declarations was to give states increased confidence that fellow signatories were not involved in the secret development or production of biological weapons.

At the 1991 Review Conference, concern was expressed that many countries were failing to submit the annual reports. As a result, the signatory states agreed to establish the “Ad Hoc Group of Governmental Experts” (VEREX) to examine other methods for strengthening the BWC. After two years, the group submitted a report recommending twenty-one measures for further study. In 1994, the signatory states convened a Special Conference to review the Ad Hoc Group’s recommendations and established the Ad Hoc Group of States Parties to the Biological and Toxin Weapons Convention to develop a legally binding addition to the BWC – called a Protocol – to strengthen confidence in compliance with the BWC. The signatory states as a collective body have requested that the Protocol be completed by November 2001. Akin to the CWC’s verification procedures, the BWC Protocol will most likely involve *declarations of dual-use facilities*, *challenge investigations*, and *nonchallenge visits*. U.S. negotiators have deliberately chosen different terms for the BWC and CWC treaties to make clear the conceptual differences between them, namely that the BWC provides a lower degree of confidence with respect to states’ compliance.

While being the most intrusive verification regime of any arms control treaty, the CWC verification regime is perhaps too young (four years) to provide sufficient empirical data to assess its functioning. In any event, differences between the chemical and biological industries prevent the CWC verification structure from fitting sleekly into the BWC’s particular circumstances. Because of the significant differences between chemical and biological production facilities, U.S. industry has staked out the position

opposing routine on-site inspections and viewing “managed access” with skepticism.

Differences between chemical and biological production facilities that affect verification mechanisms include:

- Confidential business information is more pervasive at biological facilities than at chemical facilities.
- Less information is published in the public domain on pharmaceutical industrial biological processes and developments than on chemical formulae and thus the pharmaceutical industry is more at risk from improper disclosure or industrial espionage.
- More potentially confidential business information is contained in the genetic material of living organisms - the final product or a key agent in production of biological products - than is revealed by a study of chemical processes or production techniques.
- Confidential information is more easily concealed and protected at chemical facilities than at biological ones, where the configuration of the operation or the kind of nutrient media being used to grow microorganisms is more difficult to mask.
- If sampling techniques were used in verification, genetically-engineered products and microorganisms could be easily reproduced, jeopardizing the developing company’s intellectual property and development costs.
- The pharmaceutical and biotechnology industries’ investments in new product development are heavily capitalized in the R&D phase. The perceived risk to their investments is significantly threatened by intrusive activities listed above.

These issues seriously complicate a BWC compliance regime. Other critical issues with respect to the BWC Protocol include: the level of evidence needed to launch a challenge inspection; the criteria relevant to the declarations of dual-use equipment; the implications of the fact that certain toxins are used for legitimate purposes (such as botulinum for eyecare); and the difficulty for any regime dealing with the rapid changes in biotechnology and the global dissemination of advanced research.

The efficacy of a BWC verification system is unclear due to the failure of the United Nations Special Commission (UNSCOM) to ferret out all of Iraq's chemical and biological weapons production facilities and armaments during the initial years after the Gulf War. While quite a few facilities were found and some were destroyed, no intact munitions were found. UNSCOM possessed broader powers of inspection than under the CWC or BWC and was assisted surreptitiously by Western intelligence services – yet, faced by an obstreperous Iraqi dictator, could not account for all of Iraq's CBRN capabilities. Also, unlike chemical weapons, relatively small amounts of biological weapons (such as a kilogram of anthrax spores) constitute a military threat and can be produced quickly – and may prove very difficult to find during an inspection. Indeed, the U.S. has eschewed the use of the word “verification” in the BWC context due to the fact that inspections cannot provide a high level of confidence in compliance in the biological weaponry context. It should be noted that while no arms control treaty can provide one hundred percent confidence, an arms control treaty would be considered effective if it detects militarily significant capabilities in time for other states to take offsetting actions. Notably, the level of confidence with respect to verification procedures for the BWC is low.

There are other reasons for questioning the efficacy of such inspections. While the U.S. chemical and biological industries are highly regulated, leaving a paper trail identifying each such plant, a rogue nation intent on circumventing the CWC or the BWC could locate a plant literally anywhere in its country and camouflage it well. It should be noted, however, that under the CWC, inspections tend to come with 48 hours to 120 hours of warning depending upon the type of facility. Thorough cleaning of internal

seals and gaskets in a chemical production line is a time-consuming task that usually requires disassembly of pumps and reactors and would probably not be completed within 48 hours. Few developing countries have access to advanced “clean-in-place” technologies. In the case of biological agents, telltale traces of microbial DNA are detectable with polymerase chain reaction (PCR) techniques and can survive autoclaving. Yet, as cleaning technology proliferates, rogue nations may acquire the ability to mask chemical and biological activity from routine inspections.

However, while chemical and biological arms control is not a panacea, it is a vital element of CBRN counterterrorism. Arms control treaties reinforce the moral norm against the acquisition and use of chemical and biological weapon capabilities, and provide an international legal basis for coordinated sanctions – political, economic, and/or military – against the relatively small number of violators. Moreover, a state’s public status as a signatory to an arms control treaty with respect to CBRN weapons, combined with its private violation of that treaty, just might motivate a whistleblower within that state to publicize the violation.

The creation of an international legal regime banning such weapons could also be indispensable for diplomatic purposes if the U.S. acts unilaterally. For example, if the U.S. retaliates against a state that sponsors chemical or biological terrorism, or launches a preemptive strike to prevent such terrorism, the U.S. could invoke the international norm against production of chemical or biological weapons as a component of its justification, under international law, for the military strikes. It should be noted, though, that some unilateral U.S. “counterproliferation” strikes have been ineffective or counterproductive, such as the cruise-missile attack against the Al Shifa Plant in Sudan, which led to

international condemnation, or Operation Desert Fox against Iraq, which led to the permanent expulsion of the UNSCOM weapons inspectors.

Disarmament and military conversion programs represent another avenue to stop the spread of CBRN weaponry, know-how, and technology. The Nunn-Lugar “Cooperative Threat Reduction Program,” sometimes called the “Comprehensive Threat Reduction Program,” provides funds (typically \$400 - \$500 million per year) for the Department of Defense to reduce the threat posed by these weapons in the former Soviet Union (FSU). The program was initially enacted as the Soviet Nuclear Threat Reduction Act of 1991, Title II of P.L. 102-228, and was funded by a \$400 million appropriation. At that time, the program only covered nuclear weapons. This money has been spent primarily on the dismantling and destruction of nuclear weapons, launch platforms and submarines; but a small part of the funds have been paid to nuclear scientists of the FSU to keep them from selling out to terrorist nations.

In 1993, the Nunn-Lugar program was expanded by the Cooperative Threat Reduction Act of 1993, 22 U.S.C. § 5951 et seq., which was enacted as Title XII of the National Defense Authorization Act for Fiscal Year 1994, P.L. 103-160. The new Act authorized Nunn-Lugar funds to be expended for the destruction of chemical and biological weapons as well as nuclear.

In the years since Nunn-Lugar was expanded, relatively little money has gone toward non-nuclear purposes. It is estimated that \$150 to \$200 million of the nearly \$5 billion appropriated to the program through the years since its inception has been applied to chemical weapons. For a time, it appeared that this component of the effort would be stepped up dramatically. In April 2000, a Nunn-Lugar-sponsored chemical weapons

destruction research facility was opened as part of Moscow's State Scientific Research Institute of Organic Chemistry & Technology. More importantly, work began on an \$888 million facility near Schuchye, Russia, the site of the FSU's largest chemical weapons stockpile. This was to be the first of seven planned facilities to eliminate Russia's chemical weapons inventory.

However, opposition to the Schuchye project exists in the U.S. House of Representatives. Some Representatives believed that the Russians were relying too much on U.S. funds. This fear was compounded by Russian desires to use some of the money for economic and social improvements in the region around Schuchye. As a result, in October 1999, Congress passed Sec. 1305 of P.L. 106-65, which states: "No fiscal year 2000 Cooperative Threat Reduction funds, and no funds appropriated for Cooperative Threat Reduction programs after the date of the enactment of this Act, may be obligated or expended for planning, design, or construction of a chemical weapons destruction facility in Russia." This stopped the Schuchye project and appears to bar any Nunn-Lugar funds from being used for chemical weapons destruction. To assist Russia with the destruction of chemical weaponry, this provision should be repealed – and corresponding measures for biological weaponry should also be initiated.

ii. Export and Domestic Controls

U.S. export regulations also play a role in preventing international terrorists from acquiring chemical and biological weapons. The Export Administration Act of 1979, as amended by The Chemical and Biological Weapons Control Act of 1991, prohibits U.S. or foreign companies or individuals from "knowingly" exporting any materials or technologies that would assist a foreign government or group in developing a biological

weapon. Domestic companies or individuals who “knowingly” export such materials or technologies will be subject to civil and criminal penalties. Possible sanctions against foreign companies or individuals that “knowingly” exported materials or technologies include U.S. refusal to contract for any goods or services from the offending entity.

Moreover, the U.S. is a member of the Australia Group, an informal association of thirty-one nations established in 1985, formed to monitor import and export restrictions for materials that have the potential for being developed into chemical or biological weapons. The Group’s goal is to limit these weapons by controlling their precursors. The Group seeks to achieve its goal by harmonizing each member’s legislative controls over chemical and biological weapons, by issuing guidelines for detecting weapon transactions, and by promoting information-sharing, which could lead to discovering weapons-related activities.

However, it is very difficult to use export control and supplier regimes to control the spread of chemical and biological equipment. For chemical weapons, the hardware equipment is relatively easy for any nation to build. Likewise, many nations can produce biological equipment domestically. In addition, the technology and know-how for biological equipment is extremely difficult to control because of Internet communication, open source literature, and academic conferences. Further, the Australia Group’s actions are significantly limited by the number of nations that have joined. And most of the Group’s member-nations are European countries, hence, there is little or no representation for certain parts of the world.

Turning to domestic (rather than export) controls, U.S. terrorist groups are restricted from acquiring biological weapons by virtue of the Biological Weapons Anti-

Terrorism Act of 1989 (“1989 Act”). In the 1989 Act, Congress attempted to balance the use of pathogens and toxins for legitimate purposes against research for terrorist use. The 1989 Act enables the federal government to intervene quickly after there is suspicion of improper use and before a potential biological weapon could cause injury or environmental harm. The 1989 Act makes it a federal crime for anyone to develop, manufacture, transfer, or possess any “biological agent, toxin or delivery system for use as a weapon.” 18 U.S.C. § 175(a). An exception is carved out, however, by defining “for use of a weapon” as “not includ[ing] the development, production, transfer, acquisition, retention, or possession of any biological agent, toxin, or delivery system for *prophylactic, protective, or other peaceful purposes.*” 18 U.S.C. § 175(b) (emphasis added). The 1989 Act also gives the government broad civil and investigative powers to prevent the development, production, or stockpiling of biological weapons.

Following the 1989 legislation, Congress passed the Chemical and Biological Weapons Control and Warfare Elimination Act of 1991 (“1991 Act”), in response to efforts by hostile nations to acquire CBRN weapons. The 1991 Act provides for broad economic and diplomatic sanctions (including termination of foreign financial assistance and/or sales of defense articles or services), against any country that uses biological weapons in violation of international law. See 22 U.S.C. § 5601, 5605. Sanctions may also be imposed on any foreign company that “knowingly” exports materials to “prohibited” countries. 22 U.S.C. § 2798. Likewise, offending domestic companies and individuals are subject to civil and criminal penalties. 50 U.S.C. App. §§ 2410 & 2410.

After the Oklahoma City bombing, Congress passed the Anti-Terrorism and Effective Death Penalty Act of 1996 (“1996 Act”)<sup>6</sup> to give the federal government even broader powers to combat domestic terrorism. The 1996 Act expanded the criminal provisions of the 1989 Act by making it a federal crime to threaten or attempt to develop a biological weapon. 18 U.S.C. § 175(a). Congress also made it a federal crime for anyone to create new pathogens or more violent forms of existing pathogens. 18 U.S.C. §§ 175(a) & 178(3), (4).

The 1996 Act also directed the CDC to establish a regulatory regime for biological agents. First, Congress directed the CDC to create and maintain a list of biological agents that “pose a severe threat to public health and safety.” Pub. L. No. 104–132, § 511(d)(1)(A), 110 Stat. 1214, 1284 (1996). The Act set out agent selection criteria, including effect on human health, contagiousness of the agent, method of transmission to humans, and the availability of treatment for any resulting illness. *Id.* at 511(d)(1)(B). In the same instrument, Congress also directed the CDC to establish regulations governing the use and transfer of biological agents. *Id.* at § 511(e). These regulations came into effect on April 15, 1997.

In conjunction with the CDC regulations on biological agent use and transfer, the CDC maintains a list of hazardous agents. The current list, which includes viruses, bacteria, and toxins, includes over thirty agents. 61 Fed. Reg. at 55,190 & 55, 199–200. Facilities that house these agents are subject to procedures designed to ensure that adequate safeguards exist. *Id.* at 55, 197–199. Moreover, all purchases of restricted

---

<sup>6</sup> Pub. L. No. 104–132, 110 Stat. 1214 (1996).

agents must be registered with the federal government, and any transfer of these restricted agents must be documented on an official transfer form, which identifies the shipping and receiving facilities, as well as the name of the agent, and its proposed use and amount. A copy of this form is kept in a central site, which is available to federal and state legal authorities. Any use of the agent (including for research), except for diagnostic tests, is subject to CDC's regulatory regime, which is enforceable by civil and criminal penalties. Id.

The problem with the current regulatory framework is that CDC is not a regulatory agency and will never be able to implement fully this regime. Responsibility for enforcing the possession law should be moved to a regulatory agency (FDA), or to the FBI, with CDC being given the role of providing technical assistance. The current set-up places CDC in opposition to its "clients," *i.e.*, state public health organizations and laboratories, and may remove CDC from outbreak response collaboration. More specifically, state laboratories affected by the possession law are those labs that participated with CDC to implement the national bioterrorism laboratory response network. Such laboratories may be reluctant to invite CDC as a regulatory body into their states. Creating friction between such laboratories and CDC will hamper response capabilities for a bioterrorist attack. Furthermore, CDC lacks search and arrest powers, which a regulatory agency needs in order to be effective.

b. Recommendations

Priority 2

- (1) Elevate the building of an international consensus on stopping CBRN proliferation as a top U.S. diplomatic priority. Developing a consensus of leading nations that CBRN proliferation is a problem critical to each

state's security, and causing the international community to close ranks in isolating states that develop such weapons, should be one of the President's most important diplomatic initiatives.

- (2) Strengthen the Biological Warfare Convention (BWC) while finding a reasonable balance with industry's main concerns. Though an imperfect instrument (verification being difficult and enforcement even more so), the BWC is valuable because it strengthens the international norm against development of biological weapons and helps discourage nations bent on acquiring biological warfare capabilities.
- (3) Expand the Cooperative Threat Reduction Program to include chemical and biological programs. Encourage Congress to repeal Sec. 1305 of PL 106-65, which bars Nunn-Lugar funds from being spent on a chemical weapons destruction facility. Increase funding of Nunn-Lugar programs to encompass destruction of biological weapons as well, although such efforts will be of limited value if seed stocks, recipes, and lab capabilities remain.
- (4) Filling Interstices in U.S. law. Consider filling several of the gaps in current law with respect to criminalization of possession of biological pathogens and improvement of security at U.S. labs. Such gap-filling measures could include:
  - making it unlawful for anyone to possess any biological agent, toxin, or delivery system of a type or in a quantity that is not reasonably justified by a prophylactic or other peaceful purpose;
  - requiring individuals to report their possession of biological agents to the designated agency, and failure to report is a criminal or civil penalty;
  - prohibiting the transfer of biological agents to a person who is not registered; and
  - making possession by certain restricted persons such as convicted felons unlawful.
  - requiring some sort of security clearance to work with certain agents.

### 3. Counter-Proliferation

#### a. Discussion

In contrast to non-proliferation, which utilizes more passive measures to stop the spread of CBRN weapons, agents, technology, and know-how, counter-proliferation

involves a more activist approach with respect to thwarting proliferation. For example, the U.S. might use diplomatic pressure and/or economic sanctions against states suspected of developing CBRN weapons (though it would be preferable if such measures were multilateral).

Counter-proliferation also includes the use of force against a state that is in the process of developing CBRN weapons. Consider, for example, a state building a CBRN weapon production facility that, when complete, would be hardened against attack and virtually undetectable by the IC. To prevent such an outcome, the U.S. may decide that it is better to nip in the bud a hostile state's CBRN capability before it becomes a major threat. The justification for such an attack in international law is unclear, however. And, in any event, the U.S. would likely have to offer credible proof in order to sway world opinion, meaning that the U.S. would have to decide whether justifying its action publicly would be worth the tradeoff in intelligence sources and methods. Given the potential costs associated with a military counter-proliferation operation – namely, possible loss of life, exposure of sources and methods, and ensuing criticism – this is an option to be used exceedingly sparingly. Yet it is an option that must be preserved. Furthermore, counter-proliferation applies to non-state actors as well. The U.S. should actively monitor them to ascertain the extent of their CBRN capability, and if necessary, should act decisively to disarm them.

Underlying all counter-proliferation actions is one essential prerequisite: good intelligence, which is critical to knowing what CBRN weapon capabilities are being developed by other states. The IC and its capabilities must therefore be enhanced in the ways outlined above in the section on deterrence. Additionally, the U.S. must continue

making a strong effort to develop an international consensus on stopping the spread of CBRN weapons manufacturing capabilities.

b. Recommendations

Priority 1

- (1) Exploit back channels to warn states and non-state actors who are contemplating the development of CBRN weapons that the U.S. reserves the right to conduct counter-proliferation activities (overt or covert), including military operations. This message, designed to deter, would put potential perpetrators on notice.

4. Preemption

a. Discussion

Even if deterrence, non-proliferation, and counter-proliferation fail to impede decisively the advent of a terrorist attack involving CBRN weapons, the U.S. may still learn of the impending attack with enough time to launch a preemptive strike to block the attack from taking place. Preemption is based on several components:

*First*, good intelligence is critical to learning that an attack is about to occur, as well as the details of how to intercept and neutralize the attack, and how to target a response. Given the real-time nature of preemption, the U.S. IC will likely have to cooperate with foreign intelligence services in order to obtain speedy and reliable information concerning a particular terrorist group, capability, and plan. Not only will the IC need better human intelligence capability, but the IC will need to be able to process the collected information, translate it, and analyze it quickly and with sufficient precision. Part-and-parcel of this capability is the ability to decide whether a warning of an attack is credible or not. The U.S. IC should undertake a detailed study of the subject

of warning in order to ascertain lessons learned from previous successes and mistakes in this regard.

*Second*, the U.S. government must have the ability to transmit warning information quickly to key decision-makers in order to receive their authorization for a preemptive strike. To facilitate communications, the national security establishment should build a communications system designed solely for the instant transmission to senior decision-makers of credible threat warnings.

*Third*, it is critical that the U.S. military possess the capacity to receive and assimilate intelligence information concerning an impending attack, and to deploy forces quickly for preemption of that attack. The U.S. national security apparatus should conduct exercises to test this capability for rapid response.

*Fourth*, the U.S. must either possess the legal authority to preempt an incident by operating in another country, or must be willing to accept the repercussions of conducting an operation in the absence of such authority.

b. Recommendations

Priority 1

- (1) Strengthen the U.S. warning capability. Conduct a lessons-learned study of U.S. government warning across the entire intelligence cycle (collection, processing, analysis and dissemination), in order to improve the signal-to-noise ratio and thus to facilitate preventive measures such as thwarting a terrorist act or justifying a preemptive attack.
- (2) Conduct interagency exercises of preemption capabilities. Exercises of the national security establishment's preemptive operational and communications capabilities (incorporating the full-range of such capabilities), and should be conducted on an interagency basis and cover multiple scenarios.

B. Domestic Response Preparedness

Despite our best efforts, it is doubtful that the U.S. will prevent every potential attack from occurring:

- Intelligence – no matter how good – is inherently imperfect;
- For sophisticated smugglers, U.S. borders are porous, meaning that terrorists could probably import CBRN weapons into the U.S.;
- Organizational disconnects will occur regardless of how well-designed and reformed are the organizational charts; and
- Some personnel will fail to perform.

A robust domestic response capability is therefore crucial. Yet such a capability requires major resource investments; organizational realignment; cooperation between federal, state, and local authorities; and a closer relationship between the public and private sectors. The political will for effecting such changes is uncertain for a combination of reasons: a popularly-perceived low likelihood of an attack; budgetary pressures; the complexity of the task; and competing policy issues. These could keep domestic CBRN counterterrorism preparedness low on both the national agenda, and the agendas of state and local governments.

Building and maintaining a strong domestic response capability is thus a long-run proposition, and will require sustained presidential leadership. A political coalition supporting the necessary policy initiatives, including funding increases, and programs, could be built by focusing on the “dual-use” of a robust domestic response capability. For instance, a strong U.S. response capability to a bioweapon attack could also be used to respond to a naturally-occurring outbreak of infectious disease. Many factors – including increased world travel and international trade, changing demographics and

environmental practices, growing antibiotic resistance, and the intrinsic mutability of microbes – underscore the nation’s serious, and increasing, vulnerability to infectious disease. Hospitals, health maintenance organizations, and other elements of the biomedical community stand to gain from a properly structured national effort to combat infectious diseases, and may well be enlisted to support government initiatives. The biotechnology sector (both private companies and academic research institutions), should similarly have an interest in funding to develop vaccines, antidotes, and equipment necessary for domestic preparedness, and should lend support for increased funding for research and development with respect to combating CBRN terrorism. Furthermore, the agriculture and livestock industries may lend political support because domestic preparedness for terrorism directed against agriculture and livestock will also buttress U.S. preparedness for crop blights and livestock diseases that are not terrorist-induced.

State and local governments also stand to gain from strengthened CBRN response capabilities because such capabilities are equally applicable for chemical and radiological accident response, and natural disaster management – thus assisting state and local governments in coping with such events quickly and efficiently. In sum, a coalition of powerful political interests can likely be mustered to support increased funding and significant policy and program initiatives for enhancing U.S. CBRN counterterrorism response capabilities.

In the meantime, important shortfalls in our domestic response planning can be remedied without the need for more funding. These include: gaps in legal analysis and/or authority at the federal and state levels; a dearth of information and analysis on the potential impact of psychological and social reactions to a CBRN attack; and inadequate

planning for a worst-case scenario that may require greater involvement by the Department of Defense than is contemplated in current federal response documents. Steps should be taken immediately to address these issues.

As noted above, domestic response preparedness consists of managing a CBRN crisis, as well as the consequences of such an event. It includes efforts to apprehend and prosecute terrorists, to administer emergency and long-term medical treatment, to reconstitute critical services, and to preserve or restore civic normalcy. Though Presidential Decision Directive 39 (PDD-39) draws a distinction between crisis and consequence management, that distinction breaks down in practice, where crisis and consequence management will occur simultaneously. There will be no hand-off of the baton from the crisis managers (responsible for immediate response, and apprehension of perpetrators), to the consequence managers (responsible for treating mass casualties and restoring essential services).

This traditional but artificial distinction between crisis and consequence management distracts us from the more important underlying question of whether we are properly organized in terms of domestic response preparedness.

1. Nuclear Terrorism: Highlighting the Need for Effective Organization of the Federal Government
  - a. Discussion

As noted above, a nuclear terrorist attack would generate a large area of destruction and spread radiological contamination over an even larger area. Such an incident would, in all likelihood, be too devastating for any U.S. state to handle by itself.

The federal government response to a catastrophic terrorist attack is governed by three main legal instruments: PDD-39, the Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. § 5121 *et seq.*, and the Federal Response Plan (FRP) and Terrorism Incident Annex (last updated in April 1999). PDD-39 assigns responsibility for crisis management to the FBI, who will deploy to the site an On-Scene Commander (OSC), assisted by a Domestic Emergency Support Team (DEST). The OSC will coordinate the interagency support network, likely consisting of assets from the Departments of Defense, Energy, Health and Human Services, Justice, and Defense, as well as the Environmental Protection Agency.

PDD-39 gives states primary responsibility for consequence management. However, the Stafford Act provides a mechanism for a state to call upon the federal government for assistance. A state governor may request assistance from FEMA – which, in turn, must obtain a presidential declaration allowing FEMA to respond. Subsequently, as the lead agency for consequence management, FEMA has the authority to call upon other federal departments and agencies. The Stafford Act allows the federal government to reimburse the state for particular expenses incurred.

This structure for dealing with a catastrophic terrorist attack (or series of attacks) gives rise to several issues:

*First*, the practical relationship between FBI and FEMA in the event of an attack is unclear. The FBI is concerned with the terrorist incident from the perspective of law enforcement, while FEMA is charged with protecting public safety and ensuring the continuity of government. These objectives may come into conflict, as the FBI is trying to gather and preserve evidence, while FEMA is attempting to restore essential services

and decontaminate the targeted area. Disputes on the ground in the event of an attack will hamper the effectiveness of the federal response. Potential FBI/FEMA conflicts should be resolved as much as possible before a CBRN terrorist attack takes place. To do so, the FBI and FEMA might consider programs in which members of each agency either rotate through the other or have joint training in order to gain exposure to the other agency's concerns and mission. The FBI and FEMA should also devise exercises designed to highlight possible areas of conflict and to provide an opportunity for brainstorming creative responses.

*Second*, the scope of the Stafford Act remains unclear. Specifically, the types of state expenses that the federal government will reimburse are not clear. And its specific application to certain types of terrorist attacks is subject to some dispute. Ambiguities in the Stafford Act should be clarified as much as possible, and a definitive manual on the Act should be produced by the U.S. government and distributed to all states for their reference.

*Third*, the role of the Department of Defense (DOD) in domestic preparedness for CBRN terrorism has been the subject of much debate. The debate arises due to the concern that only DOD possesses the resources – including transportation assets, basic supplies, communications facilities, etc. – necessary to manage the consequences of a terrorist attack involving CBRN weapons. Furthermore, DOD may indeed play a critical role in the event of maintaining law and order following an attack, which could require deployment of federal troops if the police and the National Guard are insufficient or incapable of doing so, and should the President so direct. Yet given DOD's primary responsibility for deterring and fighting wars outside the U.S., it is wholly appropriate for

DOD to maintain a supporting role in domestic crises, for several reasons. Beyond intent, perceptions are important. The clear perception, as well the reality of civilian control of the military should be preserved. This is particularly true in times of domestic crisis. A lead military role could engender the opposition of civil liberties groups and detract from the political support necessary to fund a complete domestic CBRN counterterrorism preparedness program. Factoring DOD's possible participation in a domestic response must also take into account that, in the event of a terrorist attack on the U.S. homeland that heralds a conventional attack against U.S. forces overseas, DOD may be forced to redirect assets earmarked for homeland defense to stations overseas.

But if not DOD, then who should be in charge? As discussed below, possible contenders such as FEMA and public health agencies are not currently up to the task. However, even if FEMA and public health agencies were fully capable, only DOD realistically has the manpower/resources necessary for more extreme and sustained domestic response actions, particularly quarantine. There should be a contingency plan for this "worst-case" scenario so as to mitigate the inevitable problems such a transfer of authority would entail. (This is very different from saying DOD should always be in charge of domestic response efforts.)

The *fourth* issue that arises with respect to the PDD-39/Stafford Act/FRP structure for dealing with CBRN terrorism is that FEMA has not been resourced to accomplish its mission. Long neglected, FEMA has been revitalized under Director James Lee Witt and has distinguished itself when responding to a series of natural disasters affecting the continental U.S. However, FEMA still lacks the administrative apparatus, logistical tail, and personnel necessary to take a lead role in domestic response.

FEMA must be capitalized in order to develop such capabilities, and responding to a CBRN attack should be made explicitly part of FEMA's responsibility. DOD should not be given the primary mission, for the reasons articulated above. Likewise, the FBI's mission is law enforcement and the Bureau does not have an organizational culture that would readily cleave to such a new mission.

These four issues highlight the fact that CBRN counterterrorism – and particularly the domestic response component – involves a plethora of federal departments and agencies. Yet the federal government has traditionally had difficulty with policy planning that cuts across long-established stovepipes.

A coordination mechanism does, however, exist with respect to national security issues – namely, the National Security Council (NSC). Representatives of the classic national security organizations meet under the rubric of the NSC in order to advise the President. The NSC staff is tasked with coordinating policy among the various national security departments and agencies. In an effort to strengthen the NSC staff's role in guiding and shaping U.S. counterterrorism policy, and with an eye toward organizing the counterterrorism efforts of all departments and agencies, Presidential Decision Directive 62 (PDD-62) created a National Coordinator for Security, Counter-Terrorism, and Infrastructure Protection.

Due to the array of federal CBRN counterterrorism programs, a coordinator within the Executive Office of the President is needed in order to ensure that departmental and agency programs, when amalgamated, constitute an integrated and coherent plan. The way to ensure the coordinator's influence over departmental and agency policies is to give the coordinator a role in the planning, programming, and

budgetary process. But the NSC staff in general - and the national coordinator in particular - lack budgetary authority with respect to how departments and agencies spend their funds. This contravenes the golden rule: he with the gold, rules. In other words, without control of, or at least influence on, the budgetary process, the NSC staff is weakened in any attempt to ensure that a department or agency allocates sufficient resources to accomplish the particular aspect of CBRN counterterrorism assigned to it. Yet, increased budget authority heightens the need for accountability to Congress. And it is unlikely a President would want a confirmable position on the NSC staff, as giving the NSC any budgetary authority is inconsistent with the notion of the NSC staff as interagency coordinators of the policy process unencumbered by operational and budgetary responsibilities.

The answer, then, may lie in splitting the coordinator off from the NSC staff and making the position an independent entity within the Executive Office of the President. In order to influence the planning, programming, and budgeting process, this newly established Assistant to the President would write guidelines for federal agencies with respect to their budgets. The Assistant would also have passback authority, meaning that he or she would work with the Office of Management and Budget (OMB) in reviewing initial departmental and agency budgetary requests. These budgetary requests are reviewed by OMB for adherence to the President's overall policy and budgetary agenda and then, if necessary, passed-back to the departments and agencies for revision. By taking part in the review and pass-back, the Assistant to the President would have the opportunity to comment on the departments' and agencies' budgetary proposals with respect to CBRN counterterrorism preparedness. The Assistant should also have the

authority to decrement up to 10 percent of any program he or she designates as a supporting program for CBRN counterterrorism that does not meet the requirements of the nation's CBRN counterterrorism plan. In essence, the Assistant to the President would perform a role somewhat akin to that of the Office of National Drug Control Policy (ONDCP), which coordinates the policies of the various federal departments and agencies involved in the counter-drug effort.

Turning to Congress, the broad span of CBRN counterterrorism programs across federal departments and agencies is mirrored in the broad span of authority to review CBRN counterterrorism programs across a host of Congressional committees and subcommittees. Without coordination between the committees and subcommittees, Members will not know how their votes on a particular budgetary item or policy will affect the overall CBRN counterterrorism program. A Congressional working group must be established. This group should be chaired and vice-chaired by Members of the majority and minority parties, respectively, and should include senior staff from the various authorizing and appropriation Committees with jurisdiction over federal agencies concerned with terrorism, crisis and consequence management, and homeland defense. By means of a monthly report, the working group would keep these authorizing and appropriating Committees apprised of ongoing legislative initiatives and funding issues in Congress.

b. Recommendations

Priority 1

- (1) Create a Senate-confirmed Assistant to the President or Vice-President for Combating Counterterrorism. Grant certification and passback authority.  
The span of departments and agencies involved in combating CBRN

terrorism requires that policy be coordinated by the Executive Office of the President. The only way to ensure that the Assistant has sway over the departments' and agencies' policies is to give the Assistant direction over their budgets. This direction is achieved by granting the Assistant authority to certify departments' and agencies' future year plans, program budgets, and annual budgets. Given this budgetary role, the Assistant should be Senate-confirmed.

- (2) Develop future year plans and coordinated program budgets. Each federal department and agency with a CBRN counterterrorism mission should develop five-year plans, and long-term research, development, testing, and evaluation (RDT&E) plans. These would then be coordinated by the Assistant to the President or Vice President for Combating Terrorism, who should support a holistic effort to use technology to improve domestic response preparedness and tie RDT&E efforts to practical deployment plans.
- (3) Empower FEMA to assume the lead role in domestic response preparedness. Capitalize FEMA with personnel as well as administrative and logistical support, and assign FEMA the training mission for consequence management. It makes little sense to hive off training for consequence management from the very organization that would handle consequence management. Moreover, FEMA is already well-integrated into state- and local-level activity in the context of natural disasters.
- (4) Resolve potential FBI/FEMA conflicts. The FBI and FEMA will be operating simultaneously in their respective crisis and consequence management roles. The goal is to save lives while also preserving criminal evidence. Exercises should be devised to encourage the dovetailing of these two missions.
- (5) Require command-and-control interoperability. Ensure that FEMA has sufficient command-and-control facilities that are interoperable with other federal agencies as well as state and local assets. This must also incorporate the National Disaster Medical System (see the Medical, Public Health, and Human Services section).
- (6) Fortify our own defense by strengthening the consequence management capabilities of our partners worldwide. This should occur through the Department of State's Coordinator for Counterterrorism, who manages the Foreign Emergency Support Team (FEST). The United States Army Medical Research Institute of Infectious Diseases (USAMRIID) and the Centers for Disease Control and Prevention (CDC) should be operationally linked to this capacity in the case of bioterrorism and infectious disease emergencies.

- (7) Immediately undertake efforts that are not resource-intensive, such as contingency planning on legal, psychosocial, and even military issues. This planning should extend to worst case scenarios, which could be far worse than the “bad days” described above, such as attacks in multiple cities with indications that future attacks may be coming.
- (8) Establish a Congressional counterterrorism working group. This group should be chaired and vice-chaired by Members of the majority and minority parties, respectively, and include senior staff from the various authorizing and appropriations committees with jurisdiction over federal agencies concerned with terrorism, crisis and consequence management, and homeland defense. By means of a monthly report, the working group would keep these authorizing and appropriations committees apprised of ongoing legislative initiatives and funding issues in Congress.

#### Priority 2

- (1) Operationalize the Stafford Act. Clarify ambiguities in the Stafford Act, and produce a definitive manual on the Stafford Act for distribution to all states.
- (2) Harmonize language. A glossary should be created listing terms and acronyms related to CBRN terrorism used by federal, state, and local agencies, especially DOD.
  2. Radiological or Chemical Terrorism: Highlighting the Need for Effective State and Local Preparedness and the Federal Interface

- a. Discussion

As apparent from “Four Very Bad Days,” chemical and radiological attack scenarios are quite similar in that the detonation and/or dispersal of chemical and radiological substances will likely be confined to a specific, delimited area. Chemical and radiological terrorist attacks will engender the same response: arrival at the scene of the attack by local police, firefighters, and emergency medical services – the “emergency responders.”

These emergency responders are part of state and local governments, not the federal government. This complicates efforts to develop a unified and effective domestic response capability. The myriad state and local jurisdictions – indeed, there are an

estimated 32,000 fire departments across the U.S. – result in a crazy-quilt of doctrine, legal authority, equipment, and training for emergency responders. Furthermore, for each local and even state jurisdiction, except for prominent targets such as the greater metropolitan areas of New York City and Washington DC, the probability of an attack in that jurisdiction is so low, and the cost so high of training and equipping emergency responders for CBRN terrorist attacks that emergency responders in many jurisdictions may not be prepared for a high-end chemical or radiological attack.

Congress attempted to remedy this lack of uniformity in training across state and local jurisdictions by enacting *The Defense Against Weapons of Mass Destruction Act* (widely referred to as Nunn-Lugar-Domenici) authorizing training in CBRN preparedness for 120 major cities across the U.S. This number has recently been increased to 157 cities. The Nunn-Lugar Domenici Domestic Preparedness program has achieved the following impressive accomplishments:

- trained over 38,500 emergency responders and medical personnel in the 105 most populated cities in the United States via 1,700 classes;
- executed a total of 239 chemical tabletop, biological tabletop and chemical functional exercises in cities across the United States;
- conducted three, and planned two more, federal, state, and local (FSL) annual interagency exercises;
- loaned over \$21,000,000 worth of nuclear, biological and chemical (NBC) defense equipment to cities;
- established an expert assistance program to create a direct link from emergency responders across the country to NBC subject matter experts;
- developed and executed the Chemical and Biological Improved Response Program that identified gaps in response capabilities and developed solutions; nine publications were generated and include technical reports, summary reports and planning guides; and

- established a Chemical Biological-Rapid Response Team (CB-RRT) that developed, tested, and fielded the Deployable Communications System, a sheltered communications system that provides the CB-RRT with an extensive over-the-horizon communications capability.

While this training has been effective in elevating the preparedness of emergency responders in those major cities, such training is lacking for the vast majority of emergency responders throughout America. Nunn-Lugar-Domenici training needs to be expanded to encompass more cities and jurisdictions in order to improve state and local emergency-response standards and to foster uniformity of knowledge and capability. Training should be provided by videotape, video conferencing and the Internet to facilitate dissemination. Moreover, Nunn-Lugar-Domenici does not provide funding for the purchase of equipment. Nor do emergency responders from jurisdictions across the U.S. have an institutionalized capability to share lessons-learned with each other. A series of conferences, as well as a private Internet site (modeled on [www.wmdfirstresponders.com](http://www.wmdfirstresponders.com) or [www.emergency.com](http://www.emergency.com)), should be utilized to facilitate the sharing of ideas and lessons-learned among emergency responders throughout the U.S. Appropriate security measures are needed to prevent information on U.S. domestic preparedness from reaching terrorists' hands.

And because the Nunn-Lugar-Domenici programs did little to galvanize the emergency responders within the health community, such as emergency departments, clinics, hospitals, and local public health officers, a separate local initiative dedicated to bioterrorism preparedness is needed. In addition, it might be useful to broaden the range of responders receiving such training so as to include, for example, public health, environmental health and human services personnel. Not only would this increase

overall awareness of relevant issues, it would also create needed links between different responder communities.

With respect to the actual equipment needed, emergency responders require personal protective equipment (PPE) to allow them to enter contaminated areas. A federal interagency program, the National Protection Center, has been working toward promulgating standards for PPE. Such standards must continually be updated as the nature of the threat changes. Indeed, certain adversaries of the U.S. have developed so-called “fourth generation” chemical weapons designed specifically to circumvent U.S. military standard-issue PPE. The U.S. IC must stay in close contact with the National Protection Center in order to ensure that emergency responders’ PPE is constantly updated to reflect changes in the CBRN weapons threat.

State and local jurisdictions must also ensure that *all* emergency responders are equipped with PPE. Traditionally, firefighters and hazardous materials (HAZMAT) team members have possessed PPE because these individuals are most likely to come in contact with chemicals in their regular duties. By contrast, law enforcement officials are not normally issued PPE. Yet law enforcement officials will play a critical role in the event of an actual attack, including preserving order at the contaminated site and searching for evidence. Without PPE, those officials will be understandably loathe to fulfill their needed roles. Accordingly, state and local jurisdictions should ensure that law enforcement and other critical emergency responders (such as emergency medical services) possess PPE.

The issue of standards for PPE raises an important point with respect to standardization of equipment, training, and terms. Efforts should be made to ensure that

equipment, training, and communications are harmonized across federal, state, and local assets. This will facilitate interoperability as responders from different local jurisdictions arrive at the scene of an attack and are later joined by state and federal units. At the most basic level, terminology must be harmonized as well. For example, there is no agreement on whether the term “casualties” includes only victims with physical symptoms from the attack or includes individuals who, out of panic, convince themselves that they have physical symptoms. Confusion over the definition of “casualties” is not academic: a local jurisdiction may request antibiotics from the national stockpile by referencing a particular number of “casualties” – by which the local public health officials mean individuals who are actually physically sickened by the attack. However, the directors of the national stockpile may reduce the amount of antibiotics given on the assumption that a significant percentage of the “casualties” are not really ill. Uniformity in terminology will prevent communications disconnects that could ultimately cost lives.

With respect to WMD threats against U.S. diplomatic/military installations abroad, the Department of State, Office of the Coordinator for Counterterrorism (S/CT), trains host nations in basic counterterrorism methods. This program includes a CBRN preparedness program designed to provide host nations and U.S. embassies with a senior crisis/consequence management seminar and host-nation first-responder awareness training. These two courses were developed leveraging the curriculum and lessons learned from the U.S. domestic preparedness programs. Since inception, seven countries have participated in the seminar and four countries in the first-responder training. Yet the initial \$4 million funding level does not support the provision of training to more than eight to ten countries per year, when S/CT estimates that more than 40 countries need the

program. Additionally, as in the U.S., there is no equipment provided to the host-nation first-responder trainees. The S/CT program should be expanded to provide training to more countries per year and to include protective equipment, decontamination equipment, and detection instruments.

The S/CT manages the interagency Foreign Emergency Support Team (FEST), designed to provide support to the victimized host nation in the event of an attack on a U.S. installation. The FEST currently fields one aircraft. Yet, terrorist attacks are occurring more frequently in tandem. The FEST should thus receive funding for additional aircraft and teams in order to be able to deploy to two or more simultaneous CBRN terrorist incidents.

b. Recommendations

The U.S. should develop practical and cost-effective programs to:

Priority 1

- (1) Increase training and exercising of state and local emergency responders. Expand Nunn-Lugar-Domenici training and exercising for additional state and local jurisdictions, broaden the range of participants (e.g., public health, environmental health and human services personnel), and provide funding for purchase of equipment – all with an eye toward standardizing training and equipment for interoperability across jurisdictions. Develop matrices for judging the effectiveness of training. State and local jurisdictions should be prepared to participate in cost sharing for maintenance and sustainability of equipment provided.
- (2) Make CBRN exercises more realistic, robust and useful. Training exercises are an indispensable part of efforts to improve domestic response preparedness. For enhanced value, there is a need for additional “no-notice” exercises, as well as more exercises involving bioterrorism scenarios and psychosocial effects (e.g., large numbers of concerned people and people with stress-induced symptoms self-reporting to medical facilities).
- (3) Create standards for judging the usefulness of training of emergency responders. Currently, no metric exists for analyzing the training provided

to emergency responders. A metric must be developed for ascertaining the sufficiency of the training, and a mechanism must be made to link the substance of such training to the specific types of CBRN threats that the CDC and the IC judge to be most dangerous and likely.

- (4) Harmonize state and local emergency preparedness plans and equipment. Harmonization raises the preparedness levels of laggard state and local jurisdictions, facilitates interoperability, and then promotes greater economies of scale with respect to purchasing personal protective equipment (PPE).
- (5) Integrate emergency responders into federal planning for domestic response preparedness. Emergency responders must have an effective seat at the intergovernmental table to ensure seamless coordination between emergency responders and later-arriving federal assets.
- (6) Share the expertise and capabilities of the Department of Defense. Sharing DOD's expertise and capabilities can be a vital contribution to the development and deployment of countermeasures against CBRN weapons. Traditionally, the DOD has provided assistance to federal, state, and local officials in neutralizing, dismantling, and disposing of explosive ordinance, as well as radiological, biological, and chemical materials
- (7) Accelerate funding for R&D for and procurement of chemical and biological detection equipment. Effective detection equipment increases emergency responders' ability to act quickly and save lives. Emergency responders need access to cheap, hand-held devices with low false-alarm rates to identify potential agents or toxins. Detection equipment for biological pathogens faces serious technical obstacles that must be overcome. In addition, R&D should be directed to lab assays, surveillance, communications, and clinical management.
- (8) Continually update protective standards. The IC and the National Protection Center, which promulgates standards for PPE, should stay in close communication so that standards can continually be updated as states' and terrorists' CBRN capabilities develop.
- (9) Protect all emergency responders. State and local jurisdictions must ensure that *all* emergency responders – including law enforcement officers – are equipped with PPE.
- (10) Create a central clearinghouse to synthesize lessons learned from exercises. Doing so would permit better allocation/appropriation of resources, and would facilitate the emergence of (common) best practices. Also organize a series of conferences, as well as a private Internet site, to facilitate the sharing of ideas and lessons-learned among emergency responders throughout the U.S.

- (11) Foster greater organizational collaboration between the health sector and emergency management officials. Such collaboration is critical at the county and city level during an epidemic. Either (a) Nunn-Lugar-Domenici programs should be broadened to focus on the training of medical and public health first responders, or (b) a separate national training strategy for bioterrorism should be developed by HHS and FEMA.
- (12) Identify and remedy legal ambiguities or inadequate authority. An interagency task force, with state and local representation, should immediately begin efforts to identify legal issues raised by a CBRN threat or attack and work to resolve those issues, whether through proposing new laws or simply clarifying the application of existing laws and authorities.

### Priority 2

- (1) Support training of allies abroad. Increase funding of the S/CT to train forty countries per year in CBRN terrorist preparedness. Provide training, PPE, decontamination equipment, and detection instruments equipment.
  - (2) Equip the FEST to respond to simultaneous terrorist attacks. As terrorist attacks are now taking place in groups, additional FEST teams and aircraft are needed to deploy to simultaneous attacks.
3. Biological Terrorism: Highlighting the Need to Mobilize the Biomedical, Public Health, and Human Services Communities

- a. Discussion

A terrorist attack involving a biological weapon is different from its chemical, radiological or nuclear counterparts. There being no dramatic explosion, the timeline involved is significantly longer than a chemical, radiological or nuclear attack. In fact, the effects of a biological attack will not manifest themselves until after an incubation period, and only subsequent laboratory testing will reveal the type of disease. Moreover, the biomedical and public health communities will play a prominent role in detection and containment of a biological incident. Yet the U.S. response capability for a biological terrorist attack is woefully subpar.

Domestic response preparedness for a biological attack begins with detection capability. The ability to detect an attack quickly is critical in order to contain its spread and treat patients with the correct medicines. The key to an effective system is a robust public health infrastructure. This has several critical elements, including:

(1) epidemiology and surveillance personnel, with appropriate training and administrative support, including information technology; (2) laboratory capacity to detect routine and unusual occurrences; (3) communications capability – to communicate critical information among levels of government and to the health provider community; and (4) education of the medical community and increasing its awareness of, and responsiveness for, disease reporting to public health authorities. The role of reporting is critical, yet too few physicians in this country understand their responsibilities in this regard. Furthermore, the vast majority of physicians are not trained to recognize evidence of – and likely do not even consider – the possibility of a biological attack. For example, the eradication of smallpox means that doctors would not recognize symptoms of the disease today. Awareness of the threat of biological terrorism, and training with respect to the symptoms of known biological weapons, should become a standard component of medical education. For example, exams administered by the National Board of Medical Examiners should include questions regarding biological weapons, and a one-day seminar during medical school could be conducted on the subject. Equally important, physicians need to be educated about the public health system and their critical, frontline role in disease reporting.

The U.S. must capitalize its public health system. It is underequipped to address a biological attack due to years of neglect. State and local public health offices are

understaffed, underfunded, and lacking in robust communications facilities – and sometimes even fax machines. The need to strengthen the working relationships between the public health and the medical care systems has been a continuing concern, made even more pronounced by the demands of the threat of bioterrorism. This was demonstrated clearly during “TOPOFF,” the May 2000 CBRN counterterrorism exercise, in which government, biomedical (particularly infectious disease specialists), and public health professionals spent an inordinate amount of time exchanging contact information. This information needs to be collected, updated, and disseminated on a regular basis. TOPOFF also showed that public health institutions are not well integrated into the other sectors involved in decision-making and response planning. In this vein, the biomedical community may resist the direction of public health officials, even where the public health community has clear statutory authority. (As discussed below, such clear authority is indeed often lacking.)

Connections must also be enshrined between the public health community and the veterinary and wildlife communities. During the advent of the West Nile virus, the Bronx Zoo noticed in July and August of 1999 that birds were dying of unusual circumstances – yet the public health department was not informed. Unusual clusters of sick or dying animals may serve as an important early warning of a bioterrorist attack against U.S. livestock or citizens. Therefore, it is critical that communications be solidified between the public health and the veterinary and wildlife communities. Similarly, new working relationships must be forged between public health and plant agriculture.

Some analysts have proposed devising sophisticated electronic surveillance of various symptoms and syndromes in order to alert public health professionals about the existence of a biological attack. However, such a system of routine data compilations and analysis needs to be carefully examined and developed so as to maximize utility and viability. Doctors are – realistically – unlikely to comply with additional reporting requirements due to the frenzied pace of medical practice and the paperwork already required by health maintenance organizations (HMOs) and federal, state, and local governments. Some physicians do not even have computers, which would preclude real-time reporting. Indeed, only ten percent of reportable diseases are currently reported by medical personnel. After the existence of the West Nile encephalitis virus was publicized in New York City in 1999, already-existing cases of encephalitis – which should already have been reported – suddenly were reported by doctors to public health officials. It is unlikely that heightened reporting requirements would lead to greater compliance.

The U.S. public health system should mine data already collected in order to monitor trends that might signal the presence of an infectious disease. Such a system is already used in New York City, whose public health department is among the best in the nation and was led by current Department of Health and Human Services Assistant Secretary Dr. Margaret Hamburg.<sup>7</sup> The New York City Office of Emergency Management monitors emergency room admissions to the hospital and intensive care admissions for infectious disease, as well as sick calls to emergency medical services, for spikes that may indicate the clandestine release of a bioterrorist pathogen or a naturally-

---

<sup>7</sup> Dr. Hamburg is a member of the study group.

occurring infectious disease. Such monitoring should be done in major metropolitan areas throughout the United States.

Additional investment is needed in diagnostic capabilities in order to provide rapid diagnosis and identification of the biological pathogen. At present, while virtually none of the likely biological weapons can be detected in a normal hospital laboratory, a bioterrorism laboratory response network includes 80 sites that can perform diagnostic tests. The CDC and the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) possess sophisticated diagnostic capabilities for the most sophisticated and dangerous threats. This means that a sample from a patient must be flown from anywhere in the U.S. to either CDC in Atlanta or USAMRIID in Maryland for a diagnosis, which creates a time lag of several precious hours or days and delays the appropriate response. The U.S. should expand its system of regional diagnostic laboratories and upgrade hospital diagnostic capabilities as much as possible, in order to decrease the time-lag before diagnosis. It should be noted that a certain number of U.S. diagnostic facilities exist in foreign countries to provide rapid diagnostics of biological agents affecting U.S. diplomatic/military installations abroad. Additional such facilities should be contemplated, with linkage to World Health Organization diagnostics and surveillance assets.

In this vein, USAMRIID must be capitalized to increase its facilities and ensure retention of key personnel. Since military laboratories such as USAMRIID and USAMRICD are integral components of the nation's response infrastructure for biological and chemical terrorism, respectively, the diagnostic, scientific, operational, and educational capabilities of these military institutes (components of the U.S. Army

Medical Research and Material Command) must be maintained and even enhanced to enable a robust national response capability. These Institutes are in fact the national “gold standards” for defensive research against these types of weapons, and have done an outstanding job of helping to educate healthcare providers and provide diagnostic capabilities for these types of threats, in concert with other agencies such as the CDC.

In addition to developing more diagnostic laboratories, the U.S. should invest in new diagnostic technologies. Such technologies could dramatically shorten the time necessary for a diagnosis while increasing its reliability. For example, one avenue proposed by noted biologist Dr. George Poste is to map the genomes of biological agents in order to compare them to the laboratory sample for rapid diagnosis. Enhancing the reliability of a diagnosis is critical for individual patient care and for the implementation of effective public health measures for disease control. It may prove essential for decision makers, who will likely shy away from declaring that a bioterrorism attack has occurred unless there is a “gold standard” of diagnostic evidence. Enhancing the reliability of a diagnosis may also play an important forensic role in a criminal investigation.

More generally, the U.S. needs to invest in the development of new drugs, vaccines, and other therapeutic approaches. This should include a fundamental investment in basic biomedical research focused on genomics, pathogenesis and human immunology. Our research agenda should focus both on disease/pathogen-specific therapies/prophylactics, as well as on more generic strategies to boost the immune system against infection. Research investments should include support for: research at NIH, USAMRIID, and other government entities.

The public health infrastructure lacks the surge capacity in manpower necessary to vaccinate individuals, distribute vaccines and antibiotics, run hotlines, and interview patients to trace the cause of the epidemic. How a public health department in a mid-sized city would organize such actions, with the requisite security to keep an understandably anxious populace in line, remains unknown. Federal and state resources that could rapidly augment local capabilities are being developed, but comprehensive strategies need to be designed and exercised to test readiness and strengthen program design.

The public health department in the area of the attack will be a focal point for the media. Information concerning the nature of the threat and appropriate public health and medical care interventions needs to be rapidly available to the public and the media. Certain materials (e.g., disease information sheets, symptom checklist, and infection control guidelines) can and should be prepared ahead of time, at least in a predeveloped rather than a preprinted form, to enable rapid dissemination of information in a crisis. Such information should be prepared in a number of different languages. Public health officials need to be trained to provide information to emergency responders, the public, and the media in real-time, particularly in this age of live television and instant communication in which the media is both a player in public policymaking and the key to getting information to the public. The media is an essential partner in getting critical information about what to do to the public that needs it.

Indeed, there is risk that biological terrorism could spark public pandemonium and a breakdown of civil order. While some analysts discount this threat as a “disaster

myth” unproven by empirical data, there likely would be certain panic-inducing triggers during an attack:

- if definitive information cannot be provided to the public about the nature of the attack and the appropriate intervention and protections that are being taken;
- if a scarcity of antibiotics or other medicines develops, causing public health officials to have to prioritize who receives treatment; and
- if the public health officials briefing the media lack credibility, creating widespread distrust of government information and a resort to self-help.

Additional research is required to forecast how the U.S. population will react to biological terrorism and what sort of communications and information strategies will keep citizens calm.

Hospitals and the overall healthcare system are also ill-prepared for a biological attack and for a severe naturally-occurring epidemic. Budgetary pressures have forced consolidation and downsizing among hospitals, meaning that there are relatively few empty beds available to handle a massive influx of patients. Much of the inelasticity is due to changes in the economics of medical care, which cannot be reversed easily. Competitive pressures in healthcare also mean that hospitals lack any excess capacity in the area of critical supplies such as antibiotics, or critical capacities such as respirator isolation units, ventilators, and burn care facilities (for a chemical attack).

National and regional planning must be undertaken to address how mass care can be provided, identifying both local and national assets that can be brought to bear – including exploiting the use of military field hospitals, school gymnasiums and local churches, and the creation of agent healthcare sites. The U.S. must build a stockpile of millions of doses of antibiotics, vaccines, and other medicines, as well as surge capacities

of protective gear such as masks, for use in an emergency. Provisions must be made to ensure that these items could be rapidly transported into a “hotzone,” and the necessary personnel mobilized, for effective distribution and delivery of care. Building such a stockpile is another example of how different parts of a comprehensive CBRN strategy reinforce each other. Good intelligence about terrorists’ CBRN weapons capabilities and threat probabilities is vital to the design and procurement of the necessary antibiotics, vaccines, and other materiel to be contained in such a stockpile.

No matter how many doses of medicine the U.S. government stockpiles, demand will almost certainly overtake available supply. And the antibiotics may have expired. Therefore, the U.S. government should work with the pharmaceutical industry to examine options to provide surge production capacity in the event of a crisis. The U.S. should consider building a biological production facility of its own for routine production of “orphan” products that could be utilized in an emergency.

The concept of quarantines is referenced loosely during discussions of biological terrorism. There remain many open issues about what public health authorities could or should be invoked in an infectious disease crisis of this kind. A range of potential public health interventions, potentially including isolation, detention, or quarantine, would need to be reviewed and considered. Certain public health interventions bring with them curbs on civil liberties to which the American people are unaccustomed. In addition, the logistics of implementing certain interventions may be daunting or unachievable. Issues such as the potential role of DOD raise further concerns.

It is important to note at this point that the statutory authority for public health officials is dangerously out of date and inadequate. Most relevant public health laws date

back to at least 1930 and their application to a bioterrorism attack is unclear, at best. Moreover, most experts believe a significant biological attack will quickly rise to the federal level, yet most of the authority needed to control a biological event, such as quarantine authority, resides at the state level. A national security threat in which state governments play such a key role presents unique legal challenges. It is essential that planners work to link expertise and ability with legal authority.

Moreover, while the health arena may present the most urgent need for legal reform, a significant CBRN threat or attack also presents complex legal issues regarding law enforcement authority, the use of foreign intelligence resources within the U.S., and the potential use of the military for domestic purposes. Our current legal framework and analysis is ill equipped for an event that so dramatically combines national security, law enforcement, and public health emergencies. Inadequate legal authority, or a lack of adequate understanding of the application of existing authority, will either hamper our response or result in action being taken without regard for the law. An effective response, with due regard for the very way of life we seek to protect, cannot be undertaken unless the necessary legal framework is in place.

Additional examples of potential legal questions include: federal authority to compel “healthy” states to provide stockpiles of antibiotics or vaccines to affected states; liability of officials or institutions involved in rationing scarce treatment resources; authority to conduct sweep searches or random stops to find biological weapons or terrorists; authority to task reconnaissance satellites to collect imagery within the U.S.; federal authority to compel autopsies or to control the disposition of the deceased to reduce the risk of contagion. A biological attack would quickly raise international and

foreign legal issues, as well. Steps should be taken immediately to identify all legal issues raised by an attack involving CBRN weapons, to remedy legal gaps, and to ensure that the application of legal authorities in such a situation is well understood.

It is unclear how law enforcement would integrate with the public health, human service, and biomedical efforts. The FBI would likely want to interview certain patients and obtain information from their medical records, but these efforts could both interfere with the outbreak investigation and run afoul of patient confidentiality. Representatives from the law enforcement, biomedical, public health, and human service communities should explore this issue together and establish governing principle to prevent conflict in the event of an attack.

The psychosocial implications of a bioterrorist attack will be enormous. How these are handled will be critical to the ultimate effectiveness of our response. Thousands of actually infected casualties, and other people not exposed to the effects of use of the biological weapon, will suffer from the psychological impact of exposure to this event. This has been proven time and again in both natural and man-made disasters. In fact, the phenomenology of psychological impact is so evident that mental psychosocial health crisis counselors are routinely deployed immediately after a major disaster. Their usual mode of operation is to support and counsel those exposed to the event and then slowly help them get over survivor guilt and other manifestations of what amounts to “battle shock.” The longer term effects of exposures to such trauma can be equally debilitating and have been codified under the official APA diagnostic criterion called Post Traumatic Stress Disorder (PTSD).

The lesson is clear: After a major incident involving CBRN weapons, extraordinary demands may be placed on the health and human service system. Hospitals and other health and human services facilities may be deluged with very large numbers of people seeking help. Regardless of what symptoms those people will be experiencing - from illness or injuries to acute stress symptoms that mimic illness - they will all require examinations and care if longer-term problems are to be avoided. As has been pointed out in a recent Institute of Medicine report, it will also be important to have effective triage protocols as well as screening methods for differentiating the more serious psychosocial problems from less serious ones. (See: Institute of Medicine/National Research Council, *Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response*, 1999). An inadequately prepared health and human service system could easily be overwhelmed. In such a situation, survivors might not receive needed care and suffering might be prolonged. In addition, such a situation could easily damage morale and result in a serious loss of public confidence. Clearly, then, it is essential that a robust psychosocial component be well integrated into the overall health response.

Finally, any efforts undertaken in the area of perception management to comfort our own citizens and confuse our adversaries, may be considered dual-use in that some of these strategies can be employed during times of natural disaster as well.

b. Recommendations

Priority 1

- (1) Capitalize the public health structure. Core functions of public health (e.g., disease surveillance and laboratory capability) will form the foundation of detection, investigation, and response for bioterrorist threats.

Development of these core functions requires investing in communications facilities, administrative support, and surge personnel capabilities so that public health offices are capable of leading the effort to contain and eradicate epidemics.

- (2) Develop a national bioterrorism surveillance capacity. Surveillance is the touchstone of public health and organizes the other capacities within the public health sector. A national bioterrorism surveillance system should allow public health and emergency managers to monitor the general health status of their populations (human, livestock and crops); track outbreaks; monitor health service utilization; and serve as an alerting vehicle for a bioterrorist attack. There should be linkage between: public health and clinical medicine; hospitals and health departments; local health officers, and local, state, and federal health authorities.
- (3) Strengthen international surveillance efforts. Working with the World Health Organizations (WHO) to monitor global infectious disease trends and outbreaks of disease would strengthen international surveillance efforts and may provide advance warning for a bioterrorist attack.
- (4) Increase physician awareness of the symptoms which could be an indicator of biological terrorism. Physicians are the tripwire for recognizing a biological attack and must be trained to spot symptoms of exotic diseases and rapidly report unusual manifestations or clusters of disease to the appropriate public health authorities. HHS should work with pertinent infectious disease professional societies and medical specialists to further this goal.
- (5) Direct FEMA and CDC to develop a national response capacity for rapid assessment of a bioterrorist emergency occurring anywhere in the U.S. These agencies should develop a Biological Emergency Support Team (BEST) that can rapidly assess and set priorities following a bioterrorist event. This will ensure that FEMA can rapidly galvanize other federal departments around a common assessment and set of response priorities during a national emergency. Furthermore, this arrangement links state and local infectious disease control agencies through CDC to the disaster management skills of FEMA.
- (6) Expand the provisions on biological terrorism in the Terrorism Annex of the Federal Response Plan and designate FEMA as the lead federal agency to coordinate the National Disaster Medical System (NDMS). The current U.S. plan for an organized response must be updated to include preparedness for a biological attack, which presents a host of unique and complicated challenges and requires re-examining lead agency roles and missions. The National Disaster Medical System, which is composed of FEMA, DOD, HHS, and the VA, has no strategy to augment rapidly medical resources at the state and local level in the event of a biological

attack. NDMS has never been resourced properly, nor has it been properly focused on the issue of bioterrorism response.

- (7) Develop a comprehensive strategy for assuring surge capacity for healthcare. Through both regional and national planning efforts, identify all existing assets and how they would be mobilized to address mass casualty care. In addition, develop working strategies for how rapid expansion of care can occur as needed, including potential mobilization of field hospitals or establishment of auxiliary care facilities (*e.g.*, in school gymnasiums, armories, or hotels). Strategies for rapid mobilization of critical equipment needs (*e.g.*, ventilators or respiratory isolation capacity), on a regional basis, must also be formulated.
- (8) Focus national pharmaceutical stockpiling efforts. Developing a national pharmaceutical stockpile of vaccines, drugs, and equipment is administratively complex and costs billions. To streamline this process and spend effectively, a Board which reports to the President should be created. Board members should include state and local emergency planning officials, federal government officials, academic research scientists, and senior pharmaceutical industry representatives.
- (9) Increase R&D for new vaccines, antidotes, and therapeutics. Harness the power of the U.S. academic and medical communities, and the pharmaceutical industry to research and develop: (a) better understanding of basic pathogens and immunology<sup>8</sup>; (b) new vaccines and antidotes, especially for unknown or “designer” toxins; (c) ways to lengthen the shelf-life of existing vaccines and antidotes; and (d) improved biological detection capability. Provide incentives to, utilize contracts with, and adopt an In-Q-Tel style format vis-à-vis universities and companies. Strengthen applied R&D programs and ensure that R&D is not concentrated solely on military needs.
- (10) Expand CDC’s national bioterrorism laboratory response network and laboratory standardization efforts. This multi-department (DOD, DOE, FBI, USDA) initiative should fully cover the nation for a coordinated laboratory network for bioterrorism. CDC’s rapid response and technology transfer laboratory activities in support of this network should be expanded, as should the development of standardized assays.

---

<sup>8</sup> In basic research, invest in developing a better understanding of the basic biology and pathogenesis (including genomics, virulence and susceptibility/resistance to antibiotics) of biological agents that are most likely to be weaponized. Further research on the human immune response to the various kinds of biological agents of concern is also critical and must underpin efforts to develop new strategies/tools for bolstering the immune system against attack.

- (11) Engage the pharmaceutical industry and the private sector as a whole. Explore new funding strategies to “incentivize” broader participation of the private sector, including ways to encourage greater engagement of hospitals/medical care providers in preparedness planning and capability building, and ways to engage more fully the pharmaceutical industry in developing and supplying new diagnostics, antibiotics, antivirals, and vaccines
- (12) Develop rapid and more reliable diagnostic capabilities and systems. Build suitable regional diagnostic centers and upgrade hospital diagnostic laboratories. Create a “library” of strains of diseases which is linked – in real-time and via a safe intranet – to public health and medical systems worldwide. “Gold standard” diagnostic capabilities are critical to recognizing and confirming a biological attack in time to mitigate mass casualties.
- (13) Identify legal issues that must be addressed. Issues such as quarantine, detention, isolation, curtailment of transport or travel, seizure/destruction of property, mass burials, and other legal issues must all be addressed in the event of a bioterrorist attack. A comprehensive review by an interagency task force, with state and local representation, should be conducted of all applicable state and federal laws/regulations to determine whether legal authorities for such purposes exist and, if so, whether they are adequate. Once the gaps in legal authority have been identified, new statutes and/or regulations can be considered.
- (14) Give greater attention on psychosocial issues and public response. Research must be conducted to better anticipate public response, short-term and long term, in the event of a bioterrorist attack. Appropriate communications strategies, interventions and response plans must be developed in light of that research. In addition, training of psychosocial service providers must be undertaken, and such providers must be fully integrated into crisis and consequence management planning.
- (15) Continue to build communication between the intelligence community, HHS, and the USDA. There is mutual need for information sharing and analysis across these two communities that have limited avenues for routine contact. Closer contact will enable the intelligence community to access greater insights into activities in the world of bioscience and potentially improved training for data collection and analysis; correspondingly, HHS and the USDA require the best possible intelligence regarding threats and threat agents so that they can develop appropriate response plans, including their pharmaceutical stockpile for civilian use and research on new drugs, vaccines and diagnostics.
- (16) Develop an integrated plan for biomedical research conducted under the auspices of both the Departments of Defense and Health and Human Services.

Civilian and military research efforts should dovetail, and applied research should not be forsaken in favor of long-term bench research projects.

- (17) Legislate emergency supplemental funding authority (akin to FEMA natural disaster supplemental) for reimbursement for CBRN response activities. This funding should be applied to both domestic and international U.S. response activities.
- (18) Increase training for other key health and human services personnel. Far too few health department, hospital, mental health, and social services personnel with crucial roles to play after a CBRN attack have received appropriate training. An inadequately prepared health and human service system could easily be overwhelmed. In such a situation, survivors might not receive needed care and suffering might be prolonged.
- (19) Investigate ways of better integrating psychosocial effects into CBRN preparedness and response efforts. This should include both overall planning and plans for hospitals and other facilities. Because knowledge of psychosocial issues related to CBRN incidents remains limited, additional research will also be crucial.
- (20) Prepare a communications and information strategy. Information packages concerning infectious disease and bioterrorism should be predeveloped in various languages. Public health officials and other governmental personnel who will liaise with the media during a biological attack should train for that role, for instance, through simulated tabletop exercises. These sorts of outreach activities in advance of an event may help to foster trust between key officials and the media.

## Priority 2

- (1) Establish the appropriate federal infrastructure to facilitate expeditious regulatory review of drugs, vaccines and diagnostics. Resources must be provided to facilitate FDA review of products that would be required in the event of a bioterrorist attack. This would include not only investigational drugs and medical devices but also new proposed uses of existing products. A critical issue that must be resolved is the off-label use of approved drugs during a bioterrorist event. Where possible, industry should be encouraged to file for supplemental labeling of approved drugs. For both the short term and the long term, this issue must be adequately addressed not only to save lives but also to be in compliance with applicable laws and regulations.
- (2) Convene FBI/HHS task force to discuss integrating law enforcement activities with public health activities in the event of a biological attack or hoax. Issues

Embargoed until 12:01 AM, December 14, 2000

such as strategies for collaboration during concurrent outbreak investigation/criminal investigation, chain of custody issues and patient confidentiality should be addressed prior to an attack to avoid disputes or misunderstandings during an actual crisis.

## **CBRN Terrorism Task Force**

### ***Task Force Chairman and Editor***

Frank J. Cilluffo  
CSIS

### ***Task Force Coordinator and Editor***

Sharon Cardash  
CSIS

### ***Task Force Editor***

Gordon Lederman  
Arnold & Porter

### ***Task Force Members***

Kenneth Alibek  
Hadron

Tom Antush  
Federal Emergency Management Agency

Joseph Barbera  
George Washington University

Steven Becker  
University of Alabama at Birmingham

Pamela Berkowsky (Observer)  
Office of the Secretary of Defense

Robert Blitzer  
SAIC, Federal Bureau of Investigation (Ret.)

Sam Brinkley  
Department of State

Seth Carus  
National Defense University

Guy Copeland  
Computer Sciences Corporation

Anthony Cordesman  
CSIS

Aaron Danis  
Nuclear Regulatory Commission

Raymond Decker  
General Accounting Office

Sheila Dryden  
Department of Defense (Ret.)

Melvin Dubee  
Senate Select Committee on Intelligence

Edward Eitzen  
United States Army Medical  
Research Institute of Infectious Diseases

Mark Esper  
Senate Committee on Governmental Affairs

Robert Filippone  
Office of Senator Bob Graham

Lisa Gordon-Hagerty (Observer)  
National Security Council

Margaret Hamburg (Observer)  
Department of Health and Human Services

Stephen Handelman  
Consultant

Jerome Hauer  
Kroll Associates

Bruce Hoffman  
RAND Corporation

Frank Hoffman  
National Security Study Group

Keith Holtermann  
George Washington University

Edmund Hull  
Department of State

Theodore Jarboe  
Montgomery County Fire and Rescue Service

Brian Jenkins  
Consultant

Robert Kadlec  
National War College

David Kay  
SAIC

Randall Larsen  
ANSER

Bruce Lawlor  
U.S. Joint Forces Command

Joshua Lederberg  
Rockefeller University

Scott Lillibridge  
Centers for Disease Control

Donald Lumpkins  
Maryland Emergency Management Agency

Martha Madden  
Consultant

John Magaw  
Federal Emergency Management Agency

Paul Maniscalco  
Consultant

Kirk McConnell  
House Permanent Select Committee on Intelligence

Alan McCurry  
Office of Senator Pat Roberts

Kenneth Myers, III  
Office of Senator Richard Lugar

Nicholas Palarino  
House Subcommittee on National Security,  
Veterans Affairs, and International Relations

John Parachini  
Monterey Institute of International Studies

H.K. Park  
Department of Defense

Paul Byron Pattak  
The Byron Group

J. David Puposzar  
Allegheny County Health Department

Daniel Poneman  
Hogan & Hartson

Linnea Raine  
Department of Energy

Timothy Sample  
House Permanent Select Committee on Intelligence

Chris Seiple  
Consultant

Walter Sharp  
Attorney

Suzanne Spaulding  
Consultant

Clark Staten  
Emergency Response and Research Institute

Kevin Tonat  
National Disaster Medical System

Jonathan Tucker  
Monterey Institute of International Studies

Bert Tussing  
Army War College

Donald Vincent  
Booz-Allen and Hamilton

Michael Wermuth  
RAND Corporation

Robert Wright  
Computer Sciences Corporation

Allan Zenowitz  
Federal Emergency Management Agency

*\*The opinions, conclusions, and recommendations expressed or implied in this report are not necessarily the product of a Task Force consensus, nor do they necessarily represent the views of the organizations above..*