Cato Policy Analysis No. 306 May 5, 1998

Policy Analysis

PROTECTING THE HOMELAND

The Best Defense Is to Give No Offense

by Ivan Eland
Ivan Eland is director of defense policy studies at the Cato Institute.

Executive Summary

Recently, several government reports have emphasized the need for increased attention to the defense of the American homeland. The proliferation of technology for creating weapons of mass terror and conducting chemical, biological, nuclear, and information warfare has reawakened interest in protecting the homeland.

A study completed for the U.S. Department of Defense notes that historical data show a strong correlation between U.S. involvement in international situations and terrorist attacks against the United States. Attacks by terrorist groups could now be catastrophic for the American homeland. Terrorists can obtain the technology for weapons of mass terror and will have fewer qualms about using them to cause massive casualties. The assistant secretary of defense for reserve affairs maintains that such catastrophic attacks are almost certain to occur. It will be extremely difficult to deter, prevent, detect, or mitigate them.

As a result, even the weakest terrorist group can cause massive destruction in the homeland of a superpower. Although the Cold War ended nearly a decade ago, U.S. foreign policy has remained on autopilot. The United States continues to intervene militarily in conflicts all over the globe that are irrelevant to American vital interests. To satisfy what should be the first priority of any security policy--protecting the homeland and its people--the United States should adopt a policy of military restraint. That policy entails intervening only as a last resort when truly vital interests are at stake. To paraphrase Anthony Zinni, the commander of U.S. forces in the Middle East, the United States should avoid making enemies but should not be kind to those that arise.

Introduction

In its December 1997 report, the National Defense Panel--a group of retired generals and civilian defense experts created by Congress to develop alternatives to the Department of Defense's plan--called for a reemphasis on defending the American homeland. (Surprisingly, because the U.S. government has concentrated its efforts on defending other nations and even continents from global communism and other perceived threats, the mission of defending the territory and people of the United States has not been prominent since the 1950s. Subsequently, civil defense plans withered on the vine as the realization grew that a nuclear war would be so devastating to American society that attempts to minimize the effects were futile.)

The panel argued that the primary reason for increased emphasis on homeland defense is the change, in both type and degree, in the threats to the United States. In addition to maintaining its ability to deter a strategic nuclear attack, the United States must defend against terrorism, information warfare, weapons of mass destruction (WMD), ballistic and cruise missiles, and other transnational threats.[1]

The threat to the American homeland is being magnified greatly by proliferating technologies associated with WMD (chemical, biological, and nuclear weapons). According to a statement made the previous month by the secretary of defense and quoted in the Department of Defense's November 1997 report, Proliferation: Threat and Response:

> With advanced technology and a smaller world of porous borders, the ability to unleash mass sickness, death, and destruction today has reached a far greater order of magnitude. A lone madman or nest of fanatics with a bottle of chemicals, a batch of plague-inducing bacteria, or a crude nuclear bomb can threaten or kill tens of thousands of people in a single act of malevolence.
>
> These are not far-off or far-fetched scenarios. They are real--here and now. WMD already have spread into new hands. As the new millennium approaches, the United States faces a heightened prospect that regional aggressors, third-rate armies, terrorist cells, and even religious cults will wield disproportionate power by using--or even threatening to use--nuclear, biological, or chemical weapons against our troops in the field and our people at home.
>
> America's military superiority cannot shield us completely from this threat. Indeed, a paradox of the new strategic environment is that American military superiority actually increases the threat of nuclear, biological, and chemical attack against us by creating incentives for

> adversaries to challenge us asymmetrically. These weapons may be used as tools of terrorism against the American people.[2]

Although America's military superiority contributes to the increased likelihood of a terrorist attack by nuclear, biological, or chemical means--or even an attack against U.S. information systems or other critical infrastructure--it is the interventionist U.S. foreign policy that our military carries out that is the real culprit. That point was acknowledged in the Defense Science Board study for the undersecretary of defense for acquisition and technology.

> As part of its global superpower position, the United States is called upon frequently to respond to international causes and deploy forces around the world. America's position in the world invites attack simply because of its presence. Historical data show a strong correlation between U.S. involvement in international situations and an increase in terrorist attacks against the United States. In addition, the military asymmetry that denies nation states the ability to engage in overt attacks against the United States drives the use of transnational actors.[3]

The Defense Science Board is not alone in concluding that a relationship exists between U.S. intervention abroad and terrorism. More important, the terrorists themselves and those who lend them support make the connection. After the bombing of the American military barracks in Dhahran, Mohammed Masari, the London-based Saudi exile who advocates democracy for Saudi Arabia, told BBC radio that foreign troops in his country were "legitimate targets" and that the United States should anticipate future acts of retaliation as long as its military remains in the kingdom propping up Saudi rulers.[4] Another Saudi, Osama bin Laden--who seeks to overthrow the Saudi government and is related by marriage to Mohammed Jamal Khalifa, a recruiter of Islamic extremists in the Philippines--asserts that "Muslims burn with anger at America." The wealthy Saudi's anti-Americanism and financing of terrorism are motivated by his perception that American assistance to Saudi Arabia against Iraq in the Gulf War was an act against Arabs. Such American intervention can spur even normally moderate groups to threaten terrorist acts. Jordan's lower house of parliament passed a resolution encouraging "all the Arab and Islamic nations to strike at American interests and the interests of those nations participating in the aggression against Iraq."[5]

Terrorists and religious cults have an obsession with the United States because of its superpower status and behavior. The beliefs of the group Aum Shinrikyo--the Japanese religious cult that perpetrated the most unnerving terrorist act to date (attacking the Tokyo subway with poison gas)--are illustrative. Aum Shinrikyo prophesied an Armageddon-type conflict between Japan and the United States in the last years of this century. To hasten it, the group believed the use of biological and chemical weapons was necessary.[6] It is noteworthy that the group chose the United States as Japan's perceived

adversary instead of China, Russia, or any other more likely potential enemy. Given its beliefs and contorted logic, the group could have just as easily chosen a target in the United States instead of Japan.

The best summary of the current state of affairs was made by Matthew Meselson, a geneticist at Harvard and co-publisher of the journal The CBW Conventions Bulletin, which tracks chemical and biological arms. He states, "The best protection would be if we didn't have any angry people or countries in the world."[7]

Logically, then, to avoid inflaming such groups and nations unnecessarily, the United States should intervene overseas only when its vital interests are at stake. Since the end of the Cold War, however, the United States has never clearly defined its vital interests. The U.S. military has been asked to intervene anywhere and everywhere for a bewildering array of purposes. Those numerous interventions--for example, in Somalia, Haiti, and Bosnia--have nothing to do with America's national security. Such a casually interventionist foreign policy only provokes hostility from factions or groups within other countries.

A terrorist attack with WMD--almost impossible to deter, prevent, or mitigate--against a target in the United States could make the World Trade Center bombing, or even the Oklahoma City bombing, seem minor by comparison. Casualties could range from the tens of thousands to the millions. The only viable way to reduce the very real threat of such an attack is to reduce U.S. interference in the disputes and conflicts of other nations. Military intervention should be confined to the rare instances in which American vital interests are at stake.

The Major Varieties of Threats to the Homeland

Although there are other important drawbacks to a policy of unnecessary overseas military adventurism--for example, lives of military personnel lost and billions of taxpayer dollars wasted--the policy can be catastrophically counterproductive, given the rising terrorist threat. The vulnerability of the American homeland to retaliation for Washington's meddling is severe--and growing.

The threats to the homeland can be put into four categories, only one of which can potentially be adequately deterred or countered:

1. WMD delivered by ballistic missiles,

2. WMD delivered by cruise missiles,

3. WMD delivered by terrorists using other means, and

4. attacks by terrorists on U.S. information systems and other critical infrastructure.

The first three categories are discussed below; information warfare is discussed later in the study.

WMD Delivered by Ballistic Missiles

The threat from WMD delivered by ballistic missiles can potentially be adequately deterred or countered. According to the secretary of defense, more than 25 countries either have or are developing nuclear, biological, or chemical weapons.[8] More than 20 nations are developing ballistic missiles. Some of those nations--such as Libya, Iraq, Iran, Syria, and North Korea--are hostile to the United States.[9] None of those nations, however, currently has a missile that can hit the United States, and according to the U.S. intelligence community, that threat is over a decade away.[10]

Some analysts argue that the huge U.S. strategic nuclear arsenal would deter even rogue states from launching a ballistic missile containing WMD at the United States. The United States has satellites that can locate the place from which a ballistic missile is launched by using infrared sensors to detect the exhaust plume of the launch vehicle. That capability could allow the United States to determine who fired the missile and retaliate accordingly. On the eve of the Gulf War, President George Bush sent a letter to Iraqi leader Saddam Hussein obliquely threatening to use nuclear weapons against Iraq if that nation used chemical or biological weapons--aboard missiles or other means of delivery--against the military forces of the coalition. A recent change in nuclear doctrine by President Clinton allows the United States to more easily threaten a rogue state with nuclear annihilation if it uses such weapons.[11]

To guard against the rare instance in which the overwhelming power of the U.S. nuclear force failed to deter an unbalanced ruler of a rogue state, proponents of national missile defense advocate the rapid deployment of a system that would kill a limited number of incoming ballistic missiles. They also argue that such missile defenses would guard against an accidental launch by a rogue nation or even the established nuclear powers. A mature research and development program for national missile defense currently exists. Because of the technical sophistication required to develop and launch a ballistic missile that could hit the United States, terrorist groups would probably not have the wherewithal to use ballistic missiles.

The U.S. government has in place or in development systems that could probably deter or counter the ballistic missile threat.[12] U.S. launch detection and large retaliatory deterrent capabilities make ballistic missiles carrying WMD the least likely of the four threat categories.

WMD Delivered by Cruise Missiles

More likely than a rogue state's delivering WMD to the United States with a long-range ballistic missile is a rogue state's or terrorist group's delivering WMD with a land attack cruise missile from a ship offshore. According to the Clinton administration's April 1996 version of Proliferation: Threat and Response, cruise missiles are even less expensive and more accurate than ballistic missiles. Their smaller size may make them an even more elusive target. Furthermore, according to the report, they may also be more difficult to defend against than manned aircraft because they are harder for radar to detect. Even though short-range anti-ship cruise missiles are already widely available, only a few countries possess long-range land-attack cruise missiles. However, the report concluded that there are no technological barriers preventing developing nations from developing or purchasing those relatively inexpensive, potentially very accurate delivery systems.[13]

In addition, it would be far more difficult to identify the perpetrator of an attack by a cruise missile from a ship or aircraft off the coast of the United States than it would be the originator of a ballistic missile fired from the territory of a particular nation. Cruise missiles are capable of being launched from either type of platform without the need for major modifications to the missile.

Although an adequate defense of the American homeland against cruise missiles is possible, the United States is much further away from having one than from having a defense against ballistic missiles. Unfortunately, terrorists are more likely to have access to cruise missiles--which are less expensive and potentially more widely available--than to ballistic missiles. Attacks by terrorists using WMD on cruise missiles are less likely to be deterred than are such attacks by rogue nations. Terrorists are often more radical, unbalanced, and stealthy than governments. However, because it is easier to attack without being identified, even a rogue nation may be more likely to fire a cruise missile from a ship than a ballistic missile from its homeland.

WMD Delivered by Terrorists Using Other Means

Of the four types of threat to the homeland, terrorists' delivering WMD and conducting information warfare are the two most probable. Richard Butler, head of the UN Special Commission's weapons inspection team in Iraq, has said, "Everyone wonders what kind of delivery systems Iraq may have for biological weapons, but it seems to me that the best delivery system would be a suitcase left in the Washington subway."[14]

Speaking of transnational actors--for example, terrorists--using WMD, the Defense Science Board maintains that the "risk of attack on US soil [is] both likely and becoming more easily carried out."[15] Deborah Lee, assistant secretary of defense for reserve affairs, put it even more strongly: "Doubts about the timing and location of possible terrorist attacks sit uneasily alongside the almost certain possibility that attacks against the U.S.

homeland will eventually occur. Counterterrorism specialists define the problem not as a question of if but of when and where such attacks will take place."[16]

Because terrorist use of WMD is difficult to deter, prevent, or ameliorate and is potentially catastrophic in most cases, it is the greatest threat to U.S. national security today and will likely remain so in the foreseeable future.

The Diversity of the Terrorist Enemy

Military and intelligence experts believe that the greatest threat to the United States from WMD is posed by terrorist groups or individuals, because nations that employed such weapons would face disproportionate retaliation.[17] The Defense Science Board notes that "the difficulty of attribution that arises with transnational threats allows attacks against the United States and its allies that nation states would not risk directly for fear of retaliation."[18] (Attributing an attack to a particular terrorist group is more difficult now than in the 1970s and 1980s because today's terrorists are less likely to brag about their actions.)[19] The National Defense Panel concurs that terrorists would be less likely to be deterred from using such weapons: "It is unlikely, moreover, that our nuclear forces would deter nonstate actors (terrorists, criminals, or others) who seek to coerce or punish the United States or its allies."[20]

Marie Isabelle Chevrier, associate director of the Harvard Sussex Program on Chemical and Biological Warfare Armament and Arms Limitation, also distinguishes between the threat from rogue states and the threat from terrorists. She argues that rogue nations may have an incentive to acquire biological weapons to deter a nuclear attack or prevent annihilation by a power with conventional military superiority but may not see an advantage in using them. In contrast, terrorist groups are likely to acquire biological weapons only if they intend to use them. Terrorists create havoc and terror by taking action rather than by making threats. She states, "Terrorists with a score to settle against the U.S. government or institutions could turn to biological weapons as an instrument of revenge."[21] Although her comments pertained to biological agents, the same applies to nuclear and chemical weapons.

Although it may be harder to attribute an attack to a terrorist group and retaliate against it--and thereby to deter such attacks in the first place--than it would be an attack by a hostile government, the likelihood of attribution may vary depending on the nature of the terrorist act. Some terrorist acts are directed by hostile governments--for example, evidence indicates that two Libyan intelligence agents, probably directed by high officials in the Libyan government, planted the bomb that downed Pan Am 103 flight over Lockerbie, Scotland. Some attacks are perpetrated by groups that are sponsored and funded by governments, although the governments do not directly control the operation. Finally, many attacks (perhaps most) are perpetrated by small, freelance groups.[22]

Acts by freelance groups are the most difficult to trace--because the groups are highly decentralized and privately financed and their members are extremely suspicious of outsiders. Bribes that intelligence agencies use to recruit moles in such groups are less likely to work because the group is likely to have a fanatical religious or ideological zeal holding it together. Thus, independent terrorist groups are hard to penetrate, even using human intelligence agents.[23]

Even in the case of government financial ties with or control of terrorist groups, it can be challenging to uncover those links. In addition, if biological, nuclear, or information warfare is conducted, few clues pointing to the perpetrator will be left. A nuclear explosion will undoubtedly destroy the evidence. Biological weapons leave few "fingerprints." Only a minuscule portion of penetrations of computer systems are even detected. Even if links to a government can eventually be established, it may take a significant amount of time for an investigation to be conducted, thus delaying retaliation. A perpetrator's knowledge that attribution would be delayed, if any can be established at all, may weaken deterrence against such attacks.

It is also more difficult to retaliate against independent freelance groups. If a terrorist attack can be found to have either direct or indirect links to a hostile nation, that country can be attacked, but if such evidence is lacking (or ambiguous), "going to the source" is not a viable option. Retaliating against freelance groups is especially difficult; even finding appropriate targets can be a problem. Instead of retaliatory bombing or missile strikes, covert action might be the preferred method of punishing such independent groups.

Threat from Terrorists Using WMD Is Rising

The Department of Defense's November 1997 version of Proliferation speaks about the increasing threat of a terrorist attack using WMD:

> Many of the technologies associated with the development of NBC [nuclear, biological, or chemical] weapons, especially chemical and biological agents, have legitimate civil applications and are classified as dual-use. The increased availability of these technologies, coupled with the relative ease of producing chemical or biological agents, has increased concern that use of chemical or biological weapons may become more attractive to terrorist groups intent on causing panic or inflicting large numbers of casualties. In addition, the proliferation of such weapons raises the possibility that some states or entities within these states could provide chemical, biological, or radiological weapons to terrorists.[24]

When asked about that assertion at a news conference, Secretary of Defense Cohen replied that he was concerned about the large volume of nuclear, chemical, and

biological material that is now available throughout many regions of the world. He stated that as many as 25 countries have produced it or are in the process of producing it. Therefore, he concluded, "We know a number of countries are seeking to acquire the technology and the capability and the precursors, then I think you can follow it to a reasonable conclusion that yes, there are groups who will seek to either design their own systems, acquire the materials necessary to produce it, and use it at some future time."[25]

DoD's report notes that concerns about the theft or sale of nuclear materials from the former Soviet Union also apply to biological and chemical materials. "Concerns about inadequate security are not confined to nuclear materials. This could also be the case for facilities in the former Soviet Union that house chemical or biological warfare-related materials. In addition, numerous scientists or technicians previously involved in key programs face severe salary reductions or loss of employment."[26]

According to the top scientist in the Soviet biological weapons program, many scientists in that program migrated abroad to unknown destinations to look for work. There has been speculation that they might have gone to Iraq, Syria, Libya, China, Iran, Israel, or India.[27]

Once terrorists acquire nuclear, biological, or chemical material and smuggle it into the United States, they could disseminate it easily using several possible methods. The bomb needed for a nuclear explosion could be small enough to fit in a satchel or large enough to require a truck for delivery. A conventional truck bomb could be used to spread medical radiological waste over a wide area. An aerosol sprayer--on a rooftop, truck, or crop-dusting aircraft--could be used to disseminate biological and chemical agents. Even more easily, terrorists using a personal computer on the other side of the world could use readily available software to attack vital U.S. computer systems.

Along with the improved capabilities to use WMD to inflict massive casualties, terrorists increasingly have the desire to do so, according the Defense Science Board.

> There is a new and ominous trend to these threats: a proclivity towards much greater levels of violence. Transnational groups have the means, through access to weapons of mass destruction and other instruments of terror and disruption, and the motives to cause great harm to our society. For example, the perpetrators of the World Trade Center bombing and the Tokyo Subway nerve gas attack were aiming for tens of thousands of casualties.[28]

According to a Secret Service agent who questioned Ramzi Ahmed Yousef--the leader of the fundamentalist Islamic group that bombed the World Trade Center--the apprehended terrorist noted that during World War II the Americans dropped on the cities of Hiroshima and Nagasaki atomic bombs that killed 250,000 civilians. Yousef then

asserted that the Americans would know they were at war when they, too, suffered casualties of that magnitude.[29] To punish the United States for its policies in the Middle East, Yousef and his followers planned to kill 250,000 people by collapsing the towers. Instead of avoiding the infliction of mass casualties, terrorist groups--whether state sponsored or acting independently--that want revenge for superpower interventions overseas might have such carnage as a goal.

Thus, the people of the United States could easily be faced with a catastrophic terrorist attack. According to Dr. Michael Osterholm, the Minnesota Department of Health's expert on responding to incidents of biological terrorism, the question is, not if, but when such an attack will occur.[30] A recent British government intelligence report detailed an Iraqi plot to smuggle large quantities of anthrax into "hostile countries."[31] The Federal Bureau of Investigation reported that 40 credible threats to use chemical and biological weapons were made in the United States in 1997 alone.[32]

The Principal Types of WMD Threats

Terrorists could use three types of WMD: biological, chemical, and nuclear. A summary of the characteristics of each WMD (along with those of information warfare) is given in Table 1.

Threat from Biological Weapons

Biological agents suitable for use as weapons are organic microorganisms--bacteria or viruses--or their toxins. They are primarily weapons of terror. All of them invade the body, and some are contagious, which magnifies their effects. Although they can be used to attack military logistics and rear areas, they are less effective in direct combat against armed forces in the field.[33] Because they can take a few days to a few weeks to incapacitate or kill their victims, their effects are too slow to stop such forces. Examples include microorganisms, such as anthrax bacteria or the plague, and toxins, such as botulism toxin.

At least 10 nations are believed to have biological weapons programs.[34] Those nations include Iraq, Iran, China, and North Korea. Some of those nations sponsor terrorist attacks worldwide.

Very Small Quantities of Readily Available Agents Are Deadly. Biological agents can be disseminated by insects, contaminated water and food, and aerosol. Dissemination by aerosol is most efficient, with injuries and death the result of inhalation. Aerosols are usually delivered by artillery, missiles, or aerosol sprayers (terrorists would probably use only sprayers). Even very small quantities of cheaply produced and easily concealed biological weapons can be lethal over very large areas (larger than the area covered by fallout from a nuclear explosion and much larger than the area contaminated by chemical weapons).[35] According to the 1996 version of Proliferation, for deliberate attacks against

civilian populations in urban areas, the quantity of agent could be small (a single gram, possibly less), production and purification methods extremely simple, and the dissemination means simple to complex.[36]

Table 1
Characteristics of Weapons of Mass Terror

Characteristic	Biological Weapons	Chemical Weapons	Nuclear Weapons	Information Weapons
Nature of agent	Live organisms or their toxins	Nonliving liquids	Fissionable material	Intrusion into computer systems
Examples	Pathogens: anthrax, plague, cholera, Q fever, tularemia Toxins: botulism, ricin	Nerve agents (sarin, VX), blister agents, blood agents	Uranium or plutonium	Various intrusion techniques
Primary use	Terror weapon	Defensive battlefield weapon	Ultimate weapon	Weapon of disruption
Secondary use	Marginal battlefield weapon	Terror weapon	Terror weapon	Could become battlefield weapon
Value as terror weapon	Wide area of destruction, readily available technology	Narrower area, readily available technology	Wide area, technology less available	Easily done, but effects temporary and somewhat less destructive
Method of killing	Breathing or ingesting	Breathing or contact with skin	Exposure to blast and radiation	Indirectly
Method of delivery	Aerosol spray, exhaust from truck, food or water contamination	Aerosol spray, exhaust from truck	Truck or ship, bombing nuclear reactor, radiological contamination	Can hack from afar
Ability to detect	Slowly, if at all	Difficult	Difficult	Difficult
Antidote	Yes, but won't know attack is occurring until too late	Yes, but must be administered quickly; antidote can be toxic	None	Defensive and backup systems may help
Decontamination	Difficult and slow	Must be done quickly, but process often difficult and slow	None	Yes, but may take time to restore systems
Ability to trace to terrorist group	Low	Low	Higher	Low
Challenges for terrorist	Dissemination or genetic engineering of resistant organisms	Few	Know-how to make weapon readily available, but need fissionable material, which is controlled	Few; techniques readily available

According to the secretary of defense, five pounds of anthrax could

annihilate half the population of Washington, D.C.[37] (That small amount could cause roughly 300,000 casualties.) If the fake anthrax attack against B'nai B'rith headquarters in Washington, D.C., had been real, the mere five ounces of anthrax released from an aerosol can on the lawn would have created a cloud of 30 square kilometers over the White House and surrounding area and resulted in 10,000 casualties, according to a study by Lawrence Livermore Laboratory.[38]

Unlike chemical agents, the production of which is measured in tons, biological agents are produced in quantities measured in kilograms. Because only very small quantities of impure toxin are needed to kill large numbers of people, the number of biological agents that could be used is almost unlimited. Proliferation (1996) states,

> Genetic engineering and other new technologies now can be employed to overcome product deficiencies in the classic agents and toxins. Moreover, toxins that exist in nature in small amounts were once considered not to be potential threat agents because of their limited availability. Today, however, a number of natural toxins conceivably could be produced through genetic engineering techniques in sufficient quantities for an adversary to consider producing them as an offensive weapon. There are many microorganisms, or their metabolic byproducts (toxins), that meet all of the criteria for effective [biological weapon] agents.[39]

Genetic engineering can be done by a few trained researchers in a small building with machines that fit on a tabletop. The machines are widely available and inexpensive. In the future, not even that much expertise and equipment may be required. Genetic engineering technology is rapidly diffusing. High school students are now learning how to create bacteria that are resistant to antibiotics using $42 kits that can be ordered through the mail.[40]

Production Technology and Equipment Are Commercially Available. The abundance of agents is paralleled by the accessibility of the technology and equipment for producing them. Proliferation (1996) concludes that there is nothing unique about the types of equipment (or technology) that might be employed in a biological warfare program. For example, biological safety cabinets have been adopted universally for biomedical research, as well as for production of commercial medical products. Fermenters, centrifuges, purification devices, and other laboratory equipment are used not only by the biomedical community; they also have other academic and commercial applications. The equipment is used by wineries, milk plants, pharmaceutical houses, and agricultural enterprises. For example, production of beer, antibodies, enzymes, and other therapeutic products, such as insulin and growth hormone, involves the use of fermenters ranging in size from 10,000 to 1 million liters. The same fermenters could produce significant quantities of biological agents. Such key technologies have an intrinsic dual-use character.[41] Amy Smithson, a security expert at the Henry L. Stimson Center, reports that the

technologies are well known and can be found on the Internet. Ingredients and machinery are also easy to obtain because they are dual use.[42]

Making a Weapon. After the biological agent is grown and concentrated or the toxin is made, a little more technical sophistication is needed to create a usable weapon, but nowhere near that needed to make a nuclear device. Some biological agents are perishable and require care in handling. However, one of the most likely agents that terrorists might use, anthrax, is very durable and easy to store.[43] Disseminating the agent through aerosol or other means is the step that requires the most expertise. Yet the technology for aerosol dissemination is available commercially.[44] As a result, none of this technology is beyond the grasp of a terrorist group. Aum Shinrikyo--the Japanese cult that released the chemical agent Sarin in the Tokyo subway--was also attempting to generate the biological agents anthrax and botulism, as well as to master methods of aerosol dissemination.[45] The group attempted to spread anthrax and botulism throughout Tokyo using a rooftop sprayer for the first and the exhaust system of an car for the second.[46] Also, the group had acquired a large Russian helicopter and remotely piloted vehicles to disseminate WMD. Fortunately for Tokyo, the group made some mistakes in producing or disseminating the agents. Next time Tokyo (or some other city) might not be so lucky.

Effects of Biological Terrorism Will Become More Lethal. Although Seth Carus, an expert on biological terrorism at the National Defense University, notes that the effects of such incidents so far have been small, he predicts that they could increase dramatically in the future.

> Unfortunately, there is strong reason for concern that future bioterrorism attacks may be far more deadly than past incidents. Three factors account for this change.
>
> First, there are terrorists who want to kill large numbers of people. There have been such groups in the past, but there appear to be a growing number who want mass casualties. The World Trade Center and Oklahoma City bombings both were conducted by people who had no compunction about mass killing. Second, the technological sophistication of the terrorist group is growing. The Aum Shinrikyo was attempting to master the intricacies of aerosol dissemination of biological agents. Some terrorists might gain access to the expertise generated by a state-directed biological warfare program. Finally, Aum Shinrikyo demonstrated that terrorist groups now exist with resources comparable to some governments. It seems increasingly likely that some terrorist group will become capable of using biological agents to cause massive casualties.[47]

The Threat of Terrorists' Using Chemical Weapons

In contrast to biological weapons, which use living microorganisms or toxins from them, chemical weapons use man-made liquids that are disseminated as droplets in aerosols and either enter the body through the skin or become vapor and cause respiratory problems.

Several other characteristics distinguish chemical from biological agents. Chemical agents are better weapons on the battlefield because they take effect much more rapidly than do biological toxins. Conversely, the delayed effect of biological agents--and the consequent delay in detection--can actually be an advantage for a weapon of terror. By the time the attack is detected, it is too late to save the victims. In addition, biological weapons leave few "fingerprints" and allow the terrorist time to get away before the authorities can pinpoint the source of the attack. Although a chemical agent contaminates a smaller area than does a biological or nuclear weapon, one or more weapons could still cause havoc and massive casualties if used on a major U.S. city.

The technology needed for chemical weapons is commercially available. The technology required to produce and disseminate a chemical weapon is even less sophisticated than that required for a biological weapon. According to Proliferation (1996),

> The precursor chemicals and intermediate states in the production process for two classic CW
> agents, nerve and blister agents, have both agricultural and industrial uses. For example, Thiodiglycol, which has been used to produce ball-point pen ink, can be converted to mustard agent by a simple (single) chlorination step. The
> technology and most of the production equipment, moreover, even the military hardware necessary for delivery and dissemination, are dual-use. Detection and discrimination between legitimate and illegal production are difficult. Facilities producing pesticides, insecticides, and fire retardant chemicals could be converte

The report continues,

> If need be, crop duster aircraft and simple spray generators can be readily adapted for delivery of a variety of agents. The quantities of chemical agent required are relatively small when compared to industrial production of similar commercial chemicals, which poses significant problems for detection. The low technology required lends itself to proliferant and even potential terrorist use. Terrorists could employ CW agents in a variety of means utilizing simple containers such as glass bottles, commercial compressed gas bottles, or propane tanks.[48]

Aum Shinrikyo demonstrated the ease with which a terrorist group could develop chemical weapons and use them in a mass attack. In 1995 the group left plastic bags containing the nerve agent Sarin on the Tokyo subway. Twelve people were killed and 5,000 were injured. The casualties were limited only by the relatively low potency of the toxin--25 percent of military strength. The group was also experimenting with VX, a nerve agent 10 to 1,000 times stronger than Sarin. Sarin and VX are both so deadly that a single drop on the skin is fatal. In a large city, a quart of VX toxic agent could reportedly kill about 12 million people in about 60 minutes if it were properly distributed.[49]

Nuclear Terrorism

The catastrophic effects of nuclear weapons are well known. Although building a nuclear device is more costly and technologically difficult for a terrorist group than is producing a chemical or biological weapon, doing so is still very possible. According to Louis Freeh, director of the FBI, "There is now greater danger of nuclear attack by some outlaw group than there was by the Soviet Union during the Cold War."[50] The Defense Science Board reaches a similar conclusion. "If the required fissile material is available, it is not difficult to design and build a primitive nuclear explosive device. It is unlikely, though not impossible, that it could be done by just a few people. But because of the diffusion of knowledge and technology over the past decades, it no longer requires the resources of a nation state.[51]

Obtaining Fissile Material, Nuclear Technology, or Atomic Weapons. Because of the relatively tight controls on nuclear material (enriched uranium or plutonium), a terrorist group would have more difficulty acquiring such fissile materials to build a nuclear device than obtaining the more readily available precursors and equipment for chemical and biological weapons. Since the breakup of the Soviet Union, however, it has become easier to obtain both fissile material and nuclear technology. According to William Potter, director of the Center for Non-Proliferation Studies at the Monterey Institute of International Studies, "The former Soviet Union's nuclear weapons and material stockpile is at risk, and America is extraordinarily vulnerable to terrorists employing weapons of mass destruction."[52]

Poor economic conditions in the nations of the former USSR, lax security at dozens of facilities with nuclear material, poor accounting and control of fissile material, and efforts by organized crime to profit from the smuggling of such material all make it more likely that terrorists could get nuclear-related items. Russian nuclear scientists, engineers, and technicians--facing drastic drops in income--could profit from the sale of nuclear materials and know-how. Experts have warned that gangs in Russia have tried to steal enriched uranium and smuggle it out of the country.[53] According to a letter from the Russian ambassador to the United Nations Sergey Lavrov to UN secretary general Kofi Annan, the world community has more than once encountered cases of "leakage" of

nuclear components.[54]

Terrorists could also get help from technical personnel associated with the now-defunct nuclear programs in Brazil, Argentina, and South Africa.[55] Scientists from those programs might also need work and be amenable to helping a rogue state or a terrorist organization to develop a nuclear weapon.

The terrorist group might not even need weapons-grade plutonium (Pu-239) or uranium (U-238) to make a nuclear device. A weapon using non-weapons-grade plutonium (material used in nuclear reactors) was tested during the 1960s. Although such a weapon might be less efficient and have a more unpredictable yield than one made with weapons-grade material, those deficiencies might mean little to a terrorist group hoping only to induce mass terror and casualties.[56] Other sources of fissile material include growing stockpiles of spent nuclear fuel around the globe.

Of course, given the moderate challenge of stealing or buying fissile material and creating a nuclear device from scratch, the terrorist might simply attempt to steal or buy the complete weapon. Gen. Alexander Lebed, former Russian national security chief, claims that 100 Russian nuclear devices the size of suitcases are missing.[57] The U.S. government has admitted holding in its arsenal a lightweight nuclear device that would have been delivered to an adversary's harbor by a Navy or Marine parachutist. Roger Heusser, an Energy Department official, acknowledged that such 60-pound devices could be seen as a precedent for a possible nuclear weapon for terrorists.[58] The admission that the United States has such weapons raises questions about the veracity of Russian assertions that they manufactured no satchel charges during the Cold War arms race. Given the current economic and security situation in Russia, if the Russian military has such small nuclear devices in its inventory, they could be vulnerable to theft or purchase by terrorists. But a terrorist group would not need to build or steal a device that was so small. A somewhat larger device could be transported to its destination by a small truck or ship or an aircraft of moderate capacity.[59]

Attacks Causing Radiological Contamination. To cause a radioactive discharge, terrorists could sabotage, bomb, or attack one of the many nuclear reactors in the United States. Hospitals and industries also use and store radiological materials that might be stolen and fashioned into a weapon. Conventional explosives could be used to spread such materials. In such an explosion, no nuclear blast or heat effects would result, but radiological contamination could be widespread. Although such contamination would not be as catastrophic as that caused by a nuclear explosion, it would be serious. And an attack using conventional explosives would be much easier to execute. Although controls exist on radiological materials, they did not stop Chechen rebels from planting cesium-137--a radiological substance with industrial and medical uses--in a Moscow park.[60]

Terrorists' Use of Information Warfare

The threat of terrorists' attacking vital information systems that run the U.S. economy (for example, computers at the stock exchanges) or key parts of the nation's infrastructure (for example, power or telecommunication grids) is also a serious concern.

The National Research Council warned in 1995--and was echoed by a Defense Science Board study on information warfare in 1996--that "the potential exists for an electronic Pearl Harbor."[61] According to the American Banker, the Clinton administration created the President's Commission for Critical Infrastructure Protection "to address the fact that most of the computer networks in this country are interrelated and vulnerable to cyber attack both by terrorists, who may or may not be state-sponsored, as well as attacks by state-sponsored groups."[62]

According to Sen. John Kyl (R-Ariz.), in classified briefings, lawmakers have learned that foreign groups are increasingly capable of conducting information warfare against the United States.[63]

Information Warfare Could Bring Goliath to His Knees

The report of the Defense Science Board's task force on information warfare argued that in the agricultural age, military campaigns were waged to gain control of the land; in the industrial age, campaigns focused on the adversary's means of production; and in the information age, "campaigns will be organized to cripple the capacity of an information-based society to carry out its information-dependent enterprises." The report warned that the computers of the U.S. telecommunications, electric power, banking, and transportation industries are now vulnerable to attack by anyone seeking to confront the United States without confronting its military.[64] According to Arnaud de Borchgrave of the Center for Strategic and International Studies, "Any thinking person knows that the traditional prerogatives of national sovereignty have not only been overtaken by the information revolution, things like logic bombs and worms are the new arsenal in a new geopolitical calculus that enables the non-states, and even individuals, to take on a superpower. That’s the sort of world we’re living in, and our leaders don’t want to face up to it."[65]

The Defense Science Board's report maintains that "information warfare is also relatively cheap to wage, offering a return on investment for resource-poor adversaries. The technology required to mount attacks is relatively simple and ubiquitous."[66]

Adm. Mike McConnell, former director of the National Security Agency, agrees that all of the attack tools can be downloaded from the Internet. He asserts that there is a "tremendous, richly robust hacker group that shares all these techniques" used for penetrating computer systems. In addition, he notes that commonly available Silicon Graphics

workstations make very capable platforms for cyber attacks.[67] The most recent attack by hackers on 11 defense computers is believed to have been the most organized assault on such military systems ever. Although authorities believe that the attack was initiated by vandals--not terrorists--they noted that the hackers used software that was widely available.[68]

Unlike other terrorist attacks, information warfare could be carried out safely from the other side of the world. The U.S. intelligence community believes that attacks from other parts of the world have already victimized U.S. banking and financial information systems. Some electronic transactions have embedded attack codes designed to cause havoc in the markets.[69] The London Times reported that several London financial institutions had paid up to $400 million to extortionists who used logic bombs (software programs that cause systematic errors) to demonstrate that they could destroy the global operations of those institutions.[70]

The Threat of Information Warfare Is Likely to Become More Severe

The threat of an attack by information warfare pales only in comparison with the horrendous effects of an attack using WMD. Information warfare against key economic and infrastructure nodes is somewhat less likely to result in a massive loss of life (causing the collapse of systems, such as those for air traffic control, can result in some loss of life) than are terrorist attacks using nuclear, biological, and chemical weapons. In addition, the effects of attacks on information systems are likely to be temporary (but could still be catastrophic). Finally, a severe threat is still a couple of years in the future, according to Jamie Gorelick, former deputy attorney general and co-chair of a presidential committee advising on computer security. Nevertheless, she believes the threat is very real. "We rest, as a nation, on a bed of computers that are privately owned and very unevenly protected. And even the government's computers, where there's been a real effort to make them more immune from attack, are vulnerable. And so it doesn't take much imagination to see what kind of threat there could be in the future to our national security."[71]

The Defense Science Board reached similar conclusions about the severity of the future threat by predicting that, by the year 2005, attacks on U.S. information systems by terrorist groups, organized criminals, and foreign espionage agencies are likely to be widespread.[72]

> Tools and techniques for penetrating networks illicitly are rapidly becoming more sophisticated and varied, the associated software tools are available, and there is a community eager to share and exploit these tools. The intended effects of an information warfare attack probably will not be subtle, particularly in the context of a carefully orchestrated information warfare campaign. Such a campaign will become increasingly likely.[73]

The Pentagon's computers alone were penetrated 100,000 times during 1997. Furthermore, before the Gulf War, someone reportedly stole military secrets--including troop movements--and tried to sell them to an unbelieving Saddam.[74] The Defense Science Board confirmed the underlying vulnerability. "Investigations into the security of DoD networks by the Armed Services and the Defense Information Systems Agency (DISA) have concluded that our networks are vulnerable to unauthorized access at the most intimate level."[75] If the Pentagon's computers are that vulnerable, much of the rest of the nation's data processing must be even more so.

Because the effects of an attack on U.S. information systems are likely to be temporary, terrorists might use such an attack to complement a nuclear, chemical, or biological strike. Disrupting information systems could impede a governmental response or amplify the psychological trauma of the main attack.

The Ranking of Threats

Of the four types of threats-—biological, chemical, nuclear, and information--biological weapons used by terrorists pose the most serious threat to the American homeland. Biological weapons involve technology that is readily available, effects that are difficult to detect, and an extensive area of destruction. The technology for chemical weapons is also readily available, but chemical agents have a smaller area of destructiveness. Nuclear warfare is at least as destructive as biological warfare, but its technology is more difficult to obtain.[76] Information warfare is a distant fourth because its effects are temporary, more economic in nature, and probably less lethal than those of an attack with WMD. It will nonetheless be a potent future threat.

Little Can Be Done against Terrorist Attacks on U.S. Soil

As scary as the potential for attacks using WMD may be, it will be very difficult to deter or prevent terrorists from making, transporting, or using such weapons. In addition, if terrorists use such weapons on U.S. soil, their effects will be difficult to detect (with sufficient warning) or mitigate. Although the effects might be temporary, a catastrophic penetration of U.S. commercial or government information systems will also be difficult to deter, prevent, detect, or mitigate.

Proliferation of WMD Capabilities to Rogue States and Terrorist Groups

Although international regimes such as the Nuclear Nonproliferation Treaty, the Nuclear Suppliers Group, the Chemical Weapons Convention, the Biological and Toxin Weapons Convention, and the Australia Group were created with the intent of controlling the spread of WMD and the material, equipment, and technologies used in making them,[77] enforcing those regimes' provisions has proved difficult because nations and companies

have flouted them. According to Ashton Carter, former assistant secretary of defense for international security policy, "export controls alone cannot prevent proliferation," because determined leaders like Saddam can "home grow their weapons of mass destruction or get them from other countries."[78] Because exporters that covertly evade economic sanctions can earn high profits, enforcement of the measures has been difficult. That is especially true when the materials, equipment, and technologies are widely available commercially, as is the case for those used in the production of chemical or biological weapons. According to the Senate Governmental Affairs Committee, such export control regimes "can only slow the spread of WMD technology."[79]

Significant proliferation of WMD technologies, especially biological and chemical technologies, will occur despite the best efforts to prevent it. According to Secretary of State Madeleine Albright, proliferation of WMD is "the most overriding security interest of our time."[80] In recent testimony before the Senate Intelligence Committee, the directors of the Central Intelligence Agency and the Defense Intelligence Agency concurred that the proliferation of WMD was the biggest threat to national security. Lt. Gen. Patrick M. Highes, director of the DIA, said that "because chemical and biological weapons are generally easier to develop, hide and deploy than nuclear weapons," they will be "more widely proliferated and have a high probability of being used over the next two decades."[81] The Defense Science Board report admits that discovering the chemical and biological warfare capabilities of transnational actors (terrorists) is difficult. "Signatures associated with acquiring a chemical or biological capability, especially by a transnational threat group, are low and ambiguous, and not completely understood."[82]

As noted earlier, biological and chemical weapons can be easily and inexpensively produced using commercially available raw materials and technologies in rather small facilities intended for developing mundane commercial products. There are so many commercial facilities capable of making chemical and biological weapons in the world that such production would be easy to hide. Thus, the intrusive inspections of commercial businesses under the auspices of the international agreements provide a false sense of security yet force innocent businesses to expose their industrial secrets to competing nations.[83] The loss of industrial information could be especially devastating for biotechnology and pharmaceutical companies.[84]

Alan Zelicoff, a scientist at Sandia National Laboratory and technical adviser to the U.S. delegation to the Biological and Toxin Weapons Convention, even argued against intrusive international inspections.

> Facilities engaged in legitimate activities can be incorrectly assessed to be in violation of the convention. Conversely, sites that are demonstrably in compliance with the convention easily can convert to illicit activity within hours after the departure of inspectors.

> The reasons for this quandary: Equipment for pharmaceutical production is identical to that used for bio-weapons processing, and even the most toxic of biological materials are used in medical therapeutics and research. In just a few days or weeks, biological agents can be manufactured in militarily significant quantities in a site no larger than a small house.[85]

Limits to the Effort to Stop Proliferation: Iraq as a Case Study

The intense interest of the international community and the most relentless inspections in history have been focused on Iraq's WMD programs. The spotlight has been much brighter than that shone on the normal enforcement of international nonproliferation agreements. Even so, the international community will never be assured that all of Saddam's weapons and the facilities needed to make them have been uncovered and destroyed, according to Zelicoff. (In fact, the only reason the international community knew about Saddam's biological weapons program was that his son-in-law defected and revealed its existence.)[86] Despite extensive efforts to determine the location of Iraqi weapon stockpiles and production facilities, information is far from complete. "Put bluntly, we don't really know what Iraq has. And that's the heart of the problem," said Charles Duelfer, deputy chief of the UN special commission in charge of inspecting suspected Iraqi sites.[87] (For example, biological weapons can be manufactured quickly and hidden, and they can be destroyed quickly if in danger of being found by inspectors.) Even military action--that is, bombing--would be unlikely to wipe out Iraq's chemical and biological weapons labs, which are small, mobile, and easily hidden (for example, in hospitals and fertilizer plants).[88]

In the unlikely event that the international community did succeed in destroying all existing stockpiles and facilities, Saddam could produce more agents using readily available commercial technologies after the inspectors left.[89] Gen. Henry Shelton, chairman of the Joint Chiefs of Staff, admitted how easy it would be for Iraqi technicians to transform a hospital, a veterans' clinic, or a fertilizer plant into a facility for making anthrax or mustard gas weapons: "You can convert one of them quickly and resume making chemical or biological weapons. One day he's making fertilizer, the next day chemical [weapons] and the next day fertilizer."[90]

If Saddam can still conduct those weapons programs under such close scrutiny, rogue nations--and especially terrorist groups--are likely to be able to do so even more successfully. Even if inspectors become a permanent fixture in Iraq, the international community does not have the energy or resources to conduct ongoing inspections in every nation that it suspects of developing--or harboring terrorists who are developing--chemical or biological weapons.

Delivering Weapons of Mass Destruction

If it is relatively easy for terrorists to get raw materials and develop WMD, how difficult would it be to smuggle such materials into the United States? With thousands of miles of borders to police and millions of travelers to inspect, U.S. Customs authorities would find it virtually impossible--without good intelligence tips--to stop the small quantities of such materials that could cause horrific casualties. As Gordon Oehler, former director of nonproliferation at the Central Intelligence Agency, noted, the small amounts required could be shipped in normal commerce.[91] This problem is even worse than that of interdicting drug shipments into the United States. Small quantities of drugs enter the country over thousands of miles of borders. As a result, law enforcement authorities stop only a paltry 5 to 15 percent of the total amount shipped.[92] Biological, chemical, or nuclear materials would be even harder to stop because they are transported in even smaller shipments.

According to the Defense Science Board,

> Potential adversaries employing inexpensive and much more readily available weapons of mass destruction can now use the global information infrastructure, along with the Global Positioning System and commercial imagery satellites, as their C3I [command, control, communication, and intelligence system]; and use the worldwide, robust commercial transportation infrastructure to project "force" anywhere, anytime. This can present a military capability as deadly as large conventional forces, and available--now--to very small adversaries, in terms of population, defense budget, and land area. In fact, it is available to adversaries with no claimed homeland--the transnational threat.[93]

Good Intelligence on WMD Is Difficult to Obtain. Good intelligence information on WMD production and shipment is usually difficult to obtain. As noted earlier, the operations of terrorist groups (and the nations that sponsor them) are notoriously hard to penetrate even with human intelligence agents.[94] Furthermore, during the Cold War, U.S. human intelligence capabilities eroded as the intelligence agencies relied more on the high technology of electronic and satellite systems to monitor the Soviet Union. Such collection systems are not good at detecting chemical and biological manufacturing and storage sites.[95]

The Defense Science Board argues that the government's primary efforts should be in "consequence management" (that is, mitigating the effects of chemical and biological attacks with detectors, protective clothing, vaccines, and medical treatment) because prevention and interdiction through intelligence efforts are likely to be too difficult. (As will be noted below, mitigating the effects of an attack is also a difficult task.)

> The chemical and biological warfare threats require particular attention to consequence management. There are two reasons: While clearly it would

> be preferable to prevent incidents rather than mitigate them, the United States cannot count on prevention. The signatures for chemical and biological weapon production, storage, transportation, and delivery can be exceedingly small. By contrast, nuclear devices present much higher signatures and thus much greater opportunity for interruption earlier in the cycle.[96]

Dissemination of Agents. Once the nuclear, biological, or chemical material has been smuggled into the United States, several dissemination methods are possible. For nuclear material, a bomb would be needed to make the nuclear material achieve critical mass. As noted earlier, it is possible to design a nuclear weapon small enough to fit in a satchel. Barring that method, any ship or vehicle could be used to deliver a crude nuclear bomb into a large metropolitan area. Even a conventional truck bomb could be used to spread medical radiological waste over a wide area.

A truck with a sprayer could also be used to deliver toxic chemical agents.[97] That method was used by Aum Shinrikyo, along with placing plastic bags filled with Sarin nerve agent in the Tokyo subway. Chemical agents could also be dispersed from a crop-dusting aircraft or a rooftop sprayer. Although it is somewhat more complex to disseminate biological agents than it is chemical agents, the same methods of delivery could be used.

Effects of Attacks Are Difficult to Detect and Mitigate

The Defense Science Board commented on the severe difficulties in responding to chemical and biological attacks by dividing biological agents into two subcategories--toxins and pathogens--and doing the same for chemical agents--nerve agents and other agents.

Biological Agents. The report notes,

> Biological toxins--especially botulism toxin, staph enterotoxin, ricin, and abrin--are more toxic than nerve agents and have the additional feature that symptoms may not develop for more than 12 hours after exposure. It is therefore difficult to detect an attack by the response of the population that has been exposed. Treatment of these agents is possible if they are detected early, but the detection methods are slow and expensive. For some, once symptoms have developed, treatment is limited to support. There are no methods of detecting these agents at standoff; detection at short range generally requires immunochemical methods, and is relatively slow (15 minutes after sample collection) and expensive. There are no methods for sampling air and soil to detect these agents. Biological toxins, in general, require that they be breathed or ingested to be toxic, and relatively simple masks afford useful protection; these masks are not available

> in quantities needed to protect . . . civilian populations. Decontamination is again slow and labor intensive, and there are no simple methods for declaring an area safe.
>
> Pathogens. Pathogens such as anthrax, tularemia, plague, glanders, cholera, and Q fever pose the most difficult problems in detection and characterization. There is no standoff detection and only limited point detection. The tests that are available now require access to what is effectively a biology laboratory. Since symptoms do not develop for several days after exposure, it's possible, in principle, to have an attack expose large numbers of people, particularly in a terrorist attack on civilian population, with no indication that an attack had taken place. Since some of these diseases are highly contagious, there is a serious problem of managing a biological attack in such a way that it does not lead to epidemic. In a biological attack, there is a crucial problem of separating those who have been exposed and require treatment from those who have not been exposed; there is no technology for triage now. Protection of the caregivers in the system from first responders to hospital personnel-- relies on conventional methods such as protective clothing and isolation, and the system would be overwhelmed in any serious attack. Decontamination will vary with the agent. There is no accepted set of protocols for decontamination and for certifying that affected areas are safe, especially for anthrax, which is persistent in spore form.[98]

The report continues, "For many possible components of a biological attack, there is no treatment once symptoms appear: pulmonary anthrax, botulism, and ricin toxicity, and essentially all viruses fit into this category." For example, the antibiotics for anthrax must be used within a day or two of exposure.[99]

If even a small city of 50,000 people was contaminated, two tons of antidote would be needed overnight. That much antibiotic is not stored anywhere in the United States. If New York City was attacked, the medical response would be easily overwhelmed.[100]

In practice, treatment is normally difficult because the first detection may be when large numbers of people start arriving at hospitals showing symptoms (such late detection would also render gas masks useless, even if they were available to the civilian population in sufficient quantities). Even after two men were arrested recently when they boasted to an informant that they possessed military grade anthrax, it took three days--including the time for tests at the Army's biological laboratory in Fredrick, Maryland--to determine whether or not the substance confiscated in Las Vegas actually was the deadly pathogen.[101]

Throughout history, prevention of disease has saved more lives than has treatment. The secretary of defense recently announced that all 2.3 million U.S. military personnel would be vaccinated against anthrax at a cost of $130 million.[102] At that price, it would require almost $15 billion to inoculate the entire population of the United States. But the vaccination is for only one of the many possible agents. Each agent must have its own vaccine, and a universal germ vaccine is still years away.[103] Indeed, one may never be developed. Most experts in mitigating the effects of biological incidents agree that mass vaccinations are not the answer.[104] Vaccines and treatments can be defeated by using modern bioengineering techniques to create a wide range of resistant microorganisms. Some evidence indicates that Russian scientists might have developed a strain of anthrax that could be resistant to antibiotics and vaccines.[105]

Detection of biological agents is very difficult because thousands of different microorganisms could be used in an attack. Even if improved detectors are developed, it will be difficult to use them effectively. Given the dearth of intelligence assets to provide warning of an attack, it is difficult to know where to place the detectors.[106] Officials in some cities are reluctant to deploy expensive sensors even at likely sites of attack--for example, subways--because they might miss attacks if the airborne germs did not waft past their immediate area; moreover, there is no possible way to protect all targets.[107]

Chemical Agents. Treatment and decontamination in response to chemical attacks also present problems. The Defense Science Board notes,

> The current systems and capabilities have many deficiencies.
>
> > Nerve Agents. Nerve agents are difficult to detect and characterize at standoff distances. The counteragents used--atropine, pyridostygmine hydrobromide--are themselves toxic, and require care in use. Protective gear is expensive, since nerve agents are toxic by skin contact: there is no effective protection for . . . large numbers of civilians. Decontamination following an attack is difficult and slow and involves caustic and reactive solutions (e.g., bleach), and there are no established criteria for declaring an area safe once it is decontaminated.
>
> > Other Chemical Agents. Many of the same criteria apply to blister, nerve, and blood, and to other agents that have been considered and developed by some nations.[108]

For example, the antidote to the powerful VX nerve agent is expensive, hard to take, and in short supply.[109] Despite the fact that decontamination methods are difficult and slow, decontamination must ideally be accomplished within one to two minutes of exposure. Rapid action often means the difference between life and death. Frequently, such a rapid response is not possible. In the 1995 Tokyo subway incident, officials took

several hours to determine the nature of the attack, which caused panic and delays in treatment that proved fatal.[110]

Nuclear Weapons. Mitigating the effects of a nuclear explosion would be extremely difficult. No vaccines or antidotes for radiation exposure exist. People cannot be decontaminated once they are irradiated. Irradiated areas would take years to recover. Mitigation efforts would be confined to the limited treatment of individuals who were exposed.

Information Warfare. A presidential commission tasked with improving safeguards to the nation's electronic infrastructure concluded that the United States is dangerously ill prepared.[111] Penetrations of computer systems are hard to detect. In the DISA's program of planned penetrations into DoD computers to determine their vulnerability, 70 percent of the intrusions were successful and only 4 percent were detected.[112]

Given that low detection rate, it would be very difficult for the U.S. government to establish an effective warning and security system to protect the plethora of private computer systems in the United States. Even when intrusions that are precursors to a major terrorist attack are detected, they may not be reported. Only one in six organizations that experience penetrations report them to law enforcement agencies. Businesses fear a loss of public confidence in their computer systems or that a competitor will take advantage of publicized incidents. They have no confidence in the government's assurances of confidentiality or fear burdensome government regulations. When businesses do make efforts to secure their computer systems (for example, security measures taken by telephone and power companies), they do so to stem financial losses rather than to monitor and prevent intrusions that could cause the networks to collapse.

Furthermore, an effective national cyber attack warning system would be difficult to create because new offensive techniques arise as fast as defensive techniques can be adopted. Ken Allard of the Center for Strategic and International Studies argues, "It's almost like trying to thwart drug lords. You can thwart them over here, but by God, two weeks later they show up over there."[113] Thus, in a diffuse private economy of many computer systems that are increasingly linked, it will become very difficult to deter, prevent, detect, or mitigate well-choreographed catastrophic penetrations by terrorist groups halfway around the world.

Defending against Attacks Using Weapons of Mass Terror Is "Too Hard"

The independent National Defense Panel was pessimistic that any defense against terrorist WMD attacks would be viable: "No defense will ever be so effective that determined adversaries, such as terrorists bent on making a political statement, will not be able to penetrate it in some fashion. This is perhaps even true in the case of a regional enemy who threatens to execute WMD attacks on the U.S. homeland employing organized infil-

tration forces."[114] Even one such penetration by terrorists could be cata-strophic.

Joshua Lederberg, a Nobel laureate at the National Academy of Sciences, made some comments about bioterrorism that could easily apply to other weapons of mass terror: "There is no technical solution to the problem of biological weapons. It needs an ethical, human, and moral solution if it's going to happen at all. Don't ask me what the odds are for an ethical solution, but there is no other solution. But would an ethical solution appeal to a sociopath?"[115]

The Defense Science Board also candidly admits the daunting challenge of responding to WMD attacks and information warfare: "There are a number of challenges that have historically been regarded as 'too hard' to solve: the nuclear terrorism challenge, defense against the biological and chemical warfare threat, and defense against the information warfare threat. This task force believes that these challenges should be addressed and incremental improvements should be sought and implemented; doing so will make a substantive difference."[116]

The report continues by extolling the virtues of pursuing an incremental approach to defending against attacks using biological agents, probably the most severe of threats:

> The biological warfare threat can appear so formidable and frightening that it can engender a posture of inaction. Indeed, it is too hard to find a perfect solution or totally effective defense. There is considerable merit in former Navy Under Secretary Richard Danzig's prescription to "think small" with respect to defense against biological weapons. A focus on incremental steps that can help mitigate the threat and raise the price to potential attackers will more likely produce a sustainable and productive effort for the long term. Many new technologies offer the potential to build components of systems that will incrementally add to national capabilities to defend against this threat. This study, like others, while identifying many promising steps, found no silver bullet that will eliminate the entire range of threats.[117]

A report by Paul Richter of the Los Angeles Times confirms that only incremental progress is being made in combating those threats. "Despite years of warnings from experts, the United States is poorly prepared to defend its armed forces from the rising threat of germ warfare and lags even more in protecting Americans at home, defense officials say. As President Clinton and other leaders have been proclaiming the dangers of biological weapons, officials acknowledge that they are taking only the first steps to develop the high-technology gear, medicine, and organization needed to respond to germ arsenals."[118]

Any incremental progress in the ability to detect and mitigate such critical threats

to U.S. security that can be achieved by reallocating DoD's resources away from the many questionable threats it spends money combating should be applauded. But that will not be enough. Such incremental improvements should not be used merely to convince the American public that the government is "doing something" about this terrifying and real threat. That could lead the American populace to have a dangerous false sense of security, thus allowing the political elites to continue to conduct a foreign policy of adventurism overseas. What is needed is a drastic sea change in thinking about what constitutes U.S. security and what foreign policy can best achieve it.

A Drastic Change in the Strategic Environment

As noted earlier, the National Defense Panel, in arguing for a reemphasis on homeland defense, asserted that "protecting the territory of the United States and its citizens from 'all enemies both foreign and domestic' is the principal task of government."[119] Yet it was also noted that the Defense Science Board admits that "historical data show a strong correlation between US involvement in international situations and an increase in terrorist attacks against the United States" and that "US policies in the Middle East have become the basis for violent retaliation from many groups."[120] That effect may have been less of a problem when great powers regarded the threat from terrorists as a peripheral security issue--that is, as merely a pinprick. Yet the same report notes that the proliferation of WMD and information warfare technology and changes in the motives of terrorists allow such previously weak groups to threaten great powers with massive destruction.

> The technology of today, and that which is emerging, allows a small number of people to threaten others with consequences heretofore achievable only by nation states. The United States' homeland, allies, and interests are vulnerable. In the judgement of this task force, the likelihood and consequences of attacks from transnational threats can be as serious, if not more serious, than those of a major military conflict.[121]

The report continues:

> Transnational adversaries, in contrast to traditional terrorists, are motivated to inflict massive destruction and casualties. In the past, analysts believed one of the key "tenets of terrorism" was that terrorists calculated thresholds of pain and tolerance, so that their cause was not irrevocably compromised by their actions. While US government officials worried about terrorists "graduating" to the use of weapons of mass destruction (almost exclusively nuclear), they believed--based on reports from terrorists themselves--that most terrorist groups thought mass casualties were counterproductive. Mass casualties were believed to delegitimatize the terrorists' cause, generate strong governmental re-sponses, and erode terrorist group cohesion. In essence, terrorists were ascribed a certain logic and

> morality beyond which they would not tread. The world has changed and this mentality is no longer the case.[122]

The Wrong Conclusion

The Defense Science Board report fails to draw the obvious policy conclusion from its own analysis: that U.S. global intervention has increased the threat of terrorism to levels that are unacceptable according to any reasonable calculus of American interests. Instead, the report reaches an incomprehensible conclusion:

> US presence, policies, and leadership will remain a major stabilizing force in the world, which will require a range of credible offensive military capabilities, forward military presence, surge capabilities, and independent or coalition operations. A credible future global model depicts an environment that will require an activist foreign policy to sustain world stability, continuing foreign presence, and occasional military interventions in areas of conflict. This same model exacerbates stresses that traditionally motivate transnational threats. Thus, the transnational threat to the United States and its citizenry will become more significant over time.[123]

The report further asserts that a by-product of such massive destruction in the homeland is that "the consequences could extend internationally, eroding America's leadership position in the world community, limiting its ability to achieve foreign policy objectives, and directly impacting performance of military missions."[124] That statement appears to reflect the view that trying to shape the international environment is more important than protecting the U.S. population at home against massive casualties. The Clinton administration's 1997 National Security Strategy also emphasizes the importance of shaping the international environment to enhance U.S. and global security, as well as preventing and reducing threats stemming from proliferation.[125] It is unclear, however, how any foreign or overseas military policy can stop the proliferation of already widely available WMD technology to the multitude of rogue nations or terrorist groups that might want to acquire it.

The Right Solution

Official reports seem oblivious to the obvious conclusion: The "activist" foreign policy itself is the problem. To avoid catastrophic terrorist attacks on the American homeland in this new and dangerous strategic environment, the United States must abandon its policy of being a military nanny in every area of the world. The nation must adopt a policy of military restraint. The foremost objective of the national security policy of any nation should be to protect its territory and the lives and well-being of its citizens. Instead, Washington's excessively interventionist foreign policy undermines that objective

in order to reap amorphous gains by "enhancing stability" or "promoting democracy" in faraway places. U.S. foreign policy invites consequences equivalent to a major military conflict on U.S. soil without any compelling need to do so.

Richard Betts, director of national security studies at the Council on Foreign Relations, makes essentially the same point in a seminal article in Foreign Affairs. His policy prescriptions, however, are not entirely adequate or appropriate. For example, he argues that the United States should refrain from intervening in only some conflicts--especially those in the Middle East--and he proposes instituting a civil defense program that he admits would undermine civil liberties.

Betts correctly perceives that U.S. support for Israel (and some less democratic regimes in the region) ultimately results in many of the terrorist attacks directed against U.S. citizens and property.[126] Yet the Middle East is not the only potential source of anti-American terrorism. The worst use of chemical and biological weapons to date was that of the Japanese religious cult (with a pronounced hostility to America) in the Tokyo subway. It is also easy to imagine a Serbian terrorist group perpetrating a WMD attack on U.S. soil in retribution for perceived U.S. support of the Moslems and Croats in Bosnia. Betts, who is very perceptive about the problem, offers the following arguments for his somewhat half-hearted solution:

> Is this a brief for isolationism? No. It is too late to turn off foreign resentments by retreating, even if that were an acceptable course. Alienated groups and governments would not stop blaming Washington for their problems. In addition, there is more to foreign policy than dampening incentives to hurt the United States. It is not automatically sensible to stop pursuing other interests for the sake of uncertain reductions in a threat of uncertain probability. Security is not all of a piece, and survival is only part of security.[127]

Contrary to Betts's argument, foreign resentments can be "turned off," or at least minimized, if the United States stays out of almost everybody's business. It may take some years for the resentments to ebb, but it can be accomplished. Although a few terrorist groups may hate the United States because of its size, secular culture (that is broadcast to the world), or captialist economic system, most despise U.S. intervention in their region. After all, few terrorist groups blame the visibly secular and capitalist--

but noninterventionist--nations of Switzerland or New Zealand for their problems.

Furthermore, a policy of greater military restraint is not "isolationism." The United States could and should still enjoy free and full economic, political, and cultural exchanges with other nations. Nor is it a policy of appeasement. If any stray terrorist attack occurred after the policy was initiated, the United States should retaliate swiftly and unilaterally with the appropriate amount of force. To deter future attacks, the U.S. response should be potent. The United States should follow the advice of its own commander of Middle East forces, Gen. Anthony Zinni, who said, "Don't make enemies [but] if you do, don't treat them gently."[128]

Betts also proposes adopting measures for enhanced civil defense, including an alarming proposal for more permissive rules for government spying on "groups within the United States that might seem to be potential breeding grounds for terrorists." He maintains that this would reduce the chances of even greater restrictions of civil liberties after a massive attack, similar to the confining of Japanese-Americans in concentration camps during World War II.[129] The Defense Science Board agrees that such a destructive attack is "likely to necessitate restrictions of democratic freedoms and individual liberties."[130]

No one would argue that an attack would not create drastic pressures to curtail civil liberties at home, but it is best to take steps that are more likely to reduce the chances of such a catastrophic incident rather than undermine the free society that the security policy should be trying to protect. As noted earlier, terrorist groups are difficult to penetrate even using human intelligence agents. Although funding more civil defense measures (for example, better planning and training for emergency response by police, firefighters, and medical personnel; more equipment and training for protection and decontamination; larger stocks of antidotes for the most common agents; and public education campaigns) is probably wise, increased domestic intelligence will only bring back the abuses of the Vietnam era. It will also lead to a false sense of security perpetrated by government bureaucrats trying to make the public believe that they are "doing something" about a largely intractable problem. If more human intelligence is needed, it should be gathered overseas--not in the United States--and should be funded by redirecting resources from the satellite and other technical intelligence programs that dominated the intelligence budgets during the Cold War.

The only sure way to significantly reduce the chance of a catastrophic terrorist attack is to move beyond Betts's suggested policy of partial military restraint to one of overwhelming restraint. Intervening in nonvital conflicts just to make the foreign policy elite feel important by "leading the world" or "fulfilling the role of a superpower" should be stopped. (The stature of the U.S. foreign policy elite in world foreign policy circles is enhanced by the status of the United States as the only remaining superpower.) Such a restrained policy is especially critical in light of Betts's own argument about terrorists' use of WMD: "The odds are higher that sometime, somewhere in the country, some of these

weapons will go off, despite the best efforts to stop them."[131] Yet he supports a security perimeter that is still somewhat extended by asserting that "survival is only part of security." That statement ignores the fact that survival should be the foundation and top priority of any security policy. If an extended security perimeter undermines survival, the security perimeter should be constricted.

American Vital Interests within a Constricted Security Perimeter

The National Defense Panel, in its argument for a reemphasis on homeland defense, asserted that "protecting the territory of the United States and its citizens from 'all enemies both foreign and domestic' is the principal task of government."[132] The Clinton administration agrees with that premise. Although President Clinton's National Security Strategy for a New Century (May 1997) ultimately defines U.S. interests in a broad, muddled way, the president states in the first sentence of the document's preface, "Protecting the security of our nation--our people, our territory and our way of life--is my foremost mission and constitutional duty."[133]

The first paragraph of the body of the document reiterates the point in more detail:

> Since the founding of the nation, certain requirements have remained constant. We must protect the lives and personal safety of Americans, both at home and abroad. We must maintain the sovereignty, political freedom, and independence of the United States, with its values, institutions and territory intact. And we must provide for the well-being and prosperity of the nation and its people.[134]

Yet repeated U.S. intervention in faraway places--for, at best, incremental and ephemeral gains in security--could result in a catastrophic net loss in security if terrorist or other groups retaliated by using weapons of "mass terror" (WMD or information warfare) on U.S. soil. Even absent retaliation by such horrific means, given that the protection of American lives is universally accepted as one of the foremost goals of U.S. security policy, some assessment should be made of whether any marginal gains in security achieved by numerous interventions are worth the military casualties required to achieve them. After all, U.S. military personnel are Americans, too, and their lives should not be wasted needlessly. In Somalia, where the deaths of 18 Army Rangers precipitated a decision to quickly withdraw U.S. forces, such an assessment was unfortunately made only after the tragedy.

U.S. officials need to be far more cognizant of the potential adverse responses to Washington's policy initiatives. For example, U.S. military and economic aid to certain nations--such as Israel and Egypt--may cause nations unfriendly to those countries to covertly sponsor terrorism using WMD in the United States. Independent groups--for example, fundamentalist Islamic cells--could also sponsor acts of mass terror in opposition

to those policies. That scenario has already occurred. The World Trade Center bombing was perpetrated by an Egyptian fundamentalist group unhappy with U.S. support for the governments of Israel and Egypt.

Forgoing any incremental gains in security that might result from intervening in the Bosnias or Somalias of the world is a small price to pay for avoiding the very real potential of having an American city annihilated with WMD or the U.S. economy devastated by the sabotage of major computer systems. Although some observers might label this policy prescription "appeasement," it is most certainly not. It is a much-needed winnowing of U.S. vital interests. The United States should openly declare what limited set of interests it considers vital instead of deliberately remaining vague in the vain hope that ambiguity will deter all aggressive adversaries everywhere. If those more limited vital interests are threatened, the United States must follow through and take decisive action--unilateral if necessary--including the swift and devastating application of military power.

A Short List of U.S. Vital Interests

What are the vital interests for which it is worth risking American lives? First and foremost are those interests listed in the preface to the president's National Security Strategy--protecting U.S. citizens and territory and the American way of life. Because the United States has two weak, friendly neighbors and two vast oceans as moats, the threat to the nation's territory and citizens from a direct invasion is remote. In fact, the United States may have the most secure geostrategic position of any great power in history. Protecting the American way of life would include safeguarding U.S. trade on the high seas and intervening in Western Europe or East Asia as a "balancer of last resort." Most of the world's economic output and technological capability that doesn't come from North America lies in those two regions. If either region fell into the hands of a would-be hegemonic great power (the danger faced by the United States during World War II and the Cold War), that colossus might use the substantial added resources to threaten American economic freedom or political independence. As a balancer of last resort, the United States would rely initially on regional powers to contain expansionist states unless a shift in the balance of power threatened to bring the entire region under a hegemon's control. The United States would then help regional states oppose the dominant, aggressive power.

The Terrible Consequences of an Interventionist Foreign Policy

If the United States adopted a less interventionist foreign policy, it would be much less of a target for acts of both minor and mass terror. Using similar logic, the nation's Founders, including George Washington and Thomas Jefferson, fashioned a foreign policy that kept us out of Europe's conflicts so that the European powers would have little cause to intervene in America. That restrained foreign policy served the country well for more than a century and a half, and it should be reinstated.[135] During the Cold War, the United States reluctantly abandoned its traditional foreign policy and, in the name of fighting the

global threat of communism, sought to micromanage conflicts in virtually every region on earth. Washington tried to implement Pax Americana by forming alliances, such as NATO, SEATO, and ANZUS. After more than 50 years of such hyperactivism, the Cold War aberration now seems like the norm.

Even with the Cold War over, America's foreign policy remains on autopilot. The U.S. military is now busier than it was during the Cold War, even though no superpower rival exists to capitalize on "instability" anywhere in the world. The operations tempo of the armed forces is at an all-time high in peacetime, with deployments substantially larger, more frequent, and of longer length than during the 1980s.[136]

With the best of intentions--enhancing stability--the United States has conducted a number of ill-advised interventions in the post-Cold War environment, most notably in Somalia, Haiti, and Bosnia. Instability in such far-flung and nonstrategic areas has always been and will continue to be a fact of life in the international system. In none of those cases did the intervention have any significant relationship to U.S. security. Furthermore, such interventions rarely increase stability or make things better, even in the target country. Somalia's armed factions have continued to fight long after U.S. forces withdrew. In Haiti, the intervention was supposed to ameliorate the pervasive corruption and poverty; it has done neither. Bosnia is no closer to ethnic reconciliation and becoming a viable nation, despite the continuing presence of U.S.-led NATO forces. The NATO occupation will only delay the resumption of bitter fighting between ethnic groups that have a long history of animosity and abhor living in the same country.

In response to those types of interventions, a disgruntled faction could sponsor a terrorist attack using WMD or information warfare on U.S. soil. As the Senate Committee on Governmental Affairs noted in Proliferation Primer, the United States is now, like Gulliver, a vulnerable giant.[137] Are such questionable interventions really worth the potential catastrophic consequences to the American people? The answer is a resounding no.

Notes

1. National Defense Panel, Transforming Defense: National Security in the 21st Century (Arlington, Va.: NDP, December 1997), p. 25.

2. U.S. Department of Defense, Proliferation: Threat and Response (Washington: Government Printing Office, November 1997), p. iii. Emphasis in the original.

3. Defense Science Board, The Defense Science Board 1997 Summer Study Task Force on DoD Responses to Transnational Threats (Washington: U.S. Department of Defense, October

1997), vol. 1, Final Report, p. 15. Cited hereafter as Transnational Threats.

4. Quoted in Ted Galen Carpenter, "Reducing the Risk of Terrorism," in Cato Handbook for Congress: 105th Congress (Washington: Cato Institute, 1997), p. 456.

5. Quoted in Stanley Kober, "Why Spy? The Uses and Misuses of Intelligence," Cato Institute Policy Analysis no. 265, December 12, 1996, pp. 9-10.

6. U.S. Department of Defense, Proliferation (1997), p. 50.

7. Quoted in Barbara Slavin, "Biochemical Weapons: Poor Man's Nukes," USA Today, November 26, 1997, p. 4.

8. William Cohen, Remarks at a Department of Defense news briefing, November 25, 1997.

9. U.S. Department of Defense, Annual Report to the President and Congress (Washington: U.S. Department of Defense, April 1997), pp. 213, 215.

10. Ibid., p. 213.

11. Steven Lee Myers, "U.S. 'Updates' All-Out Atom War Guidelines," New York Times, December 8, 1997, p. A3.

12. As a result, this paper contains only a brief discussion of the threat posed by ballistic missiles. A more complete discussion will be included in a forthcoming Cato Institute analysis on national missile defense.

13. U.S. Department of Defense, Proliferation: Threat and Response (Washington: Government Printing Office, April 1996), Appendix.

14. Quoted in Richard Preston, "Annals of Warfare: The Bioweaponeers," New Yorker, March 9 , 1998, p. 65.

15. Transnational Threats, p. 22.

16. Deborah Lee, "Preparing for Terror at Home," Washington Times, March 19, 1998, p. A19.

17. Slavin, p. 2; and Transnational Threats, p. 3.

18. Transnational Threats, p. 3.

19. Carpenter, "Reducing the Risk of Terrorism," p. 458.

20. National Defense Panel, p. 51.

21. Marie Isabelle Chevrier, "The Threat That Won't Disperse," Washington Post, December 12, 1997, p. C2.

22. Carpenter, "Reducing the Risk of Terrorism," p. 458.

23. Ibid., pp. 457-58.

24. U.S. Department of Defense, Proliferation (1997), p. 49.

25. Cohen.

26. U.S. Department of Defense, Proliferation (1997), p. 51.

27. Preston, p. 52.

28. Transnational Threats, p. ix.

29. Ibid., p. 11.

30. American Broadcasting Corporation, Primetime Live with Diane Sawyer, February 25, 1998.

31. Bill Gertz, "Officials Discount Threat of Iraq Smuggling Anthrax into the United States," Washington Times, March 25, 1998, p. A3. The article notes that, although U.S. officials found no evidence of an Iraqi attempt to smuggle anthrax into the United States in that instance, British officials took the intelligence report seriously enough to tighten security at ports and airports in the United Kingdom.

32. Slavin, p. 2.

33. Lee Buchanan, deputy director, Defense Advanced Research Projects Agency, Comments at the Jane's conference on Countering Chemical and Biological Weapons: Government Programs, Industry Options, Washington, November 19, 1997.

34. Ellen Waltersheid, "Ill Wind: Living with the Threat of Biological Weapons," The Sciences, March-April 1998, p. 10.

35. Mitch Wallerstein, deputy secretary of defense for counterproliferation policy, Comments at Jane's conference on Countering Chemical and Biological Weapons: Government Programs, Industry Opportunities, Washington, November 19, 1997; and U.S. Department of Defense, Proliferation (1996), Appendix.

36. U.S. Department of Defense, Proliferation (1996), Appendix.

37. Cited in Bradley Graham, "U.S. Gearing Up against Germ War Threat," Washington Post, December 14, 1997, p. A1.

38. Cited in Transnational Threats, pp. 19-20.

39. U.S. Department of Defense, Proliferation (1996), Appendix.

40. Preston, p. 62.

41. Ibid.

42. Cited in Slavin, p. 2.

43. Steven Lee Myers, "U.S. Armed Forces to Be Vaccinated against Anthrax," New York Times, December 16, 1997, p. A22.

44. Seth Carus, "The Threat of Bioterrorism," Strategic Forum, no. 127 (September 1997): 1.

45. Graham, "U.S. Gearing Up against Germ War Threat," p. A16.

46. Carus, p. 3.

47. Ibid., p. 4.

48. U.S. Department of Defense, Proliferation (1996), Appendix.

49. Slavin, p. 2; and Paul Beaver, "The Looming Chemical Weapons Threat," Wall Street Journal, December 31, 1997.

50. Quoted in Transnational Threats, p. 35.

51. Ibid., p. 41.

52. Quoted in Thalif Deen, "UN Prepares to Counter Nuclear Terrorist Threat," Jane's Defense Weekly, February 11, 1998, p. 5.

53. James Ford and Richard Schuller, Controlling Threats to Nuclear Security: A Holistic Model, cited in Raymond Zilinskas, "The Other Biological-Weapons Worry," New York Times, November 28, 1997, p. A39; and Charles Horner, "Military Force Has Its Limits," New York Times, February 7, 1998, p. 17.

54. Ibid., p. 5.

55. U.S. Department of Defense, Proliferation (1997), pp. 49-51.

56. On the deficiencies, see U.S. Department of Defense, Proliferation (1996), Appendix.

57. Deen, p. 5.

58. Walter Pincus, "U.S. Developed 60-Pound Nuclear Weapon a Parachutist Could Deploy," Washington Post, December 23, 1997, p. A4.

59. Transnational Threats, p. 41.

60. Ibid.; and U.S. Department of Defense, Proliferation (1997), p. 51.

61. Quoted, respectively, in Gordon Platt, "New from the Navy: Wall Street War Games," Journal of Commerce, December 22, 1997, p. 1A, and Thomas Ricks, "Report of the Defense Science Board Task Force on Information Warfare-Defense," Wall Street Journal, January 9, 1997, p. 1.

62. "Cyberterrorism," American Banker, September 8, 1997.

63. Cited in Chuck McCutcheon, "Computer-Reliant U.S. Society Faces Growing Risk of 'Information War,'" Congressional Quarterly, March 14, 1998, p. 675.

64. Ricks, p. 1.

65. Quoted in "Cyberterrorism."

66. Defense Science Board, Report of the Task Force on Information Warfare-Defense (Washington: U.S. Department of

Defense, November 1996), p. 1.

67. Quoted in "Cyberterrorism."

68. Bradley Graham, "11 Military Computer Systems Breached by Hackers this Month," Washington Post, February 26, 1998, p. A1.

69. Platt, p. 1A.

70. "Cyberterrorism."

71. Quoted on the ABC television program "Cyber Terror--A Consequence of the Revolution," December 9, 1997.

72. Ricks, p. 1.

73. Transnational Threats, p. xiii.

74. ABC television program "Cyber Terror--A Consequence of the Revolution."

75. Transnational Threats, p. 51.

76. Richard Betts, "A New Threat of Mass Destruction," Foreign Affairs 77, no. 1 (January-February 1998): 32.

77. U.S. Department of Defense, Proliferation (1997), p. 60.

78. Senate Committee on Governmental Affairs, Proliferation Primer: A Majority Report of the Subcommittee on International Security, Proliferation, and Federal Services (Washington: Government Printing Office, January 1998), Summary and p. 69.

79. Ibid., p. 69.

80. Ibid., p. 70.

81. Quoted in Walter Pincus, "CIA Chief Calls Spread of Weapons Technology Top Threat to National Security," Washington Post, January 29, 1998, p A7.

82. Transnational Threats, p. 49.

83. Bradley Graham, "Clinton Proposes Inspections for Germ War Ban," Washington Post, January 28, 1998, p. A12.

84. Zachary Selden, Biological Weapons: Defense Improves, but the Threat Remains (Washington: Business Executives for National Security, December 1997), p. 3.

85. Alan Zelicoff, "Be Realistic about Biological Weapons," Washington Post, January 8, 1998, p. A20.

86. Richard Perle, "No More Halfway Measures," Washington Post, February 8, 1998, p. C1.

87. Quoted in Neil King Jr., "Iraq's Weapons Supply Remains a Mystery to U.S." Wall Street Journal, February 9, 1998.

88. Bradley Graham and Barton Gellman, "Cohen Says U.S. Would Not Seek to Topple Iraqi," Washington Post, February 1, 1998, p. A22; Joseph Cyrulik, "So We Control the Air," Washington Post, February 3, 1998, p. A17; and Andrew Koch, "Can Bombing Remove Saddam's Chemical and Biological Weapons?" Weekly Defense Monitor, February 19, 1998, p. 11.

89. Perle, p. C1; and Senate Committee on Governmental Affairs, p. 69.

90. Quoted in John Mintz, "Air War on Iraq Would Be Similar to Desert Storm," Washington Post, February 15, 1998, p. A1.

91. Gordon Oehler, former director of nonproliferation, Central Intelligence Agency, Statement at the Jane's conference on Countering Chemical and Biological Weapons: Government Programs, Industry Opportunities, Washington, November 19, 1997.

92. Ian Vásquez, "Rethinking the International Drug War," in Cato Handbook for Congress: 105th Congress, p. 530.

93. Transnational Threats, p. vii.

94. Ibid., p. C-2.

95. Colin Clark, "A Future Look at the 'Weapons of Mass Disruption,'" Defense Week, November 24, 1997, p. 1.

96. Transnational Threats, p. 49.

97. Beaver; and Transnational Threats, p. 18.

98. Transnational Threats, pp. C-10 through C-12.

99. Bradley Graham, "U.S. Forces Better Equipped for Chemical, Biological Warfare: Facing Nerve Gases and Germ Agents, Troops Still Lack Protection, Detection Devices," Washington Post, February 8, 1998, p. A29.

100. Preston, p. 60.

101. Roberto Suro and William Claiborne, "Precautions Slowed Verdict on Anthrax," Washington Post, February 24, 1998, p. A3.

102. Emily Skor, "Anthrax: Deadlier than Ever?" Weekly Defense Monitor, February 5, 1998, p. 5.

103. Paul Richter, "U.S. Germ Defenses Porous, Officials Warn; Pentagon: Troops, and Especially Americans at Home, Remain Vulnerable to Rising Threat, Experts Say," Los Angeles Times, December 26, 1997.

104. As asserted by Dr. Mike Osterholm, Minnesota Department of Health, appearing on American Broadcasting Corporation's Primetime Live with Diane Sawyer, February 25, 1998.

105. Zilinskas, p. A39; and Nicholas Wade, "Anthrax Findings Fuel Worry on Vaccine," New York Times, February 23, 1998, p. A6.

106. Transnational Threats, p. C-2.

107. Richter.

108. Transnational Threats, pp. C-10 through C-12.

109. Beaver.

110. Lee, p. A19.

111. Graham, "11 Military Computer Systems," p. A1.

112. Transnational Threats, p. 52.

113. George Seffers, "Clinton Prepares Infowar Response: Boosts Research Funds, DoD Power to Prevent 'Electronic Pearl Harbor,'" Defense News, March 16-22, 1998, p. 1.

114. National Defense Panel, p. 26.

115. Quoted in Preston, p. 65.

116. Transnational Threats, p. 40.

117. Ibid., p. 48.

118. Richter.

119. National Defense Panel, p. 25.

120. Transnational Threats, pp. 15, 14.

121. Ibid., p. 3.

122. Ibid., p. 14. See also Richter.

123. Transnational Threats, p. 20.

124. Ibid., p. 20.

125. White House, A National Security Strategy for a New Century, May 1997, p. 6; and U.S. Department of Defense, Proliferation (1997), p. 54.

126. Betts, pp. 38-41.

127. Ibid., p. 41.

128. Quoted in Bradley Graham, "Leader of U.S. Troops in Mideast: An Unconventional Operator," Washington Post, March 6, 1998, p. A33.

129. Betts, pp. 27, 38-39.

130. Transnational Threats, p. 22.

131. Betts, pp. 36-37.

132. National Defense Panel, p. 25.

133. White House, p. i.

134. Ibid., p. 1.

135. For a more detailed discussion of the merits of a more restrained foreign policy, see Ted Galen Carpenter, A Search for Enemies: America's Alliances after the Cold War (Washington: Cato Institute, 1992), pp. 1-10.

136. James Schlesinger, Testimony on the National Defense Panel Report before the Senate Armed Services Committee,

January 29, 1998; and Patrick Kelly, "Hill Critics Charge Clinton Budget Falls Short of Mission Needs," Defense Week, February 9, 1998, p. 5.

137. Senate Committee on Governmental Affairs, p. 1.