

# Defending the U.S. Homeland

## Strategic and Legal Issues for DO D and the Armed Services

CSIS Homeland Defense Working Group

**Author:** Fred C. Ikle

January 1999

# Contents

Working Group Members

Summary and Recommendations 1

New Vulnerability to Mass Destruction Weapons 4

The Need for a Defensive Strategy 6

Contingencies That Call for a Leading DOD Role 9

Long- Term R&D Needs 11

    Importance of a Surge Capability 12

    Research Center for Biotechnology and Chemical Defense 14

Legal Authority for a Leading DOD Role 16

Notes 19

References and Related Studies 20

    Threat Assessments 20

    Operational Reports 21

About the Author 24

# **Working Group Members**

## **Project Director**

Fred C. Ikle

## **Working Group**

Kara L. Bue

FrankJ. Cilluffo

Joshua Lederberg

Lewis Libby

Philip Merrill

Gen. Edward C. Meyer, USA (Ret.)

David H. Stephens

Michelle Van Cleave

Richard Wagner

Dov Zakheim

## **With assistance by**

Joseph Cyrulik

Christopher Lennon

Alistair Shepherd

Lesley Young

# Summary and Recommendations

*...we have got to do everything we can to make sure that we close the gap between offense and defense to nothing, if possible.*

—President Bill Clinton  
January 22, 1999

- Because of the continuing global spread of technology, future enemies of the United States will be able to acquire advanced chemical and biological weapons and even first-generation nuclear weapons. Because the U.S. nuclear deterrent has not been designed against these diverse new threats and, indeed, might not be effective in preventing a catastrophic attack, a fundamental shift in U.S. strategy has become necessary: It will have to be a priority mission of the Department of Defense (DOD) to develop, deploy, and operate a wide range of *defensive* measures for the protection of the U.S. homeland.
- Today DOD is not prepared for this mission. It is as if its planning and preparations for armed conflict implicitly assume that U.S. territory would remain a sanctuary. Sometimes it is assumed the enemy would not be capable of using mass destruction weapons within the United States, an assumption contradicted by any realistic analysis. At other times it is assumed the enemy would not dare employ some weapons of mass destruction (WMD) within the U.S. homeland for fear of U.S. nuclear retaliation. Such reliance on nuclear deterrence is not warranted because the enemy would likely use clandestine forms of delivering the weapon and might expect its involvement would remain too ambiguous for nuclear retaliation. Or, to deter retaliation, the enemy might threaten to use additional weapons already emplaced.
- It is important to distinguish attacks on the U.S. homeland by isolated terrorists, on the one hand, and attacks by an enemy in time of war, on the other.
  - The U.S. government is now addressing the possibility that terrorists might use a mass destruction weapon within the United States. It is recognized that terrorist groups might someday acquire highly potent biological or chemical devices (or get hold of a nuclear weapon) for use in a U.S. city. To cope with this danger, the president has designated the Department of Justice and the

Federal Emergency Management Agency the lead agencies, Congress has granted the Federal Bureau of Investigation substantial increases in funding, and the DOD has started to provide training to the National Guard to assist local authorities in remedial measures after an attack has occurred.

- A different approach will be needed if mass destruction weapons are used against the U.S. homeland as part of the enemy strategy in warlike situations, not merely as an isolated terrorist act. Illustrative of such a contingency would be another Gulf war, in which the United States would confront a shifting coalition of hostile countries in the region, all of which might possess WMD of some sort. The United States, while preparing for such a war or already engaged in it, might have credible yet ambiguous information that a member of the enemy coalition has managed to smuggle a few mass destruction weapons into the United States. Or, conversely, as the United States is about to win this war, a biological or nuclear attack might actually occur in a U.S. city. Clearly, if the U.S. homeland is in danger of such attacks in wartime, the Defense Department—not the Justice Department—will have to be prepared to take the lead. Only the armed services would have the managerial and logistical capabilities to mount the all-out defensive effort required. For such a contingency—an attack worse than Pearl Harbor—the American people would expect and, indeed, demand that they could count on DOD and the armed forces to protect their homeland.

## **Clarify Legal Authority for DOD**

- Questions have been raised about the legal authority for U.S. military operations within U.S. territory in defense of the U.S. homeland. The insufficiently understood or perhaps inadequate legal authorities for a military role in defending the U.S. homeland against WMD pose a significant national security risk. A clarification of existing authorities and, if necessary, additional legislation can overcome this deficiency. CSIS will publish a follow-on study on the scope and limitations of relevant legal authority; however, what DOD now mainly lacks for the defense of the U.S. homeland is not the legal authority but the necessary equipment and training.

## **R&D for Surge Capability**

- The instruments, systems, and operational procedures for detecting, interdicting, or rendering harmless any clandestinely introduced mass destruction weapons have either not yet been developed or have not yet been acquired in sufficient quantities. This need not be a permanent condition. A long-term research and development (R&D) effort concentrating on such instruments and equipment holds great promise, as shown by several research projects that have been undertaken by DOD contractors and the national nuclear laboratories. These programs

should be greatly expanded to develop prototypes of equipment for countering chemical and biological attacks against the U.S. homeland and for detecting nuclear weapons that might be smuggled into the United States. Even though the best defenses could not guarantee the interdiction or disabling of every weapon, without greatly enhanced U.S. defenses any rogue country could readily acquire the means to blackmail or paralyze the United States.

- The primary purpose of this R&D effort should be to give the United States a mobilization capability to respond rapidly to a sudden increase in the threat. Before the threat is seen as truly imminent, it might not be prudent to procure the defensive systems in full quantities because of the risk of obsolescence and, in any event, the political and budgetary backing for such an undertaking might not be available.

## **Research Center for Biotechnology Defense**

- A long-term R&D effort to provide better defenses against biological weapons is of particularly high priority. Within 10 to 20 years, the danger of biological attacks will become increasingly difficult to cope with because
  1. the technology for making new types of biological agents is bound to proliferate, given the expanding (and legitimate) pharmaceutical and agricultural applications;
  2. dictatorships will find it easy to exploit this legitimate technology while they prevent international verification schemes (even with the best possible treaty controls) from turning up evidence that would be compelling enough to justify effective sanctions; and
  3. biological agents can easily be smuggled across international borders.

An effective way to ensure long-term funding and to impart a practical focus to this effort would be to establish a biotechnology and chemical defense center. This center could be colocated with an appropriate existing facility. For the emerging age of biotechnology, such a center should play a role comparable with that of the U.S. nuclear laboratories at the beginning of the nuclear age. The basic difference would be the shift to a defensive strategy.

# New Vulnerability to Mass Destruction Weapons

*We have begun to treat the threat of chemical and biological weapons use as a likely—and early—condition of future warfare. . . . Most ominous among these threats is the movement of the front line of the chemical and biological battlefield from foreign soil to the American homeland, which compels us to increase our domestic preparedness.*

—Secretary of Defense William S. Cohen  
*Washington Post*, November 26, 1997

The use of nuclear, chemical, or biological weapons against targets within the United States might occur in widely different circumstances. During the Cold War, the contingency that dominated U.S. strategy was that of a large-scale Soviet attack. Although deterring or responding to a deliberate nuclear attack from Russia (or China) is still an essential mission for our nuclear strategic forces, in the current world situation the threat of such a deliberate, massive nuclear attack is an implausible contingency. Instead, other contingencies have been justifiably receiving increased attention in recent years. In terms of the possible magnitude of destruction, these contingencies represent a vastly smaller threat; in terms of their likelihood, however, they now loom larger. This report addresses these “lesser” contingencies of the use of mass destruction weapons against targets within the United States. The important issue of air and missile defense, however, is not dealt with in this report because it has been addressed by a great many other studies.

For Department of Defense (DOD) planning purposes, the following four categories of possible nuclear, chemical, or biological attacks on U.S. territory should be distinguished:

1. A terrorist act planned and organized by people within the United States, with minimal or no support from abroad in providing technologies and equipment.
2. The launch of an armed nuclear missile or several missiles against target(s) in the United States caused by an unauthorized act or technical accident.
3. A terrorist act (or repeated acts) sponsored and technically supported by a foreign government or by foreign organizations hostile to the United States.
4. A single attack or repeated attacks with weapons of mass destruction (WMD) on targets within the United States, organized and technically supported by a hostile

country not for purposes that are normally associated with terrorism but as a strategy in support of an armed conflict with the United States.

Until a few years ago, DOD had not given serious consideration to the use of mass destruction weapons against the U.S. homeland, except for the threat of a Soviet nuclear attack. Now, DOD has training programs for the National Guard to assist the Federal Emergency Management Agency (FEMA), the Federal Bureau of Investigation (FBI), and state and local organizations in coping with the consequences of a terrorist use within U.S. territory of chemical weapons (CW) and biological weapons (BW), or perhaps even a nuclear weapon. In addition, DOD programs for protecting U.S. forces deployed overseas from chemical and biological weapons serve to develop defensive tactics, sensors, vaccines, protective suits, and other capabilities that might also be useful within the United States. However, the mission of protecting U.S. forces deployed overseas is more manageable than the mission of protecting the home territory: overseas bases and deployed military forces can be provided with a protective perimeter—barbed wire, sensors, and guard posts—but so far the means of surrounding a single U.S. city with a protective perimeter do not exist.

Several developments have recently led to greatly increased concern in the executive branch and in Congress about the danger that terrorists might use chemical, biological, or nuclear weapons within the United States.<sup>1</sup> The Clinton administration has initiated a range of programs and measures to cope with this new threat. Appropriately, priority is being placed on intelligence efforts, either to detect attempts overseas to smuggle such a weapon across America's open borders or to detect any group within the United States that might seek to manufacture a biological or chemical weapon. Timely detection helps to intercept or render harmless such attempts.

# The Need for a Defensive Strategy

During the past few years, U.S. defense planners have devoted a substantial analytic effort to the new technological, military, and political developments that have begun to threaten U.S. interests. Nonetheless, U.S. strategic theories and concepts from the Cold War era continue to exert a strong influence today. Even though this kind of thinking has lost much of its validity, it still infiltrates—frequently almost unnoticed—the work of the U.S. defense community. One pertinent example is the pervasive assumption that U.S. territory would essentially remain a sanctuary in all wars except a nuclear war with a major nuclear power (presumably Russia or China).

This assumption is as pervasive as it is hidden. It permeates the allocation of the defense budget, it accounts for the fact that until now there has been no commander in chief explicitly responsible for the defense of the U.S. homeland, and it explains the belittling of the wartime risk of homeland attacks that is reflected in the way the executive branch addresses the possible use of chemical, biological, or nuclear weapons within U.S. territory—as isolated terrorist acts (implicitly imagined as occurring in peacetime) that must be and can be managed by the Department of Justice, the FBI, and FEMA, with DOD providing backup disaster relief.

It is easy to recognize the historic origins of this assumption. The very idea of defending U.S. territory and the American people against attacks by WMD clashes with the theory of deterrence that has come to dominate U.S. nuclear strategy since the 1960s. At the beginning of the nuclear age, the United States pursued a mixed strategy that combined deterrence with defense; for example, in 1960 the United States spent more on strategic air defense than on nuclear retaliatory forces. But later, in response to the growing Soviet missile force, the United States began to rely exclusively on the threat of retaliation and negotiated the Anti-Ballistic Missile Treaty to “stabilize” a bipolar condition of mutual vulnerability to nuclear annihilation. According to this philosophy, it would be either destabilizing or pointless to maintain a capability of defending the U.S. homeland. It is argued that defenses would be destabilizing because they would undermine mutual deterrence, or pointless because in local wars (for example, Vietnam, Lebanon, or Panama) the enemy could not inflict significant damage on the homeland.

Even those most complacent about stable mutual deterrence must now recognize that this stability is meant to hold for a bipolar confrontation, not for a multiplicity of rogue states. And, although missiles and bombers are likely to invite retaliation

because they can be tracked from takeoff and thus provide the identity of the country that launched them, a smuggled weapon might not be traceable to the aggressor. Good intelligence, to be sure, might make it possible to destroy the weapon before it could be smuggled anywhere near its target in the United States, but without an effective homeland defense even our best possible intelligence capability is unlikely to provide useful warning. If the aggressor does not have to overcome multiple hurdles to reach the target, the attack becomes so undemanding in terms of preparations, levels of concealment, and number of collaborators that it will be impossible to detect. Many experts overlook the helpful symbiosis between defenses (which offer at best partial protection) and tactical intelligence (which is necessarily chancy); together, a defensive capability and intelligence can be much more effective than either alone.

A new defensive strategy against these mass destruction threats ought to exploit systematically the symbiosis between defenses and intelligence. The defenses either can be obstacles known and perhaps even visible to the perpetrators (visible x-ray scanners, checkpoints for vehicles, and so forth) or can be hidden sensors and disabling devices that are unknown to the perpetrators. The first variant will tend to increase the level of effort of a determined attacker and thus will provide greater visibility of the attack; the second variant will furnish leads about suspicious activities.

A defensive strategy must be balanced so that it will offer at least some protection against every relevant form of attack and delivery mode. An enemy that would choose to attack the U.S. homeland would obviously not select a frontal assault unless that enemy was willing to risk massive retaliation. Only Russia (and, later, perhaps China) has the nuclear forces that could effectively cripple the United States, and there is no military power in the world that could invade U.S. territory. Hence, by opting for an attack on the U.S. homeland, an enemy would be choosing to outflank the “central front.” The closest parallel in earlier wars might have been sabotage campaigns behind enemy lines; now, however, the weapons could be immensely more destructive and could therefore achieve a decisive psychological and political impact.

Ballistic missiles are regarded as the fastest and most reliable delivery means for nuclear and biological weapons. But ballistic missiles come with a “return address” (even if launched from a submarine, for the submarine might be tracked) and cannot be used to pre-position a weapon. Ballistic missile defenses are important for closing off one particular avenue of attack; but for the type of contingencies addressed here, they have to be complemented by an array of other defensive measures.

A vastly improved U.S. capability to defend friendly territory against clandestinely introduced mass destruction weapons is also important for assisting U.S. allies. In coalition warfare against an enemy that could credibly threaten such attacks, the United States would lose the support of key allies if they had to confront this threat without any prospect of establishing an effective defense.

Future biological warfare agents provide a further reason why the United States ought to shift toward a more defensive strategy because of the technical difficulties of coping with them. In biotechnology, scientific and technological advances cannot be kept from spreading to other countries because such advances are integral to the advancement of pharmacology. And in any closed, hostile nation, the misuse of this

medical technology to create highly lethal weapons could not be effectively verified, much less prevented. Also, the smuggling of BW agents across national borders is much harder to detect than the smuggling of nuclear weapons. Indeed, for many important contingencies, biological agents would be impossible to detect. This prospect makes it vitally important to mount a vigorous R&D effort to develop defensive technologies (see the subsection on page 14 that proposes a research center).

# Contingencies That Call for a Leading DOD Role

The planning and preparations by the administration so far have focused on terrorist scenarios, that is to say, on those contingencies where foreign or domestic terrorist groups would use, or plan to use, a weapon of mass destruction within the U.S. homeland. Lead responsibility for such contingencies has been given to the Department of Justice and the FBI, with FEMA having a responsibility to assist local authorities in responding to a destructive attack. DOD would provide assistance for the remedial response effort—if called for. To this end, training for the National Guard was started in 1997. In the event of foreign support for such a terrorist act, DOD might have a lead role in interdiction efforts outside of the United States; and if it came to a military retaliatory strike, Defense would likely be the lead agency.

Secretary of Defense William S. Cohen's statement, quoted on page 4 of this report, properly envisages a different type of contingency, namely the use of mass destruction weapons against the U.S. homeland as an enemy strategy that the United States might have to cope with in a future war. To understand this kind of threat it is important to expect ambiguities about the scope of the enemy attacks and perhaps even the identity of the enemy. For example, if U.S. forces again had to fight Iraq, another nation or a terrorist organization in the region might attack a target within the United States with a mass destruction weapon. The perpetrators of such an attack might have the objective of assisting Iraq (if Iraq is their secret ally) or of provoking a devastating U.S. retaliation against Iraq (if Iraq is their regional adversary). The convergence and interaction of ambiguously linked hostile activities can take many forms. U.S. planning and exercises need to prepare for a wide range of ambiguities and a variety of possible enemy coalitions and deceptive maneuvers.

It seems unlikely that the U.S. government could adequately respond to this type of contingency if the Defense Department was given merely a supporting role, leaving the Justice Department as the lead agency. Only the armed services have the managerial and logistical capabilities to mount the all-out defensive effort called for by the enormity of these threat contingencies. It stands to reason that we, as Americans, would expect and demand that our armed forces defend our own homeland against attacks worse than Pearl Harbor. Indeed, it would seem politically unacceptable for the president to let the attorney general and the director of the FBI be in charge of defending the nation, with the National Guard and perhaps some specialized units of the army and marine corps merely helping with first aid and cleanup.

Governments planners have raised the question of whether the United States has in place adequate legal authority that enables the military to defend against or deter—through defensive measures—a coordinated attack on U.S. territory that makes use of WMD. Underlying this concern is the belief that inadequate or insufficiently understood legal authorities for a military role in homeland defense against such a threat could materially impair that role, thus posing significant national security risks and endangering countless lives.

Preliminary efforts to answer this question have indeed revealed misperceptions and uncertainty regarding the lawful role of the military in preparing for and responding to such a WMD attack. It is clear that the military has the duty and the inherent power subject to constitutional rights of individuals to defend this nation. The task in this instance is to ensure that the laws governing the domestic activities of the military are adequate for the contingencies contemplated and evident to those whose responsibility it is to plan and prepare for a successful homeland defense. The section, *Legal Authority for a Leading DOD Role*, on page 16 gives a brief overview of these legal issues, and a follow-up CSIS study is being undertaken to offer a thorough legal analysis.

Where, precisely, should the line be drawn between contingencies involving mass destruction threats (or use) against the U.S. homeland for which the Department of Justice ought to have the lead responsibility and contingencies for which the Department of Defense ought to take the lead? As shown on page 9, it is possible to give hypothetical examples that fall to either one side or the other of this dividing line. But it would not be useful to define this line with too much specificity. The political–military environment at the time the threat became imminent would be a key determinant. If the homeland threat seems to be linked to a foreign enemy against which the United States is deploying forces or engaging in combat, lead responsibility for homeland defense would probably become primarily a military responsibility. Or if there was a danger of a devastating second attack after a first use of a mass destruction weapon within the United States, it seems likely the American people would demand that the military be fully committed to defend the homeland. In any event, in a real life situation, the president and Congress would make the decision regarding the DOD role.

# Long-Term R&D Needs

Although a defensive strategy against these new threats is strategically necessary, it is difficult to make the case that today it would be effective against a skillfully operating enemy. The reason for this gloomy forecast is the lack of tools across a range of circumstances for detecting, interdicting, or rendering harmless the weapons. This need not be a permanent condition. The competition between defense and offense in these contingencies does not favor the offense to the same extent it did for nuclear weapons during the Cold War. The potential adversaries do not have the scientific–industrial capability that the Soviet Union was able to bring to bear to negate U.S. defensive technologies against nuclear attack. And the very real danger of clandestine tactics that bypass our defenses is mitigated by the fact that we control the territory and can prepare countermeasures.

A long-term R&D effort that concentrates on defenses therefore holds promise. Indeed, it is essential to raise the threshold for an enemy attack to succeed: first, to improve the chances for useful intelligence and, second, to shrink the number of potential enemy nations and organizations that might acquire the wherewithal to overcome our defenses. If every hostile clan, failed state, and petty dictator can mount a biological or nuclear attack on targets within the United States, the day will come when this strategy will be employed.

Gaming and exercises can serve to identify the type of military operations that would be desirable in a crisis to forestall an attack. And a clearer idea of the military operations or missions will help identify the equipment that ought to be developed. The military will likely be tasked with:

- Monitoring crossings of the U.S. border with sensors to detect nuclear devices; perhaps also temporarily closing parts of the border to all traffic (in cooperation with the Department of Justice),
- Closing certain ports, reinforcing the U.S. Coast Guard, and monitoring approaching sea traffic with special sensors,
- Interdicting all unauthorized air traffic,
- Protecting the perimeter of key cities by checking ground traffic and installing and operating sensor networks around cities or key facilities.

## Importance of a Surge Capability

Until recently, U.S. military planners who focused on potential enemies other than the Soviet Union could safely assume that the U.S. homeland would essentially remain a sanctuary, free of significant military attacks. In planning U.S. military capabilities for the next 10 or 20 years, however, it would not be responsible to rely on this assumption. In particular, defensive capabilities will be needed to prevent or cope with the introduction of mass destruction weapons into U.S. territory. Delivery by ballistic missiles may not be the tactic that a medium-size enemy would choose. More likely, smuggling such weapons across the U.S. border by some clandestine method would be the preferred approach.

Two types of obstacles obstruct progress on an effective defensive posture against this threat. One is the scientific and technical difficulty of designing systems that would work—that would detect attempted smuggling of biological agents, disarm a booby-trapped nuclear device, clean an urban area of a persistent chemical agent, and so on. The other obstacle is the high hurdle that has to be surmounted to reach a meaningful level of effort, given the uncertainty and novelty of the threat. A substantial investment in manpower and acquisition funds would be required for the purchase, installation, and operation of defensive systems that could provide meaningful protection for the whole United States. Given the present opacity of the threat of homeland attacks (especially with smuggled weapons) as well as the uncertainty of the form such attacks might take, the necessary support in the executive branch and in Congress seems unlikely.

On the other hand, the body politic and public opinion would clamor for all possible protective measures as soon as a devastating attack on a target within the United States had occurred or even if the threat appeared imminent. In various plausible contingencies the risk of further attacks might loom large. Indeed, if additional mass destruction weapons were used against U.S. cities, the very survival of the United States as a functioning society and politically cohesive entity would be at stake. Because of this dilemma—the likelihood that the costs of building a protective system beforehand would be deemed unacceptable vs. the absolutely compelling need for defenses once an attack had occurred—preparations are needed for a rapid deployment of extensive defensive measures in the event of a crisis. Hence, a vigorous R&D program, including prototyping, as well as advance preparation for procurement in large quantities are essential.

When these R&D developments approach completion, their development will enable—and their effective use would require—procurement and mobilization of operational resources much greater than those currently devoted to countering domestic terrorism. Indeed, the R&D program is not likely to result in adequate technical capabilities unless it is based on the assumption that much larger procurement and operational resources will become available if and when the threat appears more imminent than today or after some kind of WMD attack actually occurs on a target within the United States. Preparations for mobilization should therefore be an integral part of a comprehensive national program and ought to start now, even though current protection technologies are inadequate. Only DOD has the experience and resources to support the kinds of R&D and follow-on preparations for

mobilization in time of crisis. Of course, many departments and agencies must work together in a national program.

Three main elements of the R&D program are needed to achieve these improved capabilities: information technology, sensor technology, and biotechnology. All three are relevant to threat detection and prevention as well as to protection and amelioration, in varying degrees depending on the type of threat. Information technology and biotechnology are the most active areas in technology development today, and sensor technology is not far behind.

**Information technology** has broad application. One general aspect of information technology is the ability to manipulate efficiently immense quantities of data and to extract meaning from them. These techniques can be applied (1) to intelligence data (and much information that is not strictly intelligence) to identify and characterize threat operations, (2) to sensor data to improve detection and identification of weapons and weapons materials and agents, in part by more effective use of extensive networks of large numbers of advanced sensors of many types, and (3) in biotechnology to identify and sort the large number of potential bioengineered agents and to develop protective strategies against them (vaccines and preventive medicines).

**Sensor technology** can be improved dramatically by an R&D program for chemical, biological, and nuclear detection devices. The prospect exists that advanced radiation sensors and methods for using them in large arrays will be able to detect the presence or transit of nuclear devices or nuclear material over city-size areas. Surge deployments of such capabilities eventually could cover many cities as well as ports, airports, and other points of entry. A goal for R&D regarding biological sensors, realizable in perhaps a decade, is near-real-time detection and identification of a large number of biological agents at distances of several kilometers and, for some applications, in packages small enough to be carried on small platforms such as micro-UAVs (unmanned air vehicles) or robots. Similar capabilities for chemical-agent sensors are nearer at hand.

R&D to exploit emerging capabilities to identify accurately the chemical or biological nature of extremely small samples of material (in some cases, just a few molecules) can be applied broadly, not only for sensors but also for forensics. Small samples collected by remote autonomous platforms or clandestine means can be used to identify, for warning and interdiction, the existence of threat operations as well as the nature of the threat agent so that defense strategies can be developed and, for example, threat-specific vaccines can be engineered.

**Biotechnology** R&D is needed for enhancing defenses against a broad range of biological threats, including anticipating future bioengineered threat agents and strategies; developing sensors and multiagent vaccines; and providing affordable collective protection in buildings and residences, advanced decontamination technologies, and methods of diagnosis and treatment of agent-induced illness. To this end it is essential to engage more effectively the civil U.S. biotechnology, pharmaceutical, and medical communities in the research program to prevent and protect against biological threats. A new institution to sponsor this effort will probably be required (see the next subsection).

The R&D program can also serve certain civil defense measures. Critical public buildings can be given protection against chemical and biological agents with special sensors, over-pressure systems, and so forth. Over several years, significant protection can be retrofitted into existing structures and augmented by expedient measures to be taken on warning. Preparations can also be made for rapid training programs that will enable the public to make best use of protective measures.

## **Research Center for Biotechnology and Chemical Defense**

Compared with any other country, the United States has by far the greatest capability in biotechnology research, especially given the strong presence in the United States of U.S.- and foreign-owned pharmaceutical-industry research facilities. This scientific field is much in flux, and it makes sense therefore to undertake a long-term R&D effort for defenses against BW and CW weapons that could put the United States into a defense-dominant position. This would be of enormous value in overcoming a serious and growing vulnerability of the United States and its allies to BW and CW and chemical and biological warfare (CBW) terrorism. It is likely that the results from such an R&D program would also have public health benefits against emerging diseases.

On January 22, 1999, President Clinton proposed new funding for an R&D program to defend against biological weapons. This program would be centered in the Department of Health and Human Services and seek to develop new vaccines, medicines, and diagnostic tools. However, to give some focus to this effort, a dedicated center would be useful so that the work will not be a scattered collection of grants and projects. Such a center would also help to ensure the essential long-term orientation and long-term funding for this R&D program. Long term here means 10 to 20 years and probably beyond.

It will be essential for the talent in the pharmaceutical industry to make contributions. To enable and induce the industry to give support, special financial incentives would be needed and certain legal arrangements (tort protection, patent protection), which Congress would have to legislate, might be required. The center would also need flexible contract authority.

An important mission for the biotechnology and chemical defense center will be the development of practical applications for promising findings that emerge from the basic research projects sponsored by the National Institutes of Health and universities. The center would design defensive systems that properly make use of new technologies and new pharmaceuticals for the large-scale contingencies that must be managed in an effective homeland defense. It could also conduct analyses and design exercises to perfect operational plans for treating the at-risk population with emergency vaccinations or to disseminate and administer newly developed antibiotics and other medicines. The work of this proposed center could also make contributions to the problem of emerging infections.<sup>2</sup> The following examples illustrate some of the tasks that this center might work on or coordinate among other government elements and contractors.<sup>3</sup>

- Promote and participate in the long-term development of new vaccines and antidotes as well as multipurpose antiviral and antibacterial treatments;
- Set up formal communications and standard operating procedure for local medical and emergency-service units for warning of potential CBW threats and reporting possible attacks;
- Develop lighter, cheaper, and more effective suits and equipment for operating in a CBW environment;
- Develop light and effective monitoring and detection equipment for use by first responders, doctors, and emergency management personnel;
- Develop techniques and equipment for decontaminating large groups of people quickly and efficiently;
- Increase education efforts among the medical community and the general public about CBW threats and responses.

# Legal Authority for a Leading DOD Role

Under the Constitution, the president as commander in chief has authority to use the armed forces to resist attacks against the United States, subject to restrictions imposed by law. The boundaries of such authority are ambiguous in situations where defense, law enforcement, and protection of civil liberties overlap. These contingencies straddle the divides among national security, law enforcement, and emergency management and, as such, bring into play a host of legal authorities that variously permit and prohibit different kinds of conduct by the military under different circumstances.<sup>4</sup> In most instances, government planning to date has cast the military in a supporting role vis-à-vis civil and law enforcement authorities.

Whether this view of the military's role and the legal authorities that govern its actions are appropriate or adequate given the existing threat should be questioned for several reasons.

First, some military planners, at various levels, frequently refer to firm limitations imposed by law—such as the Posse Comitatus Act—that inhibit military activities related to homeland defense. Other commentators stress a range of uncertainties about the scope of current laws. They have argued that authorities governing the military's role in domestic operations are a complex mix of outdated laws that do not provide the flexibility necessary for an effective military response against today's threat.<sup>5</sup> One commentator noted:

These [Posse Comitatus Act] constraints may have been appropriate in the late 1800s, but in a world where non-state groups have access to weapons of mass destruction...they could prove to be counterproductive....

...Outdated and inflexible American legislation has produced a patchwork consisting of constitutional and statutory exceptions so that the realities of domestic operations can be performed. Examples include the [Robert T. Stafford Act Disaster and Emergency Assistance Act], ...contingency planning for U.S. Army assistance in incidents involving use of chemical and biological weapons of mass destruction on U.S. soil, and various methods to facilitate cooperation between the FBI and the U.S. Army in anti-terrorism. The potential consequences of this approach include a convoluted chain

of command and control structure, increased response time, and continuity-of-operations problems; it also leaves the federal response vulnerable to exploitation by the adversary.<sup>6</sup>

To the extent that such limitations do impede adequate preparations for or responses to a WMD attack, it should be recognized that they are merely legal bars that could be corrected by additional legislation, if necessary.

Second, some of the confusion regarding the governing legal authorities reflects the multitude of situations in which a military role may be required. The military's role in homeland defense is regulated by an overlapping mix of constitutional, statutory, judicial, regulatory, and other executive-branch authority. For example, different laws may apply depending on whether (a) there is an incident involving a nuclear, biological, or chemical weapon, (b) efforts are undertaken to apprehend the perpetrators or contain the consequences, (c) an emergency has been declared by a governor or the president, (d) an act of war has been committed against the United States, (e) martial law has been declared, or (e) Congress has declared war. Similarly, different laws may apply depending on whether the military is fulfilling its traditional functions or is acting in assistance to law enforcement officials.

Third, often the laws that govern emergencies, such as the National Emergencies Act, do not themselves authorize conduct by the military. Instead, such laws establish a set of conditions under which DOD may exercise authorities granted under a myriad of other, more specific laws. These other laws were themselves created for other purposes and may not contain the precise authorities needed for the kinds of actions required in response to an attack with weapons of mass destruction. Although the major authorities are limited in number, it may be said without exaggeration that the number of supporting laws, regulations, directives, precedents, and constitutional provisions involved in determining whether the military may undertake the likely range of actions needed to respond to enemy strategies for WMD attack might, when taken together, run well into the scores or even hundreds.

Fourth, recent laws passed to focus on WMD were designed primarily to increase DOD assistance to local and law enforcement efforts to respond to a limited terrorist attack. To the extent that legislators have focused on homeland defense, they have seen the problem primarily in such terms. These laws, therefore, need to be examined in light of the broad-based attack that is a growing defense concern. Moreover, the terms of laws governing nuclear, chemical, and biological threats differ in ways that may make a response to some more difficult than others.

Finally, a number of the laws or authorities that might be relied on for homeland defense either have not been tested under the circumstances involved here or have been tested in court only under limited circumstances, and usually decades ago. This is not surprising given that there has been only limited need for homeland defense in the past century or more.

The potential threat to the U.S. homeland makes it important adequately to address the above concerns. Inadequate or insufficiently understood legal authorities for a military role in homeland defense against a broad-based WMD challenge pose significant national security risks. They may, for example, delay, complicate, or even prevent defensive measures within or in the immediate vicinity of the 50 states and

the District of Columbia, measures that would save lives or reduce damage before, during, or after an attack.

The president and the military may act only where they have been granted authority by the Constitution or Congress. Military officers or agency officials might be reluctant to take action with inadequate or unclear legal authority. Local officials at the state, county, or municipal level who are reluctant in a crisis to relinquish local assets for regional or national purposes may exploit unclear authorities to delay action. Emergency legal challenges could be launched by local or private parties. Such delays, multiplied and cascading through the system, could impair or defeat effective defenses.

The absence of clear legal authority, if not addressed well before a crisis, also may become known through public debate during a crisis. This can have several adverse effects. First, it could tempt an aggressor whereas clear lines of authority and the appearance of effective responses might help to deter one. Second, it could increase domestic concerns, possibly contributing to a panic on the eve of an expected attack or in the wake of an actual one. Third, public doubts about the effectiveness of our defenses will likely lead to increased public or congressional resistance to conducting a forceful foreign policy that might provoke a potential aggressor. For example, if the public had widely believed in 1990 that Saddam Hussein had had an effective BW capability and that we were not prepared to handle an attack, Congress might well have determined that the risks of Desert Shield or Desert Storm were not worth the benefits. Efforts to dissuade the aggressor or persuade allies to join us would be more difficult in the midst of such a debate. Thus, even if the ultimate outcome of a congressional vote on involvement were not different, the resulting lack of resolution in our debate would itself become a factor in the crisis, undermining our position with aggressors and allies alike.

Moreover and perhaps most important, inadequate or insufficiently understood legal authorities might obfuscate responsibilities held by executive branch agencies and affect their allocations of resources and long-term R&D. Many observers believe that only DOD has the skills and resources to organize the necessary research, development, and procurement efforts and to handle a coordinated response to an attack that involves WMD. These observers note that homeland defense related to a war or a warlike situation is properly a DOD concern. However, it is also believed that DOD, through misgivings about its lawful role or for reasons related to its own priorities, has not satisfactorily addressed its role in responding to or inhibiting (other than through the threat of a retaliatory strike) a massive attack. If so, a clearer understanding in DOD and the body politic of legal requirements for homeland defense may help bring to bear the necessary resources for undertaking research, acquiring capabilities, and training and planning for successful defensive operations.

The risks described above could be alleviated if legal authorities are better understood or if necessary changes to the law are identified and enacted. To this end, CSIS has undertaken a study of the legal aspects of the military's role in homeland defense (expected to be completed in mid-1999).

# Notes

1. The uncertain control over Russia's nuclear materials (and perhaps its tactical nuclear weapons) creates a risk of the theft by criminal organizations of nuclear weapons on behalf of some rogue state or perhaps a drug cartel. The spread of knowledge and technologies for the manufacture of chemical and biological weapons makes it possible that states and organizations hostile to the United States could acquire technologically advanced CW or BW capability.
2. Polly Harrison and Joshua Lederberg, *Orphans and Incentives: Developing Technologies to Address Emerging Infections* (Washington, D.C.: National Academy Press, 1997).
3. These missions have been developed from the conclusions and recommendations of the Institute of Medicine's *Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response* (Washington, D.C.: National Academy of Sciences, 1999).
4. Richard A. Falkenrath, Robert D. Newman, and Bradley A. Thayer, *America's Achilles' Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack* (Cambridge, Mass.: MIT Press, 1998), xxi.
5. See, for example, Sean M. Maloney, "Domestic Operations: The Canadian Approach," *Parameters* (Autumn 1997): 135–152, which contrasts "outdated and inflexible" and "patchwork" U.S. legislation with the Canadian approach to defense against weapons of mass destruction; Chris Seiple, "Consequence Management: Domestic Response to Weapons of Mass Destruction," *Parameters* (Autumn 1997): 119–134, which notes that the Posse Comitatus Act should be examined in light of the threat of terrorist attacks with weapons of mass destruction; and Charles L. Mercier Jr., "Terrorists, WMD, and the U.S. Army Reserve," *Parameters* (Autumn 1997): 98–118, which suggests that Stafford Act constraints on the military's rapid response to terrorist attacks should be examined.
6. Maloney, "Domestic Operations."

# References and Related Studies

The past two years have seen rapid growth in the number of studies and reports done by or for the U.S. government that examine the threat posed by isolated attacks with nuclear, chemical, or biological weapons within the United States. Congress, the Department of Defense, and other executive agencies such as the FBI and FEMA moved to examine what would need to be done against this threat.

The resulting studies, exercises, and programs can be divided into two main groups. The first includes threat-assessment studies that are primarily technical examinations of weapons proliferation. They look at the scientific and technological factors in the R&D and the production of these weapons in order to identify possible threats and recommend courses of action to slow or stop proliferation. The second group looks at the operational concerns of incident investigation and consequence management.

## Threat Assessments

The threat assessments have been issued primarily by DOD, Department of Energy, intelligence agencies, and by the research arms of Congress. As stated above, their concern is the issues involved in WMD proliferation, keeping the technology and knowledge out of the wrong hands before a threat can develop.

The Defense Science Board's report of the task force on transnational threats (*DoD Responses to Transnational Threats* [Washington, D.C.: Office of the Under Secretary of Defense for Acquisition & Technology, October 1997]) has an excellent threat section on pages 13–22. This report is also clear on the indeterminacy of the threat's likelihood. Referring to a nuclear device that “could be detonated in a city, or a military base in the United States...”, the report concludes—correctly—that “there is no way to assign a likelihood or probability to such an event” (p. 42). *Transforming Defense: National Security in the 21st Century* (Arlington, Va.: National Defense Panel, December 1997), the report of the congressionally mandated National Defense Panel, contains three pages on the new threat to the U.S. homeland. The danger of clandestine delivery is addressed by Richard A. Falkenrath, Robert D. Newman, and Bradley A. Thayer in *America's Achilles' Heel*, published by MIT Press in 1998.

The Department of Defense has produced many of these studies. *Chem-Bio 2010: Assessment of the Impact of Chem/Bio Weapons on Joint Operations in 2010*, written in 1997, is one such report that looks at WMD and the technical effects of their use on operations. DOD also produces an annual report, *Proliferation: Threat and Response*, that catalogs the proliferation attempts of various nations around the world and active or planned DOD programs to counter or limit them. The Defense Intelligence Agency (DIA) and the Central Intelligence Agency (CIA) also examine proliferation threats. The Quadrennial Defense Review Panel and the National Defense Panel also looked briefly at threats from WMD proliferation.

The Senate Committee on Governmental Affairs produced *The Proliferation Primer* in January of 1998. This document, based on a series of hearings held by the Subcommittee on International Security, Proliferation and Federal Services, is meant as an informational document on the subject of proliferation. Topics covered in the report include the proliferation status of various threat nations and their actions regarding the proliferation of WMD and ballistic missile technology to other parties, intelligence documents relating to technology sale and transfer, and U.S. laws and statutes regarding counterproliferation.

The new Center for Counterproliferation Research at the National Defense University (NDU) has produced a number of studies examining the threat that WMD pose to military operations and to the homeland. *The NBC Threat in 2025: Concepts and Strategies for Adversarial Use of Nuclear, Biological, and Chemical Weapons* (Washington, D.C.: NDU, 1997) and *The Effects of Chemical and Biological Weapons on Operations: What We Know and Don't Know* (Washington, D.C.: NDU, 1997) are two threat reports that try to establish how WMD might be used in conflict with a nation or nonstate actor. More recently, Seth Carus wrote *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents in the 20th Century* (Washington, D.C.: NDU, forthcoming) that catalogs all the uses and threatened uses of bioweapons (excluding open warfare) in the past century.

CSIS projects have put great stress on the challenges of terrorism and WMD proliferation. The CSIS project on global organized crime, headed by William Webster and Arnaud de Borchgrave, has produced a number of reports, including *The Nuclear Black Market* (Washington, D.C.: CSIS, 1996) that led to a number of ongoing risk-reduction initiatives and *Wild Atom* (Washington, D.C.: CSIS, 1998), a war-game attempt to smuggle a nuclear device into the United States.

## Operational Reports

Most of the reports that deal with biological or chemical attacks against the homeland deal with investigations and consequence management operations. Written primarily by DOD organizations, FEMA, and the FBI, the majority of these reports can be said to be tactical manuals. They deal with the basic operations of investigation and consequence management: Who has jurisdiction? What equipment is necessary for a decontamination unit that responds to a WMD incident? What training should be given to first responders? Which DOD office has primary liaison responsibility with the civil authorities?

The DOD report to Congress, *Domestic Preparedness Program in the Defense Against Weapons of Mass Destruction*, released in May 1997, is the basic report on DOD support to civil authorities in the event of a WMD incident. The report covers current DOD programs and responsibilities relating to attacks and lists information, equipment, and personnel that would be released to the civil authorities in the event of an incident. The report also covers those programs—in operation or planned—in which DOD nuclear, chemical, and biological warfare specialists train civil first responders such as fire, police, and medical service personnel in operations such as WMD triage, decontamination, and contamination reconnaissance. The document also briefly covers the legal aspects of DOD involvement in an otherwise nonmilitary operation.

In January 1998, DOD released a report covering reserve and National Guard involvement in WMD incident response: *Integrating National Guard and Reserve Component Support for Response to Attacks Using Weapons of Mass Destruction*, an overview of the assets the reserves and guard have available to aid in a WMD incident. Although the report looks at legal and organizational issues in appendixes, most of it addresses how the guard and reserves can be organized to back up the first responders during a WMD incident. The guard and reserves could have both permanent and reserve units to perform such functions as detection and assessment; nuclear, biological, and chemical (NBC) reconnaissance; decontamination; medical triage and treatment; stress management; security; mortuary affairs; transportation; communications; and engineering. The National Guard could also take the lead in liaison between DOD and the local civil authorities.

There are many other reports regarding operational concerns. *An Assessment of Federal Consequence Management Capabilities for Response to Nuclear, Biological, or Chemical (NBC) Terrorism* was reported to the president by the Catastrophic Disaster Response Group in February 1997. Congress and FEMA reported on *The Role of the National Guard in Emergency Preparedness and Response for the United States* in January 1997. Other reports of similar contents include *NBC Terrorism Response Focus Group for Local Government* (October 1996), *National Governor's Association Workshop with Interagency Partners* (September 1996), the FEMA City Representatives Meeting series (1996), *FEMA/FBI Report to Congress* (January 1997), the DOD Focus Group Meeting series (February 1997), and the *DOD/DOE Report to Congress* (April 1996).

In the area of defensive R&D, in early 1999 the Institute of Medicine at the National Academy of Sciences will publish *Chemical and Biological Terrorism: Research and Development to Improve Civilian Medical Response*. Produced by a committee of public health officials, physicians, biologists, emergency management experts, and government representatives, the report examines the R&D needed to develop techniques and equipment required by the medical community before, during, and after a WMD incident. It is the very type of R&D advocated by this report that the suggested research center for biotechnology and chemical defense would be in charge of financing and coordinating. A similar study was done earlier by Polly Harrison and Joshua Lederberg for the Institute of Medicine at the National Academy of Sciences. *Orphans and Incentives: Developing Technologies to Address Emerging Infections* (Washington, D.C.: National Academy Press, 1997) looks at taking on emerging natural

diseases but also has a lot to offer about the formation of a biological and chemical defense center.

A number of nongovernmental and academic organizations have also produced books and studies relating to defense and consequence management in homeland defense. Chief among these has been the Universities Study Group on Catastrophic Terrorism, run out of Harvard University's Kennedy School of Government. The group, made up of prominent academics and former government officials, looked at how the United States should prepare for major terrorist attacks, including the use of WMD. The group's findings will be published in report form by Stanford University, and distillations can be found in "Catastrophic Terrorism" by Ashton Carter, John Deutch, and Philip Zelikow in the November/December 1998 issue of *Foreign Affairs* and also in *Preventive Defense: An American Security Strategy for the 21st Century* (Palo Alto, Calif.: Stanford University, forthcoming). Recent academic books on the topic include *America's Achilles' Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack* by Richard Falkenrath et al. (Cambridge, Mass.: MIT Press, 1998) and Leonard Cole's *The Eleventh Plague: The Politics of Biological and Chemical Warfare* (New York: W. H. Freeman, 1997).

# About the Author

Before he joined CSIS, Fred C. Iklé was under secretary of defense for policy in the Reagan administration, and from 1973 to 1977 he served as director of the U.S. Arms Control and Disarmament Agency. He also serves as a director of the National Endowment for Democracy and is the author of several books and numerous articles on defense, foreign policy, and arms control. He has received the highest civilian award of the Department of Defense, the Distinguished Public Service Medal, and in 1988 he was awarded the Bronze Palm.