CHAPTER 4

International Terrorism

Terrorism is no longer a purely national phenomenon, which can be destroyed at a national level. It is an international offensive—an open and declared war on civilization itself—which can only be defeated by an international alliance of the civilized powers.[1]

PAUL JOHNSON

INTRODUCTION

The highly coordinated terrorist attack on the United States on 11 September 2001 shattered the myth of U.S. invulnerability to international terrorist strikes on its own territory. Four commercial airliners originally headed for the West Coast from the East Coast were hijacked. Their large payloads of jet fuel were used to turn the planes into bombs in suicide missions that cost the lives of approximately three thousand persons missing and presumed dead. Two of the hijacked airliners crashed headlong into the World Trade Center (WTC) in Lower Manhattan in New York City, and a third airliner crashed into the Pentagon in Washington, D.C. A fourth airliner thought to be targeted at governmental sites in Washington, D.C., was delayed in its takeoff. By the time the hijackers took over the plane, some passengers on the fourth airliner—who had already learned about the attacks in New York City and Washington, D.C.—rushed the hijackers, and the plane crashed into a rural area of western Pennsylvania.[2]

Reacting to the attacks of 9/11/2001, President George W. Bush (hereafter referred to as President Bush Jr.) issued Executive Order 13224—Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten to Commit, or Support Terrorism. This policy represents a vital component of any current or future U.S. effort to suppress international terrorism. It seeks to limit terrorists' access to funds and therefore constrains their ability to move freely and to acquire equipment necessary to carry out a terrorist act.

Bush Jr.'s Executive Order 13224 defines terrorism as "an activity that—(i) involves a violent act or an act dangerous to human life, property or infrastructure; and (ii) appears to be intended—(A) to intimidate or coerce a civilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of government by mass destruction, assassination, kidnapping, or hostage-taking."[3] This definition represents one of many characterizations of terrorism to be offered by government and academics over the past several decades. We discuss the problems of developing a workable definition of terrorism later in this chapter and the influence the definition of terrorism has on solutions proposed to counter it.

Terrorism has quickly become the defining threat in the 21st century. As Madeline Albright stated when she was secretary of state in the Clinton administration, "We have said over and over again that [terrorism] is the biggest threat to our country and the world as we enter the twenty-first century."[4] Some scholars—for example, Andrew J. Bacevich—disagree with Albright's claim. They believe that the threat, as described in the annual report by the U.S. State Department, *Patterns of Global Terrorism: 2000*[5], is overdrawn and a distortion of reality, given the numbers of incidences of terrorism.[6] But what kind of terrorist threat is the U.S. facing?[7] Is it a limited group terrorism such as that of Hamas, Hizbollah, the Palestine Liberation Organization (PLO), or the Islamic Jihad? Or is there, in fact, a "superterrorism" out there?

Writing in *Foreign Policy,* Ehud Sprinzak notes that terrorist groups "most likely to attempt a superterrorist attack" have fit three historical profiles or general categories of groups differentiated by their goals or orientation.[8] These include religious millenarian groups, such as the Aum Shinri Kyo in Japan, who released the nerve gas sarin into portions of the Tokyo subway system; brutalized groups whose energy is derived from a need for revenge after genocide; and small terrorist cells and/or "socially deranged" groups and individuals.[9]

According to the *Patterns of Global Terrorism Report: 2000*—despite efforts by some terrorists to acquire chemical, biological, radiological, and nuclear (CBRN) capabilities—bombing, shooting, and kidnapping continue to be the terrorists' preferred tactics.[10] These are the kinds of weapons that favor small-scale, individual actors as opposed to the larger-scale, more conventional approaches of standard military strategies. In an updated article, Sprinzak maintains his stance that a "superterrorism" (meaning a large overarching network of terrorist conspiracies) approach using weapons of mass destruction (WMD) is unrealistic. He argues there is little evidence that terrorists are in possession of sufficient quantities of CBRN weapons to execute such a terroristic attack efficiently. He further notes that the terroristic attack of 11 September 2001 is evidence of the continued reliance of terrorists on conventional terrorist tactics.[11]

In addition to issues of defining terrorism and assessing terrorists' likely tactics, the United States faces the dilemma of whether to use unilateral, bilateral, and/or multilateral approaches to fighting terrorism. How is the tension between U.S. unilateralism and U.S. multilateral efforts in the fight against international terrorism resolved? Despite the support offered the United States to form a global alliance against terrorism following the events of 11 September 2001, historically, and particularly in the 1970s and 1980s, the United States and Europe have had very different approaches to the management of international terrorism—with Europe, in fact, being considered "soft" on terrorism. Bruce Hoffman[12] argues that rather than being soft on terrorism, Europe has preferred, at least in the case of state-sponsored terrorism, a more conciliatory approach that permits conversations to continue rather than the harder, more rigid stance of the United States that is often played out as ostracism and political and economic sanctions against the terrorists and states supporting them. Europe, which has had numerous terrorist incidences occur in its member states (IRA actions in the U.K., Basque Nationalist attacks in Spain, Baader-Meinhoff Gang activities in Germany, and Algerian nationalist and anti-Algerian nationalist attacks in France, to name but a few), has considered the United States to be suffering from the narrowness of tunnel vision and seeking short-term answers when it should be adopting a broader, more long term perspective. Therefore, essentially, Europeans have been critical of the U.S. tendency to adopt what they have perceived to be reactive rather than proactive policy regarding international terrorism. As a consequence, there has been a basic disagreement between the United States and Western Europe regarding the nature and appropriate response to terror.

Not only the Western European allies of the United States but also U.S. allies in the Middle East have questioned U.S. actions and responses to terrorism. During the post–Cold War period, in which the United States is the dominant power, how do we develop a workable foreign policy against terrorism that does not strain our relationship with long-time allies in the Middle East such as Israel, Jordan, and Saudi Arabia? Moreover, how do we differentiate between domestic terrorism and international terrorism? Because the attacks in New York and Washington took place on U.S. soil, does that mean the policies pertaining to domestic terrorism apply? If so, how do we manage the findings that the perpetrators were, indeed, international terrorists? Domestically, how does the United States develop a counterterrorism policy that does not put the civil liberties of Americans at risk? Furthermore, how does such a policy deal with domestic policy actors that help manage and/or control the American economy?

In this chapter, we examine conventional terrorism, chemical and bioterrorism, nuclear terrorism, and cyberterrorism and information warfare. We examine the difficulties in defining terrorism by discussing the politics of definition, the multiple layers upon which any U.S. counterterrorism policy stands, and the challenges to sovereignty and democracy that counterterrorism policy present.

U.S. POLICY ON TERRORISM

The Office of Counterterrorism of the U.S. Department of State details the official U.S. policy against terrorists.[13] In an attempt to respond to the differences between domestic and international terrorism, a federal or national response to a terrorist attack is divided into two categories: (1) crisis management and (2) consequence management. Efforts to stop a terrorist attack, arrest terrorists, and gather prosecutorial evidence fall under the first category. Efforts to provide medical and emergency services, evacuation, and restoration of governmental services are included in consequence management.

The official U.S. policy on counterterrorism, although succinct, raises as many questions as it addresses as far as U.S. foreign policy is concerned. The first aspect of U.S. counterterrorism policy states that "no concessions be made to terrorists" and no deals struck, or as it is more colloquially called, "no blackmail, no concessions."[14] This policy "has been followed by successive U.S. administrations."[15] U.S. counterterrorism policy may be explained in part by role factors and in part by basic societal attitudes. Since terrorism has generally been considered by the American public and political elite to be a cowardly and evil activity, no administration has wished to be seen as contributing to the power of terrorists by publicly dealing with them. However, the gap between policy and practice, as Bacevich notes, can often be deep and wide.[16] From the formation of the PLO until Yasser Arafat won the Nobel Peace Prize, he and his organization trafficked in terror, establishing training camps in southern Lebanon in the 1970s to train the numerous other terrorist organizations that sprang up during this period.[17] Nevertheless, the United States had informal contacts with Arafat and the PLO. In fact, the United States has had contacts with various terrorist groups via a variety of covert means. Does this mean that once a terrorist and his or her organization obtain their political goals via terrorism, they attain legitimacy? Or does the fact that the Irish Republican Army (IRA) has entered into negotiations again with Britain make it less a terrorist organization than it was when bombings were a more frequent occurrence? To some degree, the answer from the perspective of political realism is yes. A realist perspective would judge as foolish a political leader who refused to talk to a potential adversary and therefore failed to explore ways to pressure terrorists to act more in line with the norms of international society. Moreover, properly applied, a realist perspective would accept the rationality of dealing openly with former terrorists once they have adopted concrete behavior that is more in line with U.S. interests. A failure to make these kinds of subtle distinctions would put U.S. leaders in the context of crusaders rather than pragmatists. Realist writers since Morganthau have consistently warned against a crusading mentality in foreign policy because crusaders tend to ignore a realist cost-benefit analysis in their decisions to exert national power for the achievement of national interest.

The second aspect of the U.S. policy against terrorists is to "bring terrorists to justice for their crimes."[18] Bringing terrorists to justice can present legal and cultural problems, because other countries may have different legal codes regarding extradition and different cultural points of view. For example, in 1985 extraditions from Colombia to the United States were imminent for several major drug lords. In an alliance with an urban guerilla group, the M-19, the narcotraffickers sought to prevent the extraditions. Colombia's Palace of Justice, which is analogous to the U.S. Supreme Court, was blown up by terrorists, killing all but one of the justices. It was almost 16 years before Colombia again seriously entertained the idea of extradition of Colombian nationals. Thus, the legal norms of the international system as embodied in international law present certain constraints to U.S. policy options in dealing with terrorism. These are constraints the United

States is reluctant to violate, for fear that (1) it will damage the general predictability of the international legal system that basically serves U.S. interests; or (2) it could create a precedent that will come back to haunt the United States when another state at another time uses the extradition precedent set by the United States to damage U.S. interests at that future date.

Another example of the problems with the extradition of terrorists was Libya's refusal for many years to turn over the terrorists who planted the bomb that brought down Pan Am flight 103 over Lockerbie, Scotland. Interestingly, it was a cooperative effort among British, American, and Dutch diplomats coordinated by the Secretary-General of the UN, Kofi Annan, that resulted in Libya's agreement to extradite the suspects in the bombing. In the case of Pan Am 103, the U.K. and to a lesser extent the United States had relatively strong legal grounds under existing international law to request the extradition of the Libyan suspects. Because the bombing of Pan Am 103 took place over Scottish territory, the U.K. had primary jurisdiction under historic international law. Because Pan Am 103 was a U.S. registered plane, the United States had secondary jurisdiction.

As Saudi Arabian–born multimillionaire Osama bin Laden emerged as the prime suspect in organizing the New York and Washington, D.C. attacks, the United States was again faced with territorial complications. A former member of the mujahideen opposition groups fighting the Soviet occupation of Afghanistan in the 1980s, bin Laden was given refuge in Afghanistan. Afghanistan itself was in the throes of a civil war between the Taliban, a group of Islamic fundamentalists educated and trained in Pakistan and Iran, and the Northern Alliance, a more moderate Sunni Islamic group. Controlling the capital, Kabul, and parts of central and southern Afghanistan, the Taliban had been refused recognition by all but the following four nations in the international arena: Pakistan, Saudi Arabia, the United Arab Emirates, and China. By 28 September 2001, all but Pakistan had withdrawn recognition of the Taliban as the legitimate ruler of Afghanistan. Until the United States and its allies—in cooperation with the Northern Alliance forces—faced forcing the Taliban from power, Afghanistan was considered, at the least, a semi-rogue state.

The ability of the United States to respond effectively to the attacks of 9/11/2001 was also substantially affected by existing international legal norms. Under the international legal principle of abatement, the United States was justified in taking action against Afghanistan and other states that sheltered or aided the al-Qaeda network. Abatement theory simply states that a victim state like the United States is justified in entering the territory of another state and conducting military actions if that target state has been unwilling or unable to prevent its territory from being used to mount an attack against the victim state. In addition, under the evolving international system, terrorism has become both somewhat less justified and somewhat less condoned by key states in the emerging system. That is, while the international system was a bipolar system, a conflict of ideologies between the two principal adversaries, the United States and the USSR, shaped the norms of that system, including the right and necessity to use any and all force necessary to preserve the state. This would include the use of terroristic tactics to preserve the power of the state. In the emerging multipolar system (in which there is greater agreement among key actors regarding the necessity of playing by agreed-upon rules of the game in order to minimize conflict in the system), it becomes much less acceptable for states to condone the use of terrorism to further the interests of a state or a subnational entity.

Having identified potential conspirators thought to be resident in Afghanistan or elsewhere, the United States has offered substantial cash payments for information leading to the capture and prosecution of these individuals. The United States has also coordinated efforts with European and other intelligence services in an effort to identify terrorist cells providing logistical and financial services in support of terrorist attacks. Through the capture of members of these cells, the United States, in coordination with foreign intelligence services, has attempted to trace links back to the al-Qaeda network in Afghanistan. This information serves both to counter potential future terroristic activity and to provide evidence that may be used to convince uncommitted states of the reality of the terrorist conspiracy against the United States.

The third aspect of U.S. counterterrorism policy involves measures to "isolate and apply pressure on states that sponsor terrorism to force them to change their behavior."[19] Here too, the framing of the U.S. Cold War conflict with the USSR within the context of a bipolar systemic configuration and a consequent zero-sum mentality by U.S. and Soviet leaders had an impact on the capacity of the United States to combat terrorism effectively. Within that mentality the United States was somewhat selective in identifying state-sponsored terror. Where the target of the terrorism was a communist state or its sympathizer, the United States was reluctant to identify the action as terrorism. On occasion, the United States has actually sponsored groups engaging in what other states perceived to be terroristic attacks. Stephen Zunes[20] argues that in the past, U.S. efforts to gain international support for actions aimed at punishing states that sponsor international terrorism may have lacked credibility. Many states did not agree with the selective United States' definition of state sponsorship of terrorism. Specifically, U.S. involvement in Nicaragua and El Salvador, particularly its support of the Contras (remnants of former dictator Anastasio Somoza's National Guard in Nicaragua), was viewed by many of the world's states as state-sponsored terrorism. Other examples of the contradictory U.S. stance toward state-sponsored terror include the continued designation by the U.S. of North Korea as a state sponsor of terrorism while the U.S. was sending food and energy supplies to that country.[21] More recently, in the aftermath of the September 11 attacks, the United States once again entered an agreement that would strike some as hypocritical. In an effort to elicit Russia's support in the formation of the global alliance against terrorism,[22] the United States appeared to accept Russia's claim that Chechnyan separatists cooperated with many terroristic groups, and therefore represented a threat to Russia in the wake of the USSR's disintegration.[23]

The fourth aspect of U.S. terrorism policy is to "bolster the counterterrorism capabilities of those countries that work with the U.S. and require assistance."[24] The consequences of U.S. programs to train the counterterrorist personnel of foreign governments have proven problematic in the past—the most notable example of a program being the notorious, and now closed, U.S. Army School of the

Americas at Fort Benning, Georgia. Sometimes calling it the School of Assassins, "[c]ritics have charged for years that some of Latin America's most notorious leaders and human rights abusers are among the school's 65,000 alumni."[25]

Terrorism "has become heavily politicized . . . relative to its real threat" and inasmuch as it is embedded in political problems, it requires political, not military solutions.[26] No less a person than former State Department spokesperson Richard Boucher of the Clinton administration, when announcing the U.S. agreement with Russia, felt compelled to note that the problems in Chechnya required a political, not military solution.[27] Zunes argues that in addressing the issue of state-sponsored terror, U.S. foreign policy has focused on unilateral military rather than political solutions to terrorism.[28] In addition, Zunes claims that the United States' overreliance on military rather than political solutions to terrorism has impaired its credibility internationally, because civilian casualties increase during military responses.

THE SOURCES OF TERRORISM

According to journalist David Lamb, terrorists are often young people with little faith in any kind of future—and more frequently, impoverished and undereducated.[29] When these characteristics occur in a historical context of cyclical violence, such as that generated by the attack by Israel on the Palestinian refugee camps Sabra and Shatilla, then the overwhelming discontent from which new terrorists emerge is created. Abu Nidal, the terrorist behind the hijacking of the cruise ship *Achille Lauro,* recruited his terrorist teams from the Sabra and Shatilla camps.[30]

Not everyone agrees about the sources of terrorism or the preference for a political rather than a military solution. Paul Johnson argues that terrorism is not a symptom of some "deep-seated social malaise" or frustration. Rather, "it is a specific and identifiable problem on its own; and because it is specific and identifiable, because it can be isolated from the context which breeds it, it is a remediable problem."[31] Johnson believes that terrorists are not "idealists pursuing worthy ultimate aims." Rather, Johnson considers terrorism and terrorists an intrinsic, evil phenomenon that should be rooted out.

According to Johnson, the reasons that terrorism is evil can be called the seven deadly sins of terrorism: (1) exaltation of violence as interest articulation; (2) suppression of moral instincts, as terroristic training provides its recruits with justification for murder; (3) the substitution of violence for politics; (4) spread and support of totalitarianism inasmuch as terrorists are ideologically driven and to maintain momentum cannot allow any dissent; (5) destruction of democracy; (6) exploitation of freedoms provided in democratic states; and (7) "sapping the will of a society to defend itself."

OUTLINE OF THE U.S. POLICY RESPONSE

Johnson's argument is a strong, frightening, and compelling one. Yet in the presence of recent statistics, how valid is it as a set of assumptions guiding U.S. foreign policy? The annual reports—*Patterns of Global Terrorism*—released by the Office of the Coordinator for Counterterrorism from 1995 to the present show variations from year to year in the number and type of terrorist attacks. For example, the 2000 report indicates there was an increase from "392 attacks in 1999 to 423 in 2000."[32] Whether these are trends or simply statistical aberrations remains unclear. Still the number of attacks hardly seems to have justified the considerable expenditures on counter-terrorism in the U.S. budget,[33] according to Bacevich. There will be less disagreement in the future about the importance of budgetary allocations for terrorism in light of the September 11 attacks. In fiscal year 2001 of the U.S. government, approximately $11 billion was projected to be spent on counter-terrorism compared to $1.552 billion for combating WMD and $2.027 billion for the protection of critical infrastructure. In testimony before the Subcommittee on Oversight, Investigations and Emergency Management, the Committee on Transportation and Infrastructure, House of Representatives during April 2000, the U.S. government's own General Accounting Office (GAO) reported that, despite such excellent funding, there were significant deficiencies regarding the United States' ability to respond to terrorist threats, its national strategies, and agency resources.[34]

The GAO reported that most of its findings complemented those of the Gilmore Panel.[35] However, there continues to be a lack of consensus among politicians, bureaucrats, and analysts regarding definitions of the terms *terrorism, weapons of mass destruction,* and *mass casualties,* as well as other key concepts around which federal programs are built and upon which the allocation of resources is determined. Additionally, whether the monies are spent on domestic or international terrorism, the lack of a conceptual consensus thwarts the allocation, oversight, priorities, and development of both a domestic and an international strategy for either short- or long-term objectives. (See the next section, "Definitional Quagmires," for a further discussion of the difficulty in defining terms relevant to terrorism.) In the absence of a conceptual consensus, it has been difficult to develop a coordinated policy. Rather, the U.S. approach was marked by an incremental decision-making approach (described on pages 29–31), at least until 9/11/2001.

How money is spent to fight terrorism should depend in some way upon which tactics terrorists are currently using. In 1990 Brian Jenkins noted, "Terrorists operate with a limited tactical repertoire. Six basic terrorist tactics comprise 95 percent of all terrorist incidents: bombings, assassinations, armed assaults, kidnapping, barricade and hostage situations, and hijacking. No terrorist group uses all of them. Bombings, generally the least demanding of tactics, predominate. . . ."[36] These same tactics remained very much in evidence in the 1990s, according to the Combating Terrorism Report, which revealed that 111 bombings occurred against U.S. citizens in 1999, with kidnapping and firebombing occupying second and third place as the most common terrorist tactics. However, this report reflects the criticisms of the GAO and Gilmore panel about definitions and classifications. Note that nowhere in that report is either a nuclear, biological, and chemical weapons (NBCWs) or cyberterrorist attack listed.

As Italian General Guilio Douhet, a revolutionary leader from an earlier period, once said, "Victory smiles upon those who anticipate changes in the character of war, not upon those who wait to adapt themselves after the changes occur."[37] Nowhere has this become so evident as in the rapid technological development in NBCWs and information warfare. U.S. budgetary and policy priorities must anticipate the nature of future terrorist attacks in order for the United States to be ready for new forms of attacks.

Further decisions remain regarding how to proceed after terrorist attacks. James Lindsay, a senior fellow at the Brookings Institution, and Gregory Michaelidis of the Hatcher Group, note that the Bush Jr. administration has been particularly aggressive in its unilateral withdrawal of U.S. support from treaties such as the Kyoto Protocol, the Biological Weapons Convention, and an International Criminal Court. This tendency to unilateralist solution may be a product of several factors. To some degree, this attitude reflects the hegemonic position of the United States in the international system. This attitude may also reflect a realist approach to policymaking (pages 22–24) that stresses state responsibility over multilateral approaches. However, the diffuse nature of the al-Qaeda terrorist network makes a unilateral U.S. response to the attacks of 9/11/2001 less than an optimal means of addressing the terrorist threat posed by that group. Consequently, in efforts to build support for a global alliance against terrorism, the Bush Jr. administration finds itself scrambling to create coalitions of consensus about strategies of retaliation and security concerns in the post-WTC and Pentagon attacks.[38]

Similarly, prior to the 9/11 attack, writing in *Le Monde* on 8 September 2001, Philip Gordon and Justin Vaisse noted that European observers had concluded that "an incorrigibly unilateralist Bush administration was hostile to international cooperation as a matter of principle." [39] The case of Iran illustrates the difficulties that the United States has as a result of being perceived as overly unilateralist in its foreign policy orientation. Reacting to its perception that the United States was in fact pursuing a unilateralist posture toward Afghanistan's support of terrorists, Iran reconsidered its earlier support for action against Afghanistan. In the dizzying round of deal making that accompanied efforts to build the global coalition, Iran amended its earlier support of such a coalition, saying it would support a UN-sponsored initiative but not a U.S.-led initiative, noting that securing the Iran/Afghan border is of central concern to Iran but not to the United States, which does not need Iran's border.[40]

Given current U.S. policy, how would we even determine which government or even groups and individuals to hold responsible? How does one charge a terrorist whose only crime may be the destruction of some property? Yet, that destruction could damage the environment beyond repair, leading in turn to damage to the economy and possibly culminating in political instability.

What is clear is that the randomness and overwhelming damage that can be done by a terrorist attack, particularly in light of the terrorist attacks of 11 September 2001 in New York City and Washington, D.C., will keep it at the top of the U.S. foreign policy agenda for some time to come. Although we can use numbers and graphs to show that terrorism is overrepresented in the U.S. budget relative to the instances and numbers of casualties, it would be a serious error to underestimate the influence political rhetoric—generously laced with moral suasion—has on political mobilization.

In the following section, we review some of the traditional definitions of terrorism and the problems associated with the classification of terrorism.

DEFINITIONAL QUAGMIRES

Definitions reflect the interests of those doing the defining. The act of defining itself involves an exercise of power. Therefore, definitions should not be regarded as anything but tools whose value lies in how close they permit us to approximate an ideal. As we enter a few definitional quagmires, or definition difficulties, we need to bear in mind that definitions often reflect politics and special interests. Those who do the defining often do so in a way that benefits their interests, whether they be groups or individuals. Thus, it is important to understand that the development of definitions represents an effort to shape and influence the policymaking process.

Definitions of terrorism draw from Just War doctrine, which posits that targets of attacks should be combatants (principle of noncombatant immunity), and that initiators of attacks should be highly discriminating in the choice of targets, meaning that incidental damage to noncombatants should be minimized. In other words, terrorists typically direct their threats and violence to both the actual soldiers of a state, or combatants, and ordinary citizens, or noncombatants. (Bush Jr. was following the principles of just war when he attempted to avoid civilian attacks and casualties in the Afghanistan conflict in 2001.)

In defining terrorism, the U.S. Department of Defense (DoD) is careful to distinguish between terrorism and other kinds of violence. The DoD definition of 1989 stated that terrorism "is the calculated use of violence or the threat of violence to inculcate fear, intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological."[41] Subsequently, departments of state and of defense attempted to find a definitional middle ground when defining terrorism as

> *premeditated, politically motivated violence perpetrated against a noncombatant target by subnational groups or clandestine state agents, usually intended to influence an audience. "International" terrorism is terrorism involving the citizens or territory of more than one country.*[42]

Some insurgents are terrorists, but insurgents are not terrorists if the insurgents abide by rules of war, refraining from acts of violence declared as terroristic acts. As mentioned in Chapter 5, "Transnational Organized Crime" (TOC), one of the complications of interactions between state and non-state actors[43] is the legitimacy of the claims of the non-state actor that such negotiations imply. Modern terrorism, on the other hand, targets noncombatants indiscriminately, defying attempts to draw some kind of line between insurgency groups and terrorists, legitimate claims and illegitimate claims, and representation and no representation. This has produced what Peter Chalk calls the "Gray area phenomenon" (GAP), by which he is referring to the threats that non-state actors and nongovernmental actors pose for sovereign states.[44]

So why does terrorism "terrify"? Chalk categorizes GAP into violent and nonviolent activities and notes "that because GAP are not directed or controlled by states, traditional defenses that governments have erected to protect themselves and their citizens are generally impotent against them."[45] Terrorism becomes all the more real when civil order is disrupted by the killing of noncombatants far from the battlefield, in some cases on the other side of the world from it. Who can forget the images from the 1985 capture of an Italian cruise ship, the *Achille Lauro,* by Palestinian terrorists that culminated in a wheelchair-bound American Jew, Leon Klinghoffer, being shot and then shoved off the end of the ship in his wheelchair? Who will ever forget the sight of the twin towers of the WTC's 110 stories crumbling to the ground, entombing those who did not leap from the windows?

Arguably, there are two general categories of terrorism: dissident terrorism and establishment terrorism.[46] Terrorists who are "dissident" are rebelling against an established order; those who are "establishment" are operating as part of the established order in an attempt to control and dominate their peoples. Sederberg points out that further distinctions of subtypes may be made in each general type, keeping in mind that the distinctions may blur between the types along a continuum. Whether to categorize terrorism as dissident or not depends upon the comprehensiveness and coherence of political objectives and ideological agendas of those doing the defining and categorization. Moreover, as it affects U.S. foreign policy, this defining occurs against the backdrop of historical context, the particular actors involved, and the competing interests at play.

Sederberg distinguishes among several types of terrorism, which provide a framework for understanding the motivations of terrorist groups. It is useful to contrast these types. "Criminal terrorism may be a tool of groups (or even individuals) with no systematic political agenda. Nihilists possess such an agenda, but it is essentially negative: the destruction of the existing order."[47] Care should be taken in labeling any terrorist nihilist. "Unfortunately, the political weakness of the nihilists is precisely what may make these groups more likely to use tactics of mass destruction."[48]

The distinctions between criminal terrorism and nihilist terrorism have become increasingly blurred. However, it is clear that some groups have definite political underpinnings. For example, groups that can have been said to engage in nihilist terrorism include the Red Army Faction and, arguably more recently, the al-Qaeda—the terrorist network financed and led by Osama bin Laden.

U.S. foreign policy may operate within coalition-building operations such as it did in Somalia in 1993 when the United States was part of the UN peacekeeping force. However, the peacekeeping operation did not have the support of important factions in Somalia. Osama bin Laden was originally a member of the mujahideen, who were financed and supplied by the United States in its proxy fight against the USSR in Afghanistan. In the aftermath of the expulsion of the USSR from Afghanistan, bin Laden trained Somali tribesmen in support of regional warlord Muhammad Farad Aideed. In addition, bin Laden became disaffected with the United States due to its continued presence in Saudi Arabia in the aftermath of Operation Desert Storm. When the United States became part of the UNOSOM II peacekeeping force in Somalia in 1993, the bin Laden–trained Somali tribesmen staged ambushes that left 18 U.S. Army Rangers dead and prompted the U.S. withdrawal from Somalia.[49]

Sederberg states that nationalist terrorism relies upon the successful appeal to the discontents of a significant group of a population. Most often these tend to be communal groups such as the Basque separatists, the Sikh separatists, the Irish Republican Army (IRA),and the PLO.[50] The numerous terrorist attacks of groups operating under the umbrella of the PLO—Hamas and Hizbollah being the better known—consistently use U.S. foreign policy and its support of Israel as the rationale for their attacks. U.S. support for Israel is rooted in the aftermath of World War II and the Holocaust as well as Israel's steadfastness as a U.S. ally and "listening post" for the United States in the Middle East during the Cold War period, when the United States and the USSR competed for supremacy in the region. U.S. support for Israel without sufficient condemnation of Israel's treatment of Palestinians remains a principal justification used by groups such as Hamas, Hizbollah, and bin Laden's al-Qaeda for their terrorism.

Establishment terrorism refers to violence used to defend the dominant order from some type of threat or subversion. This can include vigilante terrorism, which is perpetrated by private citizens with the intent to defend and preserve the established order. Another subtype of establishment terror includes covert official terrorism, which is perpetrated by public citizens. Examples would be the Guatemalan government's creation of death squads such as the Mano Blanco in the 1980s and U.S. support for the repressive governments of Guatemala, begun in the 1950s with the CIA-supported overthrow of the Jacobo Arbenz regime—which was thought to be too "leftist" for this Cold War period. Overt regime terrorism is the use of terrorism to enforce rule, or as Sederberg puts it, "to legalize terrorism."[51] Dating back to the time of Shaka Zulu in Africa, pitting family against family by requiring them to murder each other was meant to break the social organization of the kinship/clan model and redirect it toward a supreme leader. The attempt by the Nazis to exterminate the European Jews was an example of genocide. Genocide terrorism institutionalizes terroristic activity.[52]

Sederberg claims that at the extreme of establishment terrorism is genocide. Genocide institutionalizes terrorism by focusing on a particular group. While often brutally repressive, most authoritarian governments do not engage in genocide. Nevertheless, U.S. foreign policy has sustained considerable criticism for its support of authoritarian regimes such as those in Guatemala, El Salvador, and Nicaragua in Latin America, and Zaire and the Republic of South Africa in Africa.

U.S. terrorism policy has been plagued by an inability, or perhaps unwillingness, of policymakers to unlearn inappropriate lessons from the past. Consequently, the policy is marked more by organization processes (described on pages 28–29) than a rational examination of policy in light of changed circumstances. Part of the problem for U.S. foreign policy in dealing with terrorism in the 21st century is that many of the definitions are left over from the Cold War period, when a series of myths about terrorism prevailed within the Cold War context. Michael Stohl identifies what he believes are myths of terrorism[53] (from the literature up to the 1990s) that have dominated or at least influenced U.S. foreign policy. The first myth is that the use of terrorism is limited to nongovernmental actors and, despite evidence to the contrary (such as the French government's involvement with bombing the Greenpeace ship the *Rainbow Warrior* and U.S. involvement in Central America), the myth persists.

"All terrorists are madmen" is a myth that might be useful rhetoric to help in political mobilization, but it is a poor basis on which to ground foreign policy.

Bruce Hoffman concurs. As Nicholas LeMann observed, "Hoffman's view is that all terrorists have goals, and that it is dangerous to see them only as madmen bent on destruction. In other words, we should not only recognize their capability for mass murder but also make a serious effort to understand how they think in order to anticipate their movements. We need a new theory of terrorism."[54] "All terrorists are criminal" is a myth that suggests terrorists are lone rational actors and eliminates state-sponsored terrorism from consideration—at least in principle, if not in practical application. It is much easier to bring a lone individual or group to justice than it is a sovereign nation-state that one might have been supporting for a variety of other reasons.

Kshitij Prabha notes that it took the UN General Assembly 15 years to conclude that terrorism is a criminal act and should be treated as such.[55] It is ironic that the two powers voting against the resolution were the United States and Israel, with Honduras abstaining. While this might be the simplest way to treat terrorists, the absence of a resolution adopting a compulsory extradition treaty for exchange of criminals renders the definition of terrorism as a criminal act irrelevant.

"All insurgent violence is political terrorism" is a myth that complicates policymaking and ignores the context within which guerrilla groups must exist and find support.[56] Engaging in terrorist acts that often maim and kill civilians is not the way to gain support for one's political agenda. Although terrorism might be used during the revolutionary phase of a takeover of the old regime by the new, it is not a satisfactory method once the new regime is established. Afghanistan following the Soviet withdrawal is an example of this. The Northern Alliance of the 1990s was simply a patchwork of elite-dominated interest groups derived from former Afghani elites and mujahideen, now without a mission. The inability of the Northern Alliance to govern effectively and the terrorizing of elements of the civilian population by various factions of the Northern Alliance in the countryside made the restoration of law and order by the Taliban—albeit a harsh version of Islamic law and order—preferable to the daily terror experienced by the average Afghani. Vigilantes, whether of the political left or political right, have always been tolerated by governments seeking to impose their will upon or intimidate their people. Certainly, the paramilitary death squads in Colombia could not have persisted without government tolerance, if not acquiescence.

Another myth is that "political terrorism is exclusively a problem related to internal political conditions."[57] Terrorists don't limit themselves to directly responding to conditions in their own home states. Rather, they may be prompted to conduct terrorism or aid others in conducting terrorism in other states that they perceive to be allied causes. For example, Qaddafi in Libya has been rumored to be a source of support for the IRA in Ireland, and Castro in Cuba actively sent troops to fight in Angola. Certainly, the covert CIA operations where assassinations occurred have been considered by some to be instances of state terrorism.

A final myth we will discuss (although there are several others according to Stohl) is that "terrorism is a strategy of futility."[58] There is considerable disagreement among scholars as to whether or not terrorism achieves any political success. Perhaps at the root of the disagreement is a lack of consensus on what a terrorist would consider a success. Clearly, the attack on the WTC and the subsequent shakiness of the American financial markets would be considered a political success. Similarly, being able to breach security at the Pentagon would be considered successful. Understanding and elaborating upon these myths is important because myths may be used to prop up and/or build support for U.S. foreign policy.

Prabha notes that "in the absence of an agreed-upon definition of terrorism, it is difficult, if not impossible, for states to mount effective individual or collective action through the United Nations or other international organizations against international terrorism."[59] He proposes that terrorism is best defined from two perspectives. The first is a political perspective that defines terrorism as a political phenomenon in its group action and through its international linkage. Although social and economic problems may contribute to the rise of terrorism, the acquisition of political power is the ultimate goal of the terrorist. It also allows the researcher to include the organizational dimension of terrorism, which is closer to that of a political party than a criminal gang; although, as we point out in Chapter 5, "Transnational Organized Crime" (TOC), understanding a group's international linkage can provide a glimpse into its organizational structure.

Group action is a critical element in any definition of terrorism. Indeed, the 20th century is littered with political parties, such as the All India Sikh Students Federations in Punjab and the All Party Hurriyat Conference in Jammu and Kashmir, which were unsuccessful in using political means to have their demands met and resorted to political violence within their own countries. However, one must also consider a group's international connections. The level of global terrorist threat is dependent on the group's international linkages.

Changes in technology generally available to states in the international system (described on pages 13–14) have contributed to the increased capacity of terrorist groups to create new linkages and pass funds and materials to their operatives by way of these linkages. Kashmiri militants have received military and financial assistance from rebels in Pakistan and Afghanistan. Evidence from intelligence sources that Libyan mercenaries provided logistical and financial aid to the IRA prompted then Prime Minister Margaret Thatcher to approve of the U.S. attack on Libya in 1986.[60] As regards U.S. foreign policy, a political solution recognizing terrorist acts as a means of articulation might increase the room for change in policy. Take the examples of the U.S. support of the rapid departure of Central American dictators such as Anastasio Somoza from Nicaragua as well as the Duvalier family from Haiti. This support indicated the United States was aware that governmental suppression of the exercise of free assembly and criticism of governmental actions could lead the population to eventually resort to terrorism as a mechanism to express their dissatisfaction with governmental policies. However, the support flies in the face of stated U.S. policy of "no concessions, no deals."

Prabha's second perspective emphasizes the requirement of violence as a means to a political goal. Terrorist tactics are not random. Rather, they are well planned to take advantage of environments of unrest and fear. Prabha brings up the interesting technological changes we see in the 21st century and makes the important point that machine guns, bazookas, missiles, transistor bombs, letter bombs, cyanide, and RDX require proper training to operate. Failure to do so could prove fatal to the terrorist and his or her group.[61] (This would seem to support Paul Johnson's argument that terrorist acts can be separated from the context that nurtured them.) During the 1970s, when airplane hijackings at times seemed to be a daily occurrence and U.S. foreign policy appeared mired in Cold War agendas, the spate of aviation legislation served the United States well in returning safety to airline travel.

Prabha offers the following definition of terrorism and one we shall use from this point on in this chapter: "Terrorism is an act or threat of an act of tactical violence by a group of trained individuals, having international linkage, to achieve political objective. This group could be sponsored by non-state or state agencies."[62]

CONVENTIONAL TERRORISM

By *conventional terrorism* we are referring to bombing of all types, whether it is turning hijacked commercial jetliners into bombs, for example, or a suicide truck bomber driving his truck into the U.S. Marine barracks in Beirut in 1983. The events of 11 September 2001 showed an escalation of "conventional terrorism," in that more individuals were killed on that day in the three attacks plus the downed plane than in any terrorist incident in the period from 1980 to 1996 or the subsequent four years.[63] The use of commercial airliners aimed at symbols of U.S. pride and security left most people shocked as images of the twin towers of the WTC and the Pentagon flashed on television around the clock.

After the attacks on 11 September 2001, Bush Jr. issued an executive order activating reservists to support Operation Noble Eagle, the homeland defense policy. So far, no deals have been struck with anyone claiming responsibility for the airplane suicide attacks. As for the second part of U.S. counterterrorism policy, investigations into who was linked to the bombing and collection of evidence continued until Secretary of State Colin Powell announced later in September 2001 that Osama bin Laden was considered the primary suspect along with numerous followers identified in the United States.

In the aftermath of 9/11/2001, President Bush Jr. was placed in a somewhat awkward position given his prior emphasis on unilateral actions in foreign affairs. Efforts to isolate Afghanistan, the acknowledged base of bin Laden's operations, intensified after a private telephone message from President Bush to the President of Pakistan, Pervez Musharraf,[64] in which Musharraf agreed to allow the United States to use Pakistani airspace to launch attacks against the Taliban. (Pakistan was one of the few nations that ever recognized the Taliban as the legitimate rulers of Afghanistan.) Iranian leaders unilaterally ordered the closing of Iran's 559-mile border with Afghanistan,[65] with whom it has had long-standing border disputes. When interviewed, Taha Hashemi of Iran suggested such a peremptory move by Iran was meant to establish trust between Iran and the United States. Once trust was established, this trust could be used to discuss other pressing problems (from Iran's point of view) between the two countries, including the still-frozen Iranian assets in the United States as well as removing Iran from its list of terror sponsors in order to begin a sanction-lifting process.[66]

U.S. European allies quickly lined up in support for the United States, as did many Arab nations in the Middle East. Thus, all four prongs of the official U.S. Department of State counterterrorism policy were in place. The attacks upon the United States on 9/11/2001 also triggered shifts at the societal level (described on pages 19–20) within the United States. These shifts in societal attitudes have had some influence on how the United States has sought to address the problem of terrorism. The shifts reflect a change in public attitudes in the direction of greater tolerance for discretionary action by U.S. leaders in their efforts to meet the challenges posed by international terrorism. Specifically, a number of U.S. interest group leaders called upon the president to rescind the executive order issued by then President Gerald Ford in 1976 forbidding assassinations.[67] Previously unknown, but revealed in a report by CBS news correspondent Leslie Stahl, was the fact that in 1998, then President Bill Clinton issued another executive order that permitted the CIA to go after bin Laden and either bring him in to stand charges for terrorism—or, failing that, kill him. The directive remains active in 2002 because it was written based on an exception clause that would permit such actions if someone were deemed a serious enough threat to national security.[68]

To some degree, societal factors (described on pages 19–20) have come into play in another aspect of U.S. antiterrorist policy of the 1980s and 1990s. That is, certain U.S. responses to terrorist attacks on U.S. interests have been designed in ways more calculated to win favor with U.S. public opinion than to be truly effective in stopping or weakening the perpetrators of that terrorism. In a quite dismal mood, Zunes suggests that "the U.S. war against terrorism [has] often taken the form of foreign policy by catharsis."[69] (Foreign policy by catharsis is the response to terrorist activity by a brief shelling or bombing campaign against suspected training areas of the purported terrorists.) "U.S. foreign policy is far too focused on military solutions, including bombing raids by cruise missiles and fighter aircraft against targets in foreign nations."[70] As Zunes has noted, "such air strikes have played well with the American public, because they give the impression that the U.S. is taking decisive action to strike back at terrorists."[71] Does it though? And if so, why does it? Do the criticisms of Zunes and others mean there is no place for military intervention in dealing with terrorists? The framing of foreign policy as a response to terrorist acts is hampered by the rhetoric of war embedded in 50-plus years of a bipolar power configuration dominating the international arena. War as conventionally fought does not seem to have a place in this new threat to national security. So what language can be used to enable us to develop a foreign policy response appropriate to the threat issued?

Sederberg argues that counterterrorism policy is, too often, derived from the two mythic solutions of reprisal and conciliation (which, in turn, are derived from the myths of terrorism described earlier in the chapter). He states that "neither reprisal nor conciliation is likely to be an appropriate response to all cases."[72] The first mythic solution is one calling for severe retribution, understandable given the severity of terroristic violence. It is driven, even when directed at state-sponsored terrorism, by the perception that terrorists are mad dogs and the conclusion that groups and states must be dealt with severely. Certainly this seemed to be the case, as reported in the media, when President George Bush Jr. vowed to "rid the world of evil-doers."[73]

"The other mythic solution," Sederberg proposed, "exaggerates the capacity of conciliation, or compromise, to cure terrorism,"[74] de-emphasizing the role of external sponsors and calling for eradicating the social and economic conditions that nurture terrorism. In adopting policies derived from the second myth, the immediate issue of security concerns is missing. Sederberg reexamines the importance of context in framing an appropriate response to terrorism while realizing that other pressures such as the influence of external sponsors can move context farther down a list of priorities.

Prabha's definition of terrorism allows us a wider scope to examine U.S. foreign policy as it relates to two types of terrorism: (1) nuclear, biological, and chemical weapons (NBCWs) terrorism and (2) cyberterrorism and information warfare; the first of which has had limited expression and the other of which is having increasing expression. In the next section, we examine U.S. foreign policy with regard to the NBCWs, followed by a look at cyberterrorism. We conclude the chapter by incorporating some of the factors to be considered in framing a foreign policy response to dissident groups of terrorists.

NUCLEAR, BIOLOGICAL, AND CHEMICAL WEAPONS TERRORISM

The use of chemical and biological weapons is as old as civilization. During the Peloponnesian War, the Spartans created toxic fumes by igniting pitch and sulfur.[75] The use of plague-infested corpses occurred in the Crimea by the Mongols in 1346 and arguably by Russian troops against the Swedes in 1799. By 1899 the Hague Convention (II) prohibiting the use of poison or poisonous weapons was signed. A mere 16 years later, the Germans attacked the French with chlorine gas, marking the first significant use of chemical warfare in World War I.[76] The use of chemical weapons (CWs), including mustard gas used in World War I, led to the Geneva Protocol of 1925. The protocol prohibited the use of chemical and biological weapons (CBWs), but did not prohibit research or production of these agents. By 1937 the Japanese had begun their offensive CBW program and by 1940 had dropped a mixture of rice and wheat laced with plague-carrying fleas over China and Manchuria. The United States, in 1942, developed its own offensive biological weapons program. During the Vietnam War the United States used the chemical weapons of tear gas and defoliants (the best-known defoliant used was Agent Orange). In 1970, under pressure from continued demonstrations and amid daily press revelations that the U.S. intelligence services were behaving more like rogue agencies than institutions accountable to the executive, President Richard Nixon ordered the unilateral dismantling of the U.S. offensive biological warfare program and ordered all stockpiled weapons destroyed.[77] That same year there was an outbreak of pulmonary anthrax in Sverdlovsk, USSR; 64 of the 100 Soviet citizens affected died, suggesting that existing biological weapons were not always under the sufficiently strict control of states.

Changes in the distribution of technological capacities of states in the international system (described on pages 13–14) have played an important role in the emergence of chemical and biological weapons of mass destruction as issues in U.S. foreign policy. Numerous states have had the capacity to research and develop their own stockpiles of chemical weapons (see Appendix A to Chapter 3). A somewhat smaller number of states have the capacity to develop and refine biological weapons capable of mass destruction. Even fewer states have the technological capacity to develop viable nuclear weapons of mass destruction (WMD) on their own. Some states have had a large capacity to research and develop their own stockpiles of NBCWs—and have done so. Although conventional weapons such as high-powered explosives and firearms typically remain the weapons of choice for dissident group terrorism, state-sponsored terrorism has the access and ability to take advantage of the technological advances in weaponry. And it is the nexus between terroristic-oriented states and non-state actors that presents the dominant security challenge of NBCW terrorism in the 21st century. Iraq's use of CWs (hydrogen cyanide, mustard gas) in its Anfal Campaign against the Kurds, most notably in the Halabja Massacre of 1988, repulsed the international community and heightened concerns about CW. Dr. Kanatjan Alibekov, former first deputy director of Biopreparat, defected to the United States and confirmed the existence of Russia's offensive biological program including the use of smallpox in weapons manufacture.

Scholars Nadine Gurr and Benjamin Cole identify three waves of vulnerability to the proliferations of NBCWs that the United States has faced beginning in the Cold War period.[78] The first wave followed the successful testing of an atomic bomb by the Soviet Union in 1949. No longer was the United States the sole military superpower. The second wave developed as a result of the spiraling superpower nuclear arms race that followed the first wave; and the third wave, dating from 1995, has been vulnerability to NBCWs.

From 1947 to 1951 U.S. strategic superiority eroded in the face of rapid acquisition by the Soviet Union of nuclear technology and weapons. And while the United States remained on par with the USSR during the Cold War, an era dominated by its arms races, the sense of vulnerability that had marked the Cold War was alleviated with its end in 1991 following the fall of the USSR.

The third wave of U.S. vulnerability to NBCW terrorism was foreshadowed by the attack on passengers in the Tokyo subway system by a Japanese religious cult, the Aum Shinri Kyo, or Aum Supreme Truth, using the CW sarin. The political context of a liberal democracy (Japan) experiencing such an attack, and the targets being institutions and/or public transit that carried large numbers of people, represented a shift from a well-defined enemy in the form of a superpower to an international arena where threats were perceived as coming from more amorphous regional actors, as well as from a proliferating group of non-state actors to include terrorist groups, criminal organizations, and TOC groups. The Tokyo subway attack resulted in discussions of chemical and biological warfare shifting from the theoretical to the policy-relevant.

Beginning in the 1990s, technological advances in weaponry revealed the vulnerabilities of the United States and brought into question its foreign policy on counterterrorism. Additionally, the bombing of the World Trade Center (WTC) in New York City by Islamic fundamentalists in 1993; the bombing (by an American far-right extremist) of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma, in 1995; and the assault on the WTC in New York City as well as the Pentagon in Washington, D.C., demonstrated all too clearly that the United States was indeed vulnerable to terrorist attacks on its own soil.

The explosive growth of the biotechnology industry in the 1990s, the fact that biological weapons can create mass casualties, and the ease of transport and greater accessibility of these weapons increased concerns about bioterrorism. As noted in Chapter 3, the Chemical Weapons Convention (CWC) was negotiated in

1992 prohibiting the research and production of offensive CWs. By the mid-1990s, Iraq had developed a significant offensive biological weapons capability including anthrax, botulinum toxin, and aflatoxin. In 1998 Iraq clashed with the UN Security Council. Baghdad refused to allow UN Special Commission inspectors to visit potential undeclared CW sites as authorized under the CWC.[79]

Compared to incidences of conventional terrorism, NBC—nuclear, biological, and chemical terrorism—has an even smaller incidence. However, the lethality of NBC terroristic weapons could conceivably outweigh that of conventional terroristic weapons. Chemical weapons are poisonous substances that can incapacitate or kill when touching the skin or entering the body. Categorized into three basic types, these include choking agents, such as chlorine; blood gases that block the transport of oxygen, such as hydrogen cyanide; vesicants that burn and damage body tissues, such as mustard gas; and nerve agents, such as tabun and sarin. (Sarin was used by the Aum Shinri Kyo group in the Tokyo subway.)[80] The term *biological weapons* (BW) refers to pathogenic microorganisms or biologically produced toxins, which can cause illness or death directly upon contact or indirectly by contamination of water supplies and agricultural sources. Nuclear weapons wreak damage through the release of energy through "nuclear fission, splitting the nuclei of elements such as plutonium, or through a combination of fission and fusion, combining hydrogen nuclei to create helium."[81]

Until the early 1980s, terrorism was considered less a military security problem than a civil and police problem. Terroristic events in the 1970s—such as the kidnapping and massacre of Israeli athletes at the Munich Olympics by Palestinian terrorists in September 1972 and, in 1979, the seizure of the U.S. embassy in Tehran—sounded a warning bell to world powers to rethink their policies and reevaluate their organizational structures and tactical objectives. Until the 1990s, most scholars and policymakers thought the probability of any widespread terrorist attacks by non-state actors using NBCWs was small given the requirements of the knowledge necessary to develop the weapons, a reliable mechanism of delivering the weapon that would not endanger the terrorists in the process, and the problems involved in transporting the NBCWs.

This perception of the low probability of an NBC attack by non-state actors changed in the 1990s. CBW terroristic events ranged from a spate of anthrax threats in southern California in 1998 to the bombing of Russian apartments when the dissolution of the USSR unleashed dissident factions within Russia. Subsequent investigations of the Moscow bombings revealed a larger security threat at Russia's nuclear installations.[82] U.S. response in conjunction with Russia and the Newly Independent States (NIS) was the formation of a Cooperative Threat Reduction (CTR) program, or the Nunn-Lugar program. The CTR enabled the dismantling of chemical, biological, radiological, and nuclear (CBRN) weapons and improved border surveillance in the newly independent states of the Former Soviet Union (FSU) to monitor possible transnational shipments. Although this program has proved effective for monitoring nuclear weapons and materials, it has had more difficulty monitoring biological weapons. Russia denied having large quantities of biological weapons until 1992. Since then it has received funding to dismantle BW production facilities.[83] The approach of the United States and USSR to the problem of biological weapons was thus strongly influenced by the nature of their perceptions, which were to a large extent a product of the bipolar world system (described on pages 9–11). Later problems in addressing the issue of biological weapons were a product of perceptual vestiges of that system in the form of organizational process decisions (described on pages 28–29) after that system ceased to exist. That is, during the Cold War period, both the USSR and the United States were reluctant to limit their capacities in biological weaponry for fear that their opponent would gain an advantage through the possession of these weapons. Thus, neither the USSR nor the United States was willing to allow outside monitoring of their programs for fear that inspections could compromise the security of their operations. Consequently, monitoring of biological weapons remained a unilateral effort by both superpowers. After the conclusion of the Cold War and the evolution of the system from a bipolar configuration, many of the old attitudes and standard operating procedures remained in place within the decision-making structures—particularly of Russia, but to some degree within the United States. As a result, both Russia and the United States have been reluctant to put into place more intrusive international monitoring efforts. Moreover, because biological weapons programs were tightly guarded activities, responsibility for the programs was segmented to provide for greater security. Consequently, a variety of state agencies have been involved in the biological weapons programs. This situation has added to the complexity of efforts to monitor the program as a whole. In addition, because of the relatively secretive nature of the programs, there was less probability that security lapses at one location would be identified and eliminated by a central inspection authority. This has become painfully clear, through information received during 2001 and 2002, that Russian biological materials were stored in common refrigerators with little in the way of an accounting system for the contents of the refrigerator. Within the United States, more attention was paid to the security of computer equipment in biological weapons labs than to the monitoring of biological agents contained at these facilities. As a consequence, it has become very difficult for the United States or Russia to determine whether potential terrorists may have removed biological weapons material from these facilities in the past.

Terrorism in the 1960s was dominated by a variety of radical groups espousing anti-U.S. sentiments. Domestically, these included but were not limited to the Black Panthers, the Weather Underground, and the Symbionese Liberation Army. In the 1970s there emerged more foreign nationalist groups such as the Red Army Faction, the PLO, and the Shining Path in Peru, to name a few. Policies against terrorism occurred within the limitations of a bipolar Cold War rhetoric. Efforts to curtail specific kinds of terrorism, especially those involving airline security, took the form of a series of conventions beginning with, in the 1960s, the Tokyo Conference of the International Civil Aviation Organization. The Convention on Offenses and Certain Other Acts Committed on Board Aircraft was adopted in 1963. This was followed in 1970 by the Convention for the Suppression of Unlawful Seizure of Aircraft (Hijacking). In 1971 the Montreal Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, which focused on airline sabotage, was passed.[84]

The United States had multiple bilateral and multilateral agreements with other countries, but the agreements continued to focus on particular terrorist acts such as the kidnapping of the U.S. ambassador to Brazil in 1970 and the capture of the Saudi embassy in Khartoum, where the U.S. ambassador was held hostage. Disagreements over the definition of terrorism became a contentious issue when the United States approached the Organization of American States (OAS) concerning diplomatic security in Latin America, resulting in six countries withdrawing from the discussion. Ultimately, the Convention to Prevent and Punish the Acts of Terrorism Taking the Form of Crimes Against Persons of International Significance was modified by the UN, adopted in 1973, and incorporated into U.S. law in 1976.[85] By 1997 the UN General Assembly had adopted the Convention for the Suppression of Terrorist Bombings. This convention provided the "standard for international cooperation for incidents involving the unlawful and intentional use of explosives in public places with the intent to kill, cause serious bodily injury, or destroy a public place."[86]

U.S. efforts to contain the potential problem of CBRN weapons during the 1960s–1980s were highly reflective of a traditional realist perspective (described on pages 22–24). As would be expected by a realist orientation, these efforts concentrated upon other nation-states as the only significant threats in the system. Therefore, although the United States had concern about the proliferation of the CBRN weapons, until the 1990s this concern had not focused explicitly on their use in terroristic activities. Rather, conventions aimed at reducing proliferation of these weapons to other states were the dominant focus of U.S. efforts. These efforts began with the Conference on the Committee on Disarmament (CCD), which drafted the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons in 1971. These conventions were followed up by periodic reviews by conference participants throughout the 1980s and 1990s.[87]

Presidential Decision Directive 39 (PDD-39), issued by President Bill Clinton in June 1995, and PDD-62, issued in May 1998, defined U.S. policy against terrorism and specifically included NBC weapons. PDD-39 reflects this shift in emphasis in counterterrorism:

> *the development of effective capabilities for preventing and managing the consequences of terrorist use of nuclear, biological or chemical (NBCs) materials or weapons is the highest priority. Terrorist acquisition of weapons of mass destruction (WMD) is not acceptable and there is no higher priority than preventing the acquisition of such materials/weapons or removing this capability from terrorist groups.*[88]

Concerns heightened over the possibility of a nuclear attack as intelligence agencies reported a hemorrhage of nuclear materials from insecure nuclear facilities following the breakup of the USSR.[89] As the United States prepared retaliatory policies for the attacks on the WTC and the Pentagon, it placed all of its nuclear reactors on high alert while cautioning the American public this was standard operating procedure.

Phil Williams, a leading scholar on transnational organized crime (TOC) and terrorism, and Ernesto Savona suggest that a national approach is not the most effective; these authors view bilateral, regional, and global approaches as complementary, producing a synergistic effect.[90] Gurr and Cole take this a step further, emphasizing the importance of prevention and consequence management at the national level through good intelligence and police work. For example, monitoring communications traffic successfully interrupted a series of operations by cells of Osama bin Laden in 1999.[91] More to the point is that defining terrorism based on whether it is domestic or international requires different foreign policy responses. Moreover, these differing responses might well have to occur simultaneously. Examples would include the obvious attempts of the Bush Jr. administration to build an international coalition against terrorism in order to bring Osama bin Laden to justice. Equally important is correcting the lapses in security that enabled the terrorist attacks of September 11 to occur. Although there have been recommendations for the reinforcing of physical security, especially of the airlines, there was also mutual agreement that the head of security for the Federal Aviation Agency should step down for his department's failure to monitor and enforce airline security regulations. As noted earlier in the chapter, the synergistic approaches to airline security at the national and international levels have, in the past, proven effective.

Strengthening public health systems is another policy response that can occur on both the national and international levels when buttressed by multilateral agreements. This necessity became painfully clear in the 1995 Larry Wayne Harris case in the United States, when Harris, who had associations with extremist groups such as the Aryan Nations and the Christian Identity Church, purchased three vials of freeze-dried *Yersinia pestis,* a bacteria that causes bubonic plague. Although Harris's explanation suggests some mental impairment, the central revelation was that he had done nothing criminal by ordering this bacteria from the American Type Culture Collection (ATCC), which routinely supplied cultures to laboratories around the United States.[92] Harris was arrested, however, for wire fraud because he had lied to the ATCC about the laboratory he represented and in fact was unemployed at the time. Similarly, prior to the Aum Shinri Kyo attacks, there was no national Japanese law against anyone possessing sarin. Following the first Harris incident, the United States passed a law that became part of the Centers for Disease Control (CDC) regulations that prohibited transportation of bubonic plague to any but registered laboratories. This, however, covered only one pathogen, and Harris was arrested again in 1998 for transporting veterinary anthrax vaccine.

Implementation of international agreements at the national level requires a rethinking of mutual responsibilities and areas of expertise at the national level. And although the United States does have some specialized equipment for detection of CBW agents, it is held at only a few sites, making rapid response more difficult. Gurr and Cole recommend improving epidemiological surveillance to identify BW attacks and linking these into a central system that can then be disseminated to partners with whom the United States has treaties and agreements.[93] Gurr and Cole also suggest that bilateral measures can have a significant impact. Linking bilateral measures to national measures can occur not only through the use of specialized technology but also by financial assistance agreements such as the Nunn-Lugar program, through which the United States can financially and scientifically assist Russian nuclear facilities as Russia proceeds with the dismantling of nuclear weapons. This, in turn, lays the groundwork for greater accountability and transparency over the control and management of nuclear materials.[94]

Although some have criticized the U.S. propensity to limit its counterterrorism foreign policy to bilateral agreements, the record suggests these bilateral agreements have been effective due to the individualistic nature of most terrorism prior to 9/11/2001. Unlike more encompassing multilateral agreements, bilateral agreements can address issues such as law enforcement cooperation, extradition treaties, and mutual legal assistance treaties. After the bombing of the U.S. embassies in Kenya and Tanzania, the United States relied upon its bilateral links to extradite suspects from Pakistan. However, the ability of the United States and other states to share intelligence more effectively as well as better coordinate their responses to terrorists has been hampered by the traditional preference of the United States to lead and not follow in relationship to other states. The history of U.S. intelligence services "meddling" in the affairs of other nations as part of U.S. foreign policy, such as occurred in Iran when the United States covertly facilitated the Shah's return to power and in Chile when the United States aided General Augusto Pinochet's rise to power, has not developed the level of trust that multilateral agreements can develop. Ironically, the United States in 2001 again called upon its bilateral relationships to gain access to territory to launch forces against Afghanistan, because its leaders continued to refuse to release Osama bin Laden, thought to have masterminded the destruction of the WTC in New York and the partial destruction of the Pentagon in Washington, D.C.

All of this is not to say that multilateral agreements are to be avoided. To the contrary, they can effectively provide the structural web by which the United States can link and reinforce its bilateral agreements. Changes in the international system in the post–Cold War era have made multilateral arrangements somewhat more attractive to the United States as a policy instrument in its efforts to address the problem of international terrorism. In some ways, the UN has become a more realistic apparatus for attaining U.S. policy goals regarding the suppression of terrorism. For example, by persuading Libya to turn over the terrorists charged with the bombing of Pan Am 103, Kofi Annan, Secretary General of the UN, provided an important contribution to U.S. and U.K. efforts to resolve the Pan AM 103 incident. Moreover, regional integration provides, again, enhanced cooperation on criminal justice matters. The Clinton administration effectively used the G-7 forum in 1995 to obtain a "Declaration on Countering Terrorism."[95] (G-7 means the seven wealthiest Western industrial countries.) Other global conventions include the Program for Preventing and Combating Illicit Trafficking in Nuclear Material in 1995 at the G-8 Moscow Nuclear Safety and Security Summit, the Tokyo Convention, the Hague Convention, the Montreal Convention, the New York Convention, and the Hostages Convention.[96] Overall, whereas the conventions encourage and, in some instances, provide specific and strong guidelines for settling disputes, they lack provisions for sanctions.[97]

Counterbalanced against the enhanced U.S. policy options provided by changes in the international system were certain governmental factors (described on pages 20– 21). Specifically, recalcitrance by the U.S. Congress to approve multilateral measures has sent ambiguous signals to allied governments and has caused some of these multilateral measures to be less effective than they might have been. For example, the U.S. Senate has delayed ratifying the Convention on the Marking of Plastic Explosives for the Purpose of Detection, but has included marking requirements in the Omnibus Counter Terrorism Act of 1995.[98]

The International Atomic Energy Agency (IAEA) has also provided assistance to states in monitoring and coordinating responses to trafficking in nuclear materials. A mutual exchange of information between the IAEA and member states was agreed upon in 1994 as IAEA began strengthening its relationship to regional nuclear agencies within the UN and the EU, including the European Atomic Energy Agency (Eurotom) as well as the International Criminal Police Organization (Interpol). However, the effectiveness of small-scale nuclear programs conducted by non-state actors and the vigor with which individual member states would pursue them depends on available resources, and the capacity of organizations such as Interpol to effectively address problems of smuggled nuclear technology and materials is constrained by the increased sophistication of potential terrorists.

CYBERTERRORISM AND INFORMATION WARFARE

The Nature of Cyberterrorism

Cyberterrorism is a product of changes in the technological capacities of states and non-state actors in the international system (described on page 14) that occurred over the last decade of the 20th century. These changes enabled governments and private individuals in a significantly larger proportion of the world's states to have access to virtually unlimited communications networks. As a result, it has become possible for both the government professional and the gifted amateur to use this communications network to gain unauthorized access to the data archives of governments and private businesses. Cyberterrorism involves the use of information technology by an attacker in an effort to disrupt the information technology resources of a target state for the purpose of damaging the economic, political, and military capabilities of that state or its citizens. In this sense, the terror results from the unpredicted loss of information or control of equipment, which in turn may result in a loss of life or economic capacity in the target state.

As noted in a report by the National Information Protection Center, Chinese hackers apparently responded to the U.S. accidental attack upon the Chinese embassy in Yugoslavia by compromising a variety of U.S. government websites.[99] In addition, there was strong evidence that the government of the Former Republic of Yugoslavia (FRY) directly or indirectly encouraged cyber-attacks against the North Atlantic Treaty Organization (NATO) in response to NATO air operations in the Kosovo humanitarian intervention (discussed in Chapter 6). Although these attacks did not directly interfere with NATO's ability to conduct its air campaign, they did disrupt various other aspects of NATO's operations. [100]

If there had been any doubts about the likelihood of a "cyber-attack" as a form of terrorism, they were definitively dispelled in April and May 2001 when a mini-cyberwar took place between Chinese and American hackers, apparently provoked by the midair collision of a U.S. surveillance plane and a Chinese fighter jet. Contrary to the mythic stereotype of teenaged hackers bent over a laptop in their bedrooms for 20 hours a day, these hackers had a well-developed network of allies.[101] A leading Chinese Internet security firm claimed that by 1 May 2001, U.S. hackers had penetrated approximately 300 websites in China, and that Chinese hackers had entered into nearly 100 U.S. sites.[102] American sites included the White House, Labor Department, Office of Personnel Management, Pacific Bell Services, and United Press International. The American hackers and their allies, which included Brazil, Argentina, Saudi Arabia, Pakistan, India, and Malaysia, successfully penetrated approximately 300 Chinese websites. Although no major damage was done, the revelation that even a loosely organized group such as this could have this level of success was startling. Responding to the attack by al-Qaeda on the United States on 11 September 2001, pro-U.S. hackers apparently penetrated and disrupted websites in Afghanistan and Pakistan.[103]

Information warfare is not new, but the older image of organized crime groups is no longer applicable in the information revolution age. Harvey Kushner, an associate of the Rand Corporation and a terrorism expert, noted in 1999 that state-sponsored terrorism as we understood it had changed, and that the terrorist of today—particularly the cyberterrorist—is more likely to be part of a group working within a loosely organized network. Kushner described the structures of cyberterrorist networked organizations with the acronym, “SPIN: segmented, polycentric, ideologically integrated networks.”[104] *Countering the New Terrorism,* a 1999 RAND report, also notes that Osama bin Laden’s organization, al-Qaeda, appeared to have acquired an array of information technology for communication among members of his network, including Web access, e-mail, and electronic bulletin board capacity, where members can exchange information with a minimal risk of detection by Western intelligence communities.[105] Thus, we see that information technology has provided a method for both loosely organized hackers and organized terrorist groups to better coordinate their activities while avoiding detection. But when does a hacker stop being a mischief maker and become a terrorist, and how does any nation geared up for conventional and traditional war engage the enemy in the case of the cyberterrorist?

In 1994 the School of Information Warfare and Strategy was created within the U.S. Department of Defense (DoD) to develop U.S. strategies for the conduct of information warfare. By 1997, it had redefined information warfare.[106] Congressman Joseph R. Pitts (R–PA, member of the House Armed Services committee, and founder of the Congressional Electronic Warfare [EW] Working Group) noted that “the real military struggle in the twenty-first century will be between awareness and deception,” and the objective of this form of military will be to gain knowledge dominance of a new form. That is, gaining awareness of your enemy without your enemy being aware of you will involve securing a range of new information sources including electronically stored, transmitted, and encrypted information.[107] Pitts observed that although the U.S. military distinguishes between electronic and information warfare, the practical perspective has been controlling electromagnetic spectrums—whether it be in radar, infrared guided missiles, and defensive sensors—so the United States can know the enemy better than the enemy knows it.

As noted by Carlo Kopp, it is now technologically possible to deny an enemy state this same capacity through sophisticated nonnuclear explosive devices that produce an electromagnetic pulse (emp) strong enough to permanently disable an enemy’s electronic surveillance capabilities. Although these new forms of nonnuclear emp-generating devices are complex, they are not so complex that either rogue states or committed terrorist groups might not be able to engineer them.

Either through independently engineering these devices or stealing them, terrorists may use emp in the future to disrupt U.S. civilian electronic communications, storage, and control devices. [108]

The porosity of borders and types of relationships that accompany globalization have raised new challenges for governments in the Internet age. Even developing nations have acquired a level of capability in information technologies that allow their own home-grown hacker terrorists to operate internationally. The hacker terrorist is able to disrupt and/or corrupt any of the world's major information systems, funds transfers, transportation control, air traffic safety, phones, electric power, oil and gas distribution, and, of course, military systems.[109] Libicki disagrees, however, that this is a credible threat and asserts that until proven to the contrary by someone actually taking down an electricity grid or telecommunications systems, using cyberterrorism to paralyze a nation is in fact harder than it seems. But Libicki is thinking in terms of the more conventional military goal of the takeover of a nation. There is evidence that hackers could relatively easily disrupt aspects of the U.S. power grid. Speaking before the U.S. Information Agency, James Adams, CEO of Infrastructure Defense, revealed that in 1997 the U.S. military conducted an exercise—Operation Eligible Receiver—with 35 government employees as hackers using laptops purchased locally from computer stores.[110] Within a very short time, the governmental hackers were able to break into the power grids of four major cities linked to the U.S. military's ability to deploy forces: Los Angeles, Chicago, Washington, D.C., and New York City.[111] These same governmental hackers were also able to penetrate the command and control system of the Pentagon. In another simulation conducted by the U.S. Naval Postgraduate School and the RAND Group, John Arquilla and Robert Neubecker imagined a scenario where an unknown fundamentalist group engages in "cybotage," producing rolling power outages throughout the United States and causing the congealing of flowing oil by manipulating the automated pipeline control, making the pipes burst and creating an environmental disaster. The conclusions derived from these simulations will continue to remain salient today whether the object of the attack is military targets or civilian systems.

Information warfare is as much, if not more, of an issue for the U.S. business community as a military issue. Attacks via personal computers (PCs) into network servers can disrupt foreign exchange markets, cause wastewater plants and automated banking services to fail, and, as was seen in the 1993 bombing of the World Trade Center (WTC), render cell phones totally ineffective.[112]

U.S. Government Responses to International Cyberterrorism

Adams identifies a series of challenges facing any government in the midst of rapid change:[113] What does government mean in this new age of information warfare when communities can be formed and reformed as the need arises? How do we defend our critical infrastructure when most of our government remains mired in a Cold War mentality? The U.S. government's response to these issues is complicated by domestic interest group pressures. Interest groups for whom the issue of intellectual property is a large consideration are concerned about the potential implications of intelligence sharing for the continued protection of those rights.

Considerations of bureaucratic politics (described on pages 28–29) appear to have been an important factor in the relatively late response of the United States to the threat of cyberterrorism. That is, entrenched interests within the DoD pressed for allocations to meet their needs while ignoring or downplaying the need for resources in areas beyond their immediate sphere of responsibility. More specifically, as of 2000, Defense Department priorities continued to be requests to Congress for conventional weapons systems such as the F-22 joint strike fighter, as opposed to expanded allocations for information technology (IT) programs. A second aspect of the problem was the difficulty in convincing civilian and military policymakers that cyberterrorism was a pressing and realistic threat requiring a more active response. At this point in U.S. history, no overwhelming cyber-attack that devastated financial markets and other critical systems had taken place.[114]

Although elements of the U.S. government were aware of the potential threat of a cyberterrorist attack on the United States, there was no coordinated effort to develop a consistent policy until 1995. In the aftermath of the Oklahoma City bombing in 1995, President Clinton issued PDD-39, which directed Attorney General Janet Reno to develop a policy to counter terrorist attacks on the United States. Reno convened a cabinet-level committee for the purpose of assessing U.S. vulnerability to attack and developing policies to meet such an attack. Initially, there was no mention of cyberterrorism as a subject for this committee.

Cyberterrorism was raised as a potential concern of the Reno cabinet committee as a result of the deliberation of a sub-cabinet-level task force composed of representatives from the CIA, DoD, National Security Agency (NSA), and FBI, which was chaired by Michael Vatis.[115] This task force had been charged with defining the scope and meaning of terrorism against critical infrastructure. The task force concluded that critical infrastructure protection would necessarily include "[s]ervices vital to the national economy and national security."[116]

Parallel to the work of this interagency task force, President Clinton had convened the Commission on Critical Infrastructure Protection. Presidential Decision Directive 63 (PDD-63) was based on the recommendations from a 1997 report of President Clinton's Commission on Critical Infrastructure Protection. This report called for "a national effort to assure the security of the United States' increasingly vulnerable and interconnected infrastructures, such as telecommunications, banking and finance, energy, transportation, and essential government services." Attorney General Reno proposed that energy services be included as an additional category of critical infrastructure.[117] The purpose of PDD-63 was to ensure the security of infrastructure through the immediate establishment of a national center for warning of attacks and responding to them and the development of the capability to protect critical infrastructures from intentional acts by 2003. Each governmental department and agency was ordered to assess its own cyber and physical infrastructure to reduce its exposure to new threats. The federal government was directed to serve as a model of how to protect the infrastructure for the rest of the country. Congress was to fully participate and contribute ideas. In addition, the directive created the position of National Coordinator to oversee critical infrastructure, foreign terrorism, and "threats of domestic mass destruction (including biological weapons) because attacks on the U.S. may not come labeled in neat jurisdictional boxes."[118] As part of PDD-63, the National Infrastructure Protection Center (NIPC) was developed by the Federal Bureau of Investigation (FBI) in response to the recommendations calling for coordination of information among representatives from the FBI, Department of Defense, U.S. Secret Service, the departments of Energy and Transportation, and the intelligence community, as well as the private sector. In other words, NIPC was charged with developing a public-private partnership to protect critical systems. (Interestingly, although there is no mention of including international cooperation in the recommendations despite the presence of those agencies often critically involved in an international response, it is through an alliance with private industry in the United States that NIPC was created.) Thus, we see the recognition by the Clinton administration that U.S. government agencies and departments, the Congress, the president, and the private sector were not working together to make the United States secure from terrorist attack. Whether this lack of explicit coordination is a vital concern or merely somewhat problematic is open to question. We also do not see in PDD-63 an explicit discussion of a program for coordinating with other governments actions to identify, monitor—and most importantly—disrupt efforts by cyberterrorists based abroad to disrupt U.S. information networks.

The relative lack of interest by U.S. government agencies may be traced to various factors. Government agencies appeared to feel that their infrastructure was relatively secure. In addition, despite concerted efforts of the NIPC to convince members of Congress that the issue was real and potentially significant, the issue of cyberterrorism had not resonated as a hot-button issue for most key or powerful members of Congress.[119] Although Senator Judd Gregg, the chairman of the Appropriations Committee Subcommittee on Commerce, Justice, and State, was a believer in the potential seriousness of the problem and did manage to retain funding for NIPC, he represented a minority in either house.[120] An important factor in congressional indifference to the issue during the 1990s may have been the source of the warnings about the issue of cyberterrorism. That is, warnings from the Clinton administration regarding threats to information infrastructure were dismissed out of hand by many members of Congress in a political climate of hostility on the part of a Republican-controlled Congress against a Democratic administration that many members thought was overly concerned with the Internet. Consequently, the Congress put little pressure on the bureaucracy to act aggressively to address the issue. The Clinton administration also sought to ease the fears of U.S. interest groups associated with information technology resources that U.S. government policy would hinder the expansion of private enterprise. At the time that cyberterrorism was emerging as an issue, interest groups representing high-technology industries were concerned about avoiding new governmental regulation of their activities. Their distrust of governmental regulation, in turn, stemmed from dissatisfaction with the restrictive nature of previous government regulation of the export of encryption technologies, due to national security considerations. As a result, influential high-tech interests lobbied both the Congress and administration to refrain from overly prescriptive regulation of Internet infrastructure.

Unlike other aspects of U.S. policy toward international terrorism, U.S. cyberterrorism policy has not been heavily influenced by 11 September 2001, although obviously the incident did to some degree increase interest in the potential for cyberterrorism. Among those who have become more interested in the issue of cyberterrorism in the wake of 9/11 have been Senators Lieberman and Edwards, two potential Democratic candidates for the presidency in 2004. To the extent to which U.S. policy regarding cyberterrorism has evolved, this has been a product of the effects of viruses and worms such as Nimda and Code Red, which have caused significant problems for private industry. The effects of these viruses and worms sensitized industry to the potential need for more coordinated efforts to forestall the reoccurrence of such penetrations of their infrastructure. Governmental interest in the issue of countering cyberterrorism was dramatically increased by two other events. Solar Sunrise, an action by hackers in which a large number of military systems were penetrated and root access was compromised, caused grave concern within the defense department. At the time, the military was firmly convinced that Solar Sunrise was instigated by Saddam Hussein. A second penetration of U.S. government information infrastructure, Moonlight Maze, triggered graver concern among the military and civilian bureaucracy in that this action resulted in the actual theft of classified material. Government concern was heightened when it was determined that the penetration originated in Russia.

Despite the heightened levels of concern within the bureaucracy, U.S. counter-cyberterrorism policy has remained remarkably consistent. It continues to be shaped by the basic conflict between the need to regulate vital, yet essentially private, components of the nation's information infrastructure with the reluctance of private industry to subject itself to governmental scrutiny. Although the Bush Jr. administration publicly argued that it was adopting a completely different plan for addressing the potential problem of cyberterrorism, in practice the Bush Jr. administration approach has been essentially similar to that adopted by the Clinton administration.[121] Policy continues to rely on voluntary cooperation by industry. There has been little more public pressure, or pressure from Congress, for the government to do more to force the regulation of critical infrastructure. Where the Congress has acted to mandate protection of information resources, it has been done in the name of protecting the privacy of information rather than protecting the infrastructure network.[122] In the opinion of Michael Vatis, the failure of the U.S. government to agree upon a more active counter-cyberterrorism policy will become a major subject of controversy only when, not if, a catastrophic penetration of the nation's critical infrastructure takes place.[123] Only when an industry providing critical services (whose interruption will significantly damage both the economy and national security of the United States) is crippled by a cyberterrorist penetration will government and interest groups be galvanized to develop a more stringent regulatory policy.

In 2001, in response to a General Accounting Office (GAO) report, "Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities," Chris Klaus, CEO and Founder of Internet Security Systems in testimony before the Senate Judiciary Committee,[124] disagreed with the GAO's finding that NIPC's analysis and warning capabilities were limited. Although Klaus did have concerns about whether law enforcement and industry could react rapidly enough in response to a threat, he agreed that lack of interagency cooperation at NIPC also impedes the effective and rapid sharing of information.

Klaus concurred with the GAO finding that private industry was quite reluctant to engage in information sharing when corporate information security practices would be placed at risk, whether it jeopardized market positions, strategies, customers, or capital investments.[125] Klaus pointed out that private companies not only run their own communication facilities but often subcontract to run those of the government, and he lent support to Information Sharing and Analysis Centers, a voluntary program to bring industry and the public sector closer together. Klaus called for information-sharing legal protections that clarify and strengthen the existing Freedom of Information Act, such as the bills being drafted by the Senate and the Congress. (One of the principal ways NIPC is cooperating with private industry is through a program called InfraGard, a cooperative undertaking between the U.S. government, associations of businesses, academic institutions, and law enforcement agencies to strengthen critical infrastructure.)

Major Robert D. Critchlow, on the other hand, sees military opportunity for the United States to use information warfare (IW) offensively, particularly with the changing terms of engagement emerging in the post–Cold War period. Critchlow argues that IW is uniquely constructed to respond to terrorist attacks in ways that avoid the larger number of deaths associated with less well controlled NBC or conventional military approaches.[126] Moreover, cyberwar produces a "decapitation" effect without having to kill the leaders. Critchlow argues that IW is particularly suited as a central part of our deterrence posture in that escalation dominance can be maintained in ways the enemy could not match. Techniques that would be used include those usually associated with computer network attack: viruses, worms, and knowledge robot (knowbot) bombs, in the form of "Trojan Horses" (programs that mimic legitimate programs, but target specific computer components to gain access to enemy databases).[127]

Developing such capabilities to keep ahead of the most technologically sophisticated cyberterrorist requires the Department of Defense to drastically adjust and restructure its policies to accommodate IW, to say nothing of the costs involved in developing the expertise required. Additionally, the government would have to reassess its policies on export control and technology transfer, again putting itself into possible opposition with the same private sector with which it is trying to build a coalition. Beyond that, according to Critchlow, overcoming the military's traditional posture of "machismo," emphasizing brains over brawn, might be the largest hurdle.

The United States has a vital interest in protecting its security, defending its critical infrastructure, maintaining its economy, and promoting its democratic values. Confronted with faceless enemies, the United States will no longer be able to rely exclusively upon traditional military instruments to achieve its foreign policy objectives. Although the United States has considerable capabilities to act unilaterally to address some of the threats posed by cyberterrorists, the nature of the international technological environment (described on page 14) in which cyberterrorism may occur dictates that the United States must also rely upon multilateral approaches to adequately address the threat posed by cyberterrorism. For example, the initial response of the Bush Jr. administration to the terroristic activity of Osama bin Laden on 9/11/2001 involved the use of information technologies to trace and disrupt bin Laden's communications and his financial transactions. IW does provide an opportunity for threatening punishment while limiting the enemy's ability to strike U.S. forces. Such strategies, however, require that U.S. foreign policy, especially its counterterrorism policy, increasingly adopt multilateral efforts; sustain friends; and confront adversaries. Again, the response of the United States to the terrorist incidents of 9/11/2001 reflected a recognition that only a sustained and coordinated effort involving the largest possible international coalition of cooperating states will be effective in addressing the problem of international terrorism. Governments, therefore, have an interest in developing a coordinated approach to the monitoring of the use of the Internet and wire transfers as a means of controlling terrorism.

The most effective means of limiting the terrorists' capacity appears to be to disrupt their communications and their funding, especially the transfer of funds from cell to cell and from the central organization to the cells, for example, from al-Qaeda to field operatives. Both of these operations require international cooperation in monitoring and interception. However, the refinement of this cooperation does raise the issue of "Big Brother" watching all. As a consequence, the United States and other concerned states must work toward developing some form of workable regulations that protect privacy, while continuing to monitor and interdict internationally harmful uses of the Internet.

Since January 2000, the United States has considered it a priority to deny terrorists the capacity to fund their operations. Toward this end, the United States signed the International Convention for the Suppression of the Financing of Terrorism. This convention put into place "an international legal framework for investigating, apprehending, and prosecuting those involved in terrorist financing."[128]Although 35 countries including the G-8 initially signed this convention, the United States has devoted considerable effort to pressing signatory states (132 as of April 2002) to ratify and implement this convention as quickly as possible and to convince other members of the international community to accede to the convention. In addition, as mentioned in this chapter's introduction, in September 2001 Bush Jr. signed Executive Order 13224—Blocking and Prohibiting Transactions by Persons who Commit, Threaten to Commit, or Support Terrorism.[129]

COSTS VERSUS BENEFITS AND RISKS VERSUS REWARDS—THE EVOLUTION OF U.S. POLICY TOWARD TERRORISTS

In making any policy decision, especially a foreign policy decision, the U.S. government strives to apply a rational decision-making model, as described in the introduction to this book. The United States considers the costs versus the benefits and the risks versus the rewards of actions before taking them. These benefits may be to the United States or its allies.

Prior to the conclusion of World War II, although terrorists certainly operated worldwide, the United States was not a prime target of that terror. Unlike the colonial powers of Great Britain, France, the Netherlands, Belgium, and Portugal, the United States was by and large not seen to be the principal protector of a status quo deemed to be oppressive by dissatisfied governments or subnational groups. During this period the United States was also not perceived to be the principal proponent of the expansion of an international system that was damaging the capacity of either states or subgroups to preserve a way of life they valued.

Even after the conclusion of World War II, the then colonial powers of Western Europe were seen to be more central to blocking the aspirations of populations in the areas of the world we now call less developed countries (LDCs) or Third World. As a consequence, France was subject to terroristic attacks by dissidents both in its colonial possessions in East Asia and Africa and later domestically, as the liberation movements and those opposed to emerging French policy concerning the grant of independence to selected colonies took their struggle to France itself. In particular, this was the case with respect to French policy in Algeria in the 1950s and 1960s concerning the grant of independence to that colony. Great Britain, too, was the subject of terrorist attacks aimed at altering its position regarding the grant of independence to its colonies such as Palestine, India, and several locations in Africa. Among the most serious of these attacks was the bombing of the King David Hotel in Palestine by elements of the Jewish population, who wished to speed British end to control over the area so that a state of Israel could be declared.

Although in the aftermath of World War II the United States became the undisputed leader of the market-oriented, democratically inclined states in the developing Cold War between the Soviet bloc states and the West, the United States was not immediately the target of terrorism, except for the occasional targeting of its citizens resident in Latin America. There the United States had long been perceived as a bully by many elements of the population. In some ways, the Cold War constrained direct, large-scale attacks upon the United States by terrorists receiving direct aid from the USSR. Given U.S. rhetoric of the time (massive retaliation), the United States clearly would have responded directly against the USSR if the United States had been able to identify the USSR as having provided aid to the terrorists.

By the 1970s, the United States had become a significantly more active presence in the protection of the world status quo. U.S. economic interests had become more global, and its visible economic presence in terms of large numbers of U.S. multinational enterprises had also increased. Consequently, the United States was more likely to directly or indirectly support actions aimed at suppressing the actions of subgroups located abroad who were dissatisfied with the consequences of the emerging international political and economic system. Because the targets of terrorist actions by dissatisfied groups overseas were at that time private American citizens (for example, corporate executives kidnapped for ransom), the United States clearly had an interest in addressing the problem. However, because the number of incidents was relatively low and the cost in loss of human life was also relatively low, the U.S. response too was relatively low-key. Among these responses was the formulation of the doctrine of not negotiating with terrorists.

In many ways, the U.S. response to the 1973 Yom Kippur War in the Middle East dramatically altered, particularly in the Middle East region, international perceptions of the position of the United States in the world. By that time both France and Britain had withdrawn from their colonial empires and more direct involvement in the affairs of the region. As a consequence, when the United States felt compelled by significant considerations of security and moral principle to intervene and support Israel by resupplying military equipment and restraining Soviet aid to the Arab participants in that conflict, the United States became associated to some degree with blocking the aspirations of key Arab elements in the region. Moreover, as the United States took a significantly more active role in brokering the settlement of that conflict, it became dramatically more involved in the affairs of the region. Further, the emphasis on preserving the stability of the region by promoting economic development along Western capitalist lines introduced a significantly expanded U.S. corporate presence in the Middle East region.

As U.S. corporate interests—in particular U.S. airlines—became the target for hijackings, the United States took an active role in formulating international conventions aimed at suppressing hijacking by denying the perpetrators safe haven once they had committed their act. However, the willingness of the United States to mount a large-scale operation to suppress terrorism was somewhat constrained by the low number of U.S. casualties resulting from the practice of hijacking and limited the extent to which this form of terrorism had long-term serious economic impacts on the United States.

When the United States did take a more active role in addressing the problem of the collapse of the Lebanese governmental system under the pressures of Palestinian nationalist aspirations, it again placed itself in a more visible role in the Middle East. It further placed itself in the position of being perceived, rightly or wrongly, as being more supportive of Israeli interests and less supportive of the interests of Arabs in the region, who were dissatisfied with the lack of progress in addressing the concerns of the Palestinians. Because of a somewhat poorly executed intervention, U.S. troops became the direct target of a terrorist bombing attack.

The United States responded to the attack in two ways. First, it withdrew its troops. Second, it undertook direct aerial attacks on the training camps of the suspected perpetrators. However, since the long-term impact of the attack was relatively low and the attack was conducted abroad, the United States generally contented itself with taking measures to prevent its troops from being similarly exposed in the event of future overseas operations.

The terrorist attack on Pan Am 103 brought a significantly more coordinated and prolonged response from the United States. This response included attempts to identify and punish the direct perpetrators. In support of this policy, the United States was able to elicit the cooperation of allied governments. This cooperation derived from the fact that the plane was bombed over Scottish territory, killing Scottish citizens. It also was a product of increased evidence that the event was partially due to lax security at the airports of allied states. As a consequence, U.S.

policy to some degree concentrated on putting into place international measures to ensure that security at airports would be improved.

U.S. reactions also involved the attempt to organize direct measures to punish the state of Libya economically since it was thought to have supported the terrorist action. Debates over the legal authority upon which sanctions against Libya would rest slowed down the foreign policy process. When the sanctions option is on the table, economic departments within the U.S. government attain a high degree of significance. Treasury officials become critical to the process because of their knowledge of the procedures for imposing sanctions. The Department of Commerce is similarly important in assessing the economic outcomes of imposing sanctions. Adding to this is the response of domestic and international interest groups among the business communities. Ultimately, the United States imposed unilateral economic sanctions banning importation of Libyan oil, freezing Libyan assets in the United States, and forbidding U.S. oil companies from doing business in Libya. Libya's response was to make even more attractive investments for European-based oil firms, many of which were U.S. allies.[130]

The extent to which the loss of American civilian lives and the damage to U.S. commercial interests (Pan American Airways flight 103) resulted in a concerted long-term effort to punish the perpetrators is evidenced by the willingness of the government to explore a variety of policy options over a multiyear period. In 1993, the United States and the U.K. finally convinced the UN Security Council to impose multilateral sanctions on Libya in an effort to get that country to turn over suspects in the Pan Am 103 bombing. This, however, occurred only when the terrorists responsible for the bombing were indicted in Scottish court as part of a police investigation and discovered to be Libyan intelligence agents. Formal requests by international diplomats for the terrorists' extradition, which had already dragged on for 7 years, were fueled considerably by the political mobilization of the victims' families. And each year another UN sanction was imposed in an effort to move the Libyan government closer to cooperation.[131] Attempts to bring these terrorists to trial were complicated because the United States and the U.K. distrusted having the trial occur in an international court. Finally, a coordinated response involving UN Secretary General Kofi Annan, members of the Arab League, Nelson Mandela, and diplomats from London and Washington resulted in a formal proposal, accepted by Libya in 1998, to turn the accused terrorists over for trial.

As noted elsewhere in this book, the Iraqi invasion of Kuwait at the end of the Cold War profoundly affected a number of U.S. foreign policy priorities, including ballistic missile defense (BMD) and conventional force structure. However, the U.S. response to the Iraqi invasion of Kuwait by organizing operations Desert Shield and Desert Storm significantly altered U.S. presence in the Middle East. Whereas the United States had been an occasional presence in the past, it was now a more or less permanent presence in considerable force, and most importantly, stationed on land in Arab states. Consequently, the United States became considerably more visible in the region. In addition, its presence provided considerably more targets of opportunity for elements dissatisfied with the U.S. role in the region. Two of these targets of opportunity were the barracks compound in Saudi Arabia that was targeted for a terrorist suicide bombing in the 1990s and the subsequent attack on the USS *Cole,* which took place in 2000 as it undertook its patrol mission in the Middle East. Both targets, however, represented "military" targets. In addition, both attacks could be reasonably addressed in part by enhanced or altered security arrangements by U.S. forces abroad. Apart from this response, the United States also engaged in an ad hoc retaliatory campaign of missile attacks on the suspected training sites used by the perpetrators. As a consequence, U.S. response was essentially a military response by the military branches of the U.S. government.

The attacks on the U.S. embassies in Tanzania and Kenya in 1998 represented a somewhat different policy situation for the United States. In this case civilian and not specifically military personnel were the primary victims of the attack. Moreover, most of the attack victims were citizens of Tanzania and Kenya—not Americans. As a result, the United States received somewhat greater cooperation from indigenous governments in tracking the perpetrators than appears to be the case when the primary victims were U.S. military. In addition, these attacks raised an important issue for a variety of foreign governments—the sanctity of diplomatic missions or embassies. That is, for at least the past 33 years, governments have generally considered an attack on any country's embassy to be a potentially serious precedent for fear that their embassies could become the next targets.

U.S. response to the attacks on the embassies involved both rhetorical condemnation and more sustained, though still largely unilateral ad hoc actions. President Clinton ordered missile attacks on the operational bases of the suspected perpetrators within Afghanistan and Sudan. In addition, he issued an executive order aimed at freezing and seizing assets of Osama bin Laden in the United States. Further, the Clinton administration was able to convince the Saudi Arabian government to freeze bin Laden's assets in Saudi Arabia. However, U.S. efforts to orchestrate a wider seizure of bin Laden assets did not succeed. There was a concerted effort to bring the perpetrators of the attacks to justice. Finally, Clinton administration efforts to address the attacks apparently involved the lifting of a more than 20-year-old presidential directive (originally issued by President Ford) banning the targeting of specific individuals for assassination if they were deemed to pose a direct security threat to the United States.

Although all of the instances previous to 1993 of international terrorist attacks on the United States and its citizens involved attacks planned and executed abroad, in 1993 the United States was subject to a successful penetration of its domestic security measures when international terrorists bombed a basement garage in the World Trade Center in New York. Clearly, this represented a different terrorist problem for the United States because these international perpetrators had carried their attack onto U.S. soil. Consequently, the number of U.S. agencies (FBI as well as CIA) concerned with the incident expanded. Moreover, unlike most of the other terrorist attacks on U.S. interests discussed so far, this attack specifically targeted the U.S. civilian population.

The government's response was relatively vigorous in tracing the initiators of the attack and bringing them to trial. In addition, the government did increase domestic security measures to some degree. However, the U.S. government's capacity to mount an all-out effort to control terrorism was constrained by several factors, not the least of which was the relatively contained physical and fiscal cost of the attack. In the absence of large-scale loss of life or a dramatic economic impact upon the United States, costly and potentially politically sensitive large-scale responses to the attack were not seen to be cost-effective. Rather, continued vigilance by domestic and foreign intelligence agencies, coupled with enhanced security measures domestically, appeared to be adequate and prudent responses. That is, the U.S. government's ability to win either domestic or large-scale international support for a prolonged direct attack on the terrorist networks that the United States knew to exist was unlikely given the lack of a perceived, overriding threat.

The attacks of 11 September 2001 on the World Trade Center (WTC) in New York City and the Pentagon in Washington, D.C., plus the crash of a fourth airliner before it could carry out a similar attack on another U.S. site, dramatically altered the cost-benefit calculus of U.S. policymakers with respect to the issue of terrorism. This coordinated set of attacks dramatically affected not only U.S. security interests but also U.S. economic interests. In addition, the events of 11 September 2001 galvanized U.S. popular support for concerted action in a way that none of the previous attacks on U.S. interests by international terrorists had done. Further, because the WTC was occupied by significant numbers of foreign nationals, these countries could not as easily dismiss the attack as being solely directed against the United States. As a result, the United States was in a much stronger position in any effort to organize a concerted multilateral response to this terrorist attack than in any previous international terrorist attacks on its interests. Finally, due to the nature of the attack, the internal bureaucratic isolation of departmental response to previous terrorist attacks on U.S. overseas interests could more easily be pushed aside in favor of a more coordinated U.S. approach.

With the incentive provided by the direct terrorist attack on the United States, the U.S. government could more easily explore a more creative, coordinated response to the act. This support included not only the standard rhetorical condemnation—increasing of security and selected ad hoc missile attacks—but also more politically creative and fiscally expensive responses. That is, in the wake of 11 September 2001, the U.S. government could count on greater international cooperation in interdicting the finances and communication of terrorist cells. Toward this end, President Bush Jr. ordered the creation of the Foreign Terrorist Asset Tracking Center in an effort to both monitor and coordinate the interdiction of financial transfers among terrorist groups. The U.S. government could also count on the support of the U.S. population and foreign governments for a more prolonged and politically sensitive general assault on the government of Afghanistan for its apparent support for such terrorist activity.

HOMELAND SECURITY—U.S. RESPONSE TO TERRORISM

Among the most significant responses of the Bush Jr. administration to the terrorist attacks of 9/11 have been its incremental steps to establish a Department of Homeland Security (DoHS). The decision of the Bush Jr. administration, publicly announced on 6 June 2002, to establish a DoHS represents a culmination of congressional and executive department studies dating back to the period before 9/11/2001. Among the many task forces and special panels that had investigated the issue of homeland security, two stand out. These are the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, otherwise referred to as the Gilmore Commission, and the U.S. Commission on National Security/21st Century, often referred to as the Hart-Rudman Commission. These two commissions proposed divergent organizational frameworks for addressing the problem of homeland security. Whereas the Gilmore Commission adopted a framework similar to that chosen by the United States to pursue the War on Drugs (discussed in Chapter 5), namely a coordinating office similar to the Office of Drug Control Policy, the Hart-Rudman Commission proposed a more thorough reshuffling of agency location and responsibilities. The proposal to create a DoHS by President Bush Jr. on 6 June 2002, drew heavily upon the recommendations of the Hart-Rudman Commission. It also added a set of functions associated with the problem of weapons of mass destruction that was not part of the Hart-Rudman recommendations.[132]

The establishment of this department will reorganize a variety of governmental functions and agencies into a single cabinet-level department in order to more effectively address the threat posed by domestic and international terrorism. The establishment of this new cabinet-level department is in itself a recognition of the increasingly intermestic nature of even the issue of state security. Moreover, the proposed mix of agencies included in DoHS, together with their missions, present a number of problems concerning the crosscutting domestic and international responsibilities of these agencies. As proposed, the DoHS would include four principal functions: protection, computer security, domestic disaster preparedness, and response to weapons of mass destruction. Within the first function, the DoHS would incorporate the Border Patrol, the Coast Guard, and the Customs Service. In addition, DoHS would be given oversight of certain Immigration and Naturalization Service functions. Under the computer security function, DoHS would address issues concerning the protection of the security of U.S. private and governmental computer infrastructure. The preparedness function would incorporate existing agencies, such as the Federal Emergency Management Agency (FEMA), which responds to a wide variety of national disasters (such as hurricanes) and a crisis response mechanism charged with coordinating a response to nonnatural disasters. Finally, the WMD function of DoHS would incorporate a variety of functions from a diverse set of agencies, including HHS, DOE, and the Department of Agriculture Animal and Plant Health Inspection Service (APHIS) program (discussed in Chapter 8).[133]

The proposed formation of the DoHS has already raised significant issues for a variety of private and governmental constituencies. Consequently, the formation of this agency and its eventual response functions will almost certainly be subject to considerable bureaucratic politics (discussed on pages 28–29). For example, the reshuffling of agency locations will affect the powers of congressional committee oversight. In addition, many departments will be losing agencies, and therefore power that had been theirs to wield for decades—in some instances (secret service and treasury department) over 100 years. In addition, a number of the agencies to be transferred to DoHS for the purposes of coordinating U.S. security have other responsibilities that are only indirectly related to security or reflect an overlap of security and prosperity goals (as presented in Figure 1.7 page 32). Coordinating and prioritizing these functions will present many problems during the early 21st century. Finally, in instances in which the DoHS has oversight but no implementation authority, such as the issuing of visas (a state department function), there is certain to be a high degree of bureaucratic disputes and wrangling.

Perhaps the most serious remaining problem in the coordination of homeland security by DoHS will be the issue of intelligence coordination. The Bush Jr. proposal for DoHS does not provide for a consolidation of intelligence functions within the DoHS, unlike other functions. As a consequence, DoHS will be in the position of borrowing or begging for information from existing intelligence agencies in order to amass the data necessary to develop its planned response to potential attacks upon the United States. Consequently, the bureaucratic rivalries and compartmentalization of intelligence assessments that marked the pre–9/11 period are unlikely to be materially affected by the establishment of DoHS. As a result, DoHS runs a real risk of being in the position of developing policy and programs with less than complete information resources.

A final component of the U.S. response to terror through a coordinated homeland security mechanism involves the role of U.S. military forces.[134] Here, too, there is at present a lack of specificity of responsibility as the DoD tries to decide whether the U.S. homeland should be a separate command, and what types of forces might be best allocated to address the type of threat posed by a terroristic, rather than a mass conventional or strategic (nuclear) attack by a foreign power on the United States. As in the case of the formation of DoHS, the process of U.S. decision making on this issue will almost certainly be subject to bureaucratic politics considerations and incrementalism. In addition, the decisions made regarding the proper force structure will inevitably influence questions of overall U.S. conventional force structure (discussed in Chapter 1).

CONCLUSION

Terrorism is now among the highest-priority items on the U.S. foreign policy agenda. Since 11 September 2001 it has come to be seen as affecting not only U.S. security and moral principle goals, but prosperity goals as well. As terrorism has risen in priority on the U.S. foreign policy agenda, the U.S. policy community has had to reorient itself to some degree from its traditional process of bureaucratic competition.

As we have examined the issue of international terrorism, it is clear that although defining terrorism may appear to be a vague, academic exercise, definitions to some degree drive policy. By defining terrorism in particular ways, the government has shaped the responses that the country has elected to adopt toward particular terrorist attacks on U.S. interests. In response to the more recent international terrorist attacks on the United States, the government has been forced to reexamine some of its traditional assumptions about the nature of terrorism, and therefore, the appropriate governmental response to terrorism.

Structural changes in the international system have proven to be important factors in the emergence of terrorism as a U.S. foreign policy concern. The erosion of tight controls of the bipolar Cold War period has increased the flow of goods and people throughout the world. This situation has made it more possible for terrorists to potentially gain access to weaponry such as chemical, biological, radiological, or nuclear weapons and thereby inflict significantly greater damage on their targets. A shift in the structure of the international system—to one in which the United States has both the opportunity and the inclination to involve itself in the affairs of a greater number of states—has created a situation in which the United States has a greater potential to create enemies by its decisions to act or refrain from action. Its position as the leading proponent of economic globalization has also made the United States a primary target for states or groups that are dissatisfied with the effects of that increased economic globalization on their economic standing or ability to uphold their cultural norms.

The technological changes associated with globalization have also significantly affected both the nature of the terrorism faced by the United States and the methods that the United States must employ to counter terrorism. Specifically, the expansion of international air travel has made it more possible for terrorists to move themselves and their equipment around the world in order to engage in terroristic activities. Changes in communications technology, such as the development of the Internet, have made it more possible for terrorists to coordinate their activities and transfer the funds necessary to support their activities. At the same time, changes in the technological capacities of the United States and other key international actors have made it more possible to meet the threats posed by terrorism. However, the nature of the technological capacities of terrorists has also made it more imperative that the United States incorporate various multilateral measures as components in its foreign policy to deal with terrorism.

The U.S. response to terrorism reflects a variety of tensions. Like many issues discussed in this book, U.S. policy toward terrorism reflects a tension between tendencies toward unilateral ad hoc action versus the need for a more coordinated multilateral approach to the problem. Within U.S. policy responses there is a further tension. On the one hand, government has the desire to orchestrate a publicly visible response to terrorism, including the launching of missile attacks or bombing of selected targets associated with the perpetrators of the terrorism. On the other hand, it has the need to execute the potentially more effective, though largely publicly invisible, tactics of constraining future terrorism by disrupting the terrorists' ability to move and fund their operations.

In responding to terrorism, the United States is also faced with the underlying problem of how to hold together the domestic and international coalitions necessary to make its responses most effective. It is becoming more evident that the international coalition initially forged by the United States in light of the particularly heinous nature of the attacks on 11 September 2001 may be somewhat fragile. The United States has been confronted with an unpleasant reality. Despite its success in seizing control of most, if not all, of the territory of Afghanistan and its ability to put into place a provisional government that is more supportive of generally accepted norms of international behavior than was the Taliban government, the provisional government remains fragile at best. Moreover, despite considerable effort, coalition forces have been unable to definitively eliminate a substantial portion of the al-Qaeda network. As a consequence, the United States continues to face a very real threat of either a direct terrorist attack upon the United States or an attack upon U.S. interests overseas by remnants of the al-Qaeda network. Ultimately, the U.S. government must be prepared to formulate a realistic policy to recognize that the most realistic goal it can hope to achieve in addressing the issue of international terrorism is the containment of the problem, not its elimination. Unlike past security threats to the United States, for which there has been a definable locus (country, set of countries, or persons) on which to concentrate its attacks, with the current generation of terrorists, the U.S. government is facing an amorphous set of targets, that is, loosely organized groups of cells that are more difficult to attack and eliminate.

As the United States formulates a long-term strategy to address the threat of international terrorism, it is incumbent upon the government to recognize the increasingly multifaceted nature of the threat posed by terrorists. International terrorists now have at their disposal a vast potential array of weapons in addition to the use of planes as manned missiles directed at civilian targets. Chemical and biological weapons are now more realistic alternatives. In addition, advances in the nature and use of new information technologies have made these both the tool and potential target for terrorists bent on disrupting the U.S. economy and security. It is the paradox of U.S. 21st century security that the United States potentially must now be more concerned about the group that wants one biological, chemical, or nuclear weapon than the state that attempts to produce 20 such weapons. Whereas the state wants the weapons for prestige and diplomatic leverage, the group almost certainly intends to use their one weapon to inflict damage on an enemy state.

The nature of these existent threats makes concerted multilateral approaches to containing terrorism essential. However, such approaches raise profound issues for the U.S. government. For example, in order to maintain the international coalition against international terrorism, will the United States downplay or ignore actions that could be considered state terror by key members of that coalition against their own populations? In addition, if multilateral cooperative actions are required to address the problem of terrorism, will the U.S. government be willing to experience the diminution in its sovereign prerogatives that such cooperation inevitably involves? That is, will the United States be willing to share its intelligence with other states to the same degree that it expects them to share their intelligence with it? Such questions must be debated in the U.S. policy community in the 21st century.

~ Up for Debate ~

Prior to the 11 September 2001 attacks on the World Trade Center and the Pentagon, many in the United States viewed terrorist activity as a limited tactic to attack and frighten peoples and their governments. The result of the 9/11 attacks was a change in U.S. policy. This policy change involved a coordinated, extensive, and prolonged military response on the part of the United States and the rapid development of an international coalition to cooperate with the United States in its efforts to eliminate international terrorist activity.

As the al-Qaeda organization has been disrupted and the search for Osama bin Laden and the remnants of the al-Qaeda network continues, the Bush Jr. administration has begun to provide military personnel to aid the Philippine government in its operations against Moslem terrorist groups in the southern part of that country. The Bush Jr. administration now faces the following questions: Where does the war on terrorism take us now? Do we expand the scope of the war on terrorism and move forward to address other states, such as Iraq, which continue to act as rogue states and support terroristic activities?

Debate the following:

The Bush Jr. administration should take its war against terrorism to a deterrent level. It should bring political and military pressure to bear against Saddam Hussein's continued covert support for international terrorism. The United States should respond forcefully to Saddam Hussein's continued reluctance to honor international demands to allow weapons inspectors from the UN to search for weapons of mass destruction in Iraq. Ultimately, the U.S. government should authorize direct use of military force against Iraq if Saddam Hussein refuses to cooperate fully with international weapons inspection efforts.

Arguments in favor of the debate statement:

Christopher Dickey and John Barry, "Next Up: Saddam," *Newsweek*, December 31, 2001 (accessed 20 January 2002 through Lexis-Nexis).

Dickey and Barry argue that Saddam Hussein will ultimately be a U.S. target, if only because Bush Jr. "and his national-security team have decided that Saddam has to go." They point out that at the very least the Bush Jr. administration wishes to destroy Iraq's capacity to construct weapons of mass destruction (WMDs) and potentially provide these weapons to terrorists. They also argue that opposition to operations against Saddam Hussein is lower in 2002 than it has been in the past several years, and that some Middle Eastern leaders—such as Prince Abdullah of Saudi Arabia—are now willing to discuss the possibility of action against Saddam Hussein.

continued . . .

***Up For Debate* continued . . .**

Michael Eisenstadt, "Iraq's Weapons of Mass Destruction: An Emerging Challenge For The Bush Administration," Policy Watch #515, January 29, 2001. The Washington Institute for Near East Policy; available at http://www.ciaonet.org/ (accessed 7 March 2002).

Eisenstadt speculates about the exact CBW capabilities of Iraq. He argues that Bush Jr. should not rule out "preventive" military action to damage Iraq's WMD capabilities. However, the best way to address the problem of Iraq's WMD is to remove Saddam Hussein and his regime.

Gary Schmitt, "Why Iraq? If Saddam Stays in Power, the War on Terrorism Will Have Failed," *Weekly Standard*, 29 January 2001 (accessed 10 March 2002 through Lexis-Nexis).

Schmitt cites evidence that he believes links Iraq and al-Qaeda in both the 9/11 and the anthrax attacks against the United States. He argues against containment of Iraq and for removing Saddam Hussein from power before Iraq has nuclear capabilities.

Stephen F. Hayes, "Target Iraq? We Will, If Paul Wolfowitz Has His Way," *Weekly Standard*, October 1, 2001 (accessed 12 December 2001 through Lexis-Nexis).

Hayes describes the long history of Wolfowitz's belief that Saddam Hussein should be removed from power and how influential Wolfowitz has become in relationship to other members of the Bush administration.

Nile Gardiner, "British and European Responses to the Proposed U.S. Military Action Against Iraq," Heritage Foundation, April 1, 2002; available at http://www.heritage.org/Research/MiddleEast/BG1531ES.cfm (accessed 10 May 2002).

Gardiner details the reasons Prime Minister Tony Blair might not support U.S. military action against Saddam Hussein's regime, but concludes that it is "highly likely" that Britain will offer its support "should Saddam Hussein continue to pursue programs to acquire weapons of mass destruction."

Robert Kagan and William Kristol, "What to Do About Iraq: For the War on Terrorism to Succeed, Saddam Hussein Must Be Removed," *Weekly Standard,* January 21, 2002 (accessed 20 March 2002 through Lexis-Nexis).

Kagan and Kristol discuss Iraqi WMD capabilities, including (1) nuclear weapons (suspected to be imminent); (2) VX, a lethal chemical weapon in amounts as small as a drop; and (3) weapons-grade anthrax. The authors suggest a unilateral action against Iraq is an acceptable risk, given Iraq's WMD capabilities and the likelihood of their using them against the United States or its allies. However, the authors agree that any strike must work quickly and cannot be modeled on the conventional force structure used in Afghanistan.

continued . . .

Up For Debate continued . . .

Arguments opposing the debate statement:

Phillip H. Gordon and Michael E. O'Hanlon, "Should the War on Terrorism Target Iraq? Implementing a Bush Doctrine on Deterrence," Policy Brief #93, January 2002, The Brookings Institution; available at http://www.brook.edu/comm/policybriefs/pb93.htm (accessed 21 January, 2002).

Gordon and O'Hanlon offer a variety of reasons that Saddam Hussein would not be an appropriate next target for the U.S. War on Terrorism, despite his clear support for terrorist causes. These reasons include among others, the weakness of opposition forces in Iraq, the inability of the United States to oust Saddam Hussein using air power alone, the lack of allies for the United States in such an operation, and the generally unfavorable international reaction that would occur if the United States were to mount such an operation either unilaterally or as part of a small coalition of developed states.

Charles Duelfer, "Inspectors in Iraq?" *Washington Post*, 9 January 2002; available at http://www.globalpolicy.org/unmovic/2002/At the site click on site search and type the title (accessed 7 March 2002).

Duelfer emphasizes the risks of any plan to pressure Saddam Hussein into accepting weapons inspectors.

Jessica Mathews, "The Wrong Target," *Washington Post*, 4 March 2002; available at http://www.globalpolicy.org/ At the site use site search (accessed 7 March 2002).

Matthews argues that the United States should "force" Iraq to comply with UN Security Council resolutions requiring it to eliminate its WMD program. However, the United States should not overthrow Saddam Hussein's regime, because the United States lacks international support for this action and a new regime may also favor the use of WMD.

For a balanced chronology of articles dealing with the issue of Iraq and weapons of mass destruction, see the Global Policy Forum at:

"Iraq Crisis, Weapons Inspection;" available at http://www.globalpolicy.org/security/issues/irqindx2.htm (accessed 7 March 2002).

SUGGESTED READINGS AND RESOURCES

Adams, James. "Cyberthreat: Protecting U.S. Information Networks." "Information Warfare: Challenge and Opportunity." *U.S. Foreign Policy Agenda*, November 1998. Available at http://usinfo.state.gov/journals/itps/1198/ijpe/pj48adam.htm

Alexander, Yonah, and Michael Swetnam. *Cyber Terrorism and Information Warfare: Threats and Responses.* MS Reader: Oceana Publishers, November 2001.

America's Response to Terrorism. Available at http://www.brook.edu/dybdocroot/terrorism/

Betts, Richard K. "The New Threat of Mass Destruction: What If McVeigh Had Used Anthrax?" *Foreign Affairs.* Available at http://www.ciaonet.org/ (accessed 30 October 2001).

Campbell, Kurt M., and Michele A. Flournoy. *To Prevail: An American Strategy for the Campaign Against Terrorism.* Washington, D.C.: Center for Strategic and International Studies, 2001.

CNN.com. Material on Cyberterrorism:

Verton, Dan. "Interview: Outflanking the Cyberterrorist Threat." 11 April 2002.

Venzke, Ben. "Expert Ben Venzke on the 'Code Red' Worm." 31 July 2001.

Walton, Marsha. "Companies Examine Cyber-security." 6 September 2001.

Williams, Martyn. "Rumsfeld: Cyberwar Among Possible Threats." 4 February 2002.

Combs, Cindy C. *Terrorism in the Twenty-First Century,* 2nd and 3rd eds. Upper Saddle River, N.J.: Prentice Hall, 2001 and 2002.

Cordesman, Anthony H., and Justin G. Cordesman. *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection.* New York: Greenwood, 2001.

Counter-Terrorism Issues Page. Available at http://www.cdt.org/policy/terrorism/ (The Center for Democracy and Technology site offers access to various reports and analyses relating to counterterrorism legislation and U.S. agency roles.)

Crenshaw, Martha, and John Pimlott, eds. *Encyclopedia of World Terrorism.* Armonk, N.Y.: M. E. Sharpe, 1996), 3 vols.

Cyber Protests: The Threat to the U.S. Information Infrastructure, October 2001. Available at http://www.nipc.gov/publications/nipcpub/nipcpub.htm

de Borchgrave, Arnaud, Frank J. Cilluffo, Sharon L. Cardash, and Michele M. Ledgewood. *Cyber Threats and Information Security: Meeting the 21st Century Challenge.* Washington, D.C.: Center for Strategic and International Studies, 2001.

Deutch, John. "Think Again: Terrorism." *Foreign Policy,* Fall 1997; reprinted September–October 2001.

Eland, Ivan. "Does U.S. Intervention Overseas Breed Terrorism?: The Historical Record." *Foreign Policy Briefing,* December 17, 1998. Washington, D.C.: Cato Institute. Available at http://www.ciaonet.org/ (accessed 3 November 2001).

ERRI (Emergency Response and Research Institute). Counter-Terrorism Archive. Available at http://www.emergency.com/cntrterr.htm (Provides a summary of worldwide terrorism events, groups, terrorist strategies, and tactics. Offers various full-text articles and reports arranged under regions. Also provides a section on histories of terrorist leaders, and related websites).

Falkenrath, Richard A. "Analytic Models and Policy Prescription: Understanding Recent Innovation in U.S. Counterterrorism." *BCSIA Discussion Paper 2000-31, ESDP Discussion Paper 2000-03,* John F. Kennedy School of Government, Harvard University, October 2000. Available at http://www.ciaonet.org/wps

Federal Computer Incident Response Center. Available at http://www.fedcirc.gov

Garrett, Laurie. "The Nightmare of Bioterrorism." *Foreign Affairs,* January–February 2001.

The Gilmore Commission. "Toward a National Strategy for Combating Terrorism." Washington, D.C.: Rand, 2000. Available at http://www.rand.org/nsrd/terrpanel

______. "For Ray Downey." Washington, D.C.: Rand, 15 December 2001.

Hoffman, Bruce. "Terrorism and Counterterrorism." *U.S. Foreign Policy Agenda* 6 November 2001. Available at http://www.ciaonet.org

______. *Terrorism and Weapons of Mass Destruction: An Analysis of Trends and Motivations*. P-8039-1 Santa Monica, Calif.: Rand, 1999.

Hoge, James F. Jr., and Gideon Rose, eds. *How Did This Happen? Terrorism and the New War.* New York: Public Affairs, 2001.

Homer-Dixon, Thomas. "The Rise of Complex Terrorism." *Foreign Policy,* January–February 2002.

Institute for Security Technology Studies at Dartmouth College. Available at http://www.ists.dartmouth.edu

Institute for Security Technology Studies. "Counterterrorism: a Compendium of Recommendations 2000." Available at http://www.ists.dartmouth.edu/ISTS/counterterrorism/ct_compendium.htm

Juergensmeyer, Mark. *Terror in the Mind of God: The Global Rise of Religious Violence.* Berkeley: University of California Press, 2001.

Kayyem, Juliette N. "U.S. Preparations for Biological Terrorism: Legal Limitations and the Need for Planning." *BCSIA Discussion Paper 2001-4, ESDP Discussion Paper 2001–02,* John F. Kennedy School of Government, Harvard University, March 2001. Available at http://www.ciaonet.org/

Kushner, Harvey W., ed. *The Future of Terrorism: Violence in the New Millennium.* Thousand Oaks: Sage Publications, 1997.

Legislation related to the attack of September 11, 2001. Available through THOMAS at http://thomas.loc.gov/ search phrase: terrorism.

Laquer, Walter. "Postmodern Terrorism: New Rules for an Old Game." *Foreign Affairs,* September–October 1996.

______. "The New Face of Terror." *Washington Quarterly,* Vol. 2, No. 4 Autumn 1998.

Larsen, Randall J., and Ruth A. David. "Homeland Defense: Assumptions First, Strategy Second." *Journal of Homeland Security,* October 2000.

Lessig, Lawrence. "The Internet Under Seige." *Foreign Policy,* November–December 2001.

Martin, Col. John R., ed. "Defeating Terrorism: Strategic Issues Analyses." Carlisle, Pa.: Strategic Studies Institute, United States Army. Available at http://www.carlisle.army.mil/usassi/main.html terror

National Commission on Terrorism. *Countering the Changing Threat of International Terrorism.* Available at http://www.fas.org/ irp/threat/commission.html

National Infrastructure Protection Center (NIPC). Available at http://www.nipc.gov

National Infrastructure Protection Center, related sites with links. Available at http://www.nipc.gov/sites.htm

NIPC. Cyber Protests Related to the War on Terrorism: The Current Threat. Available at http://www.nipc.gov/publications/nipcpub/cyberprotests1101.pdf

Pate, Jason. "Anthrax and Mass-Casualty Terrorism: What Is the Bioterrorist Threat After September 11th?" *U.S. Foreign Policy Agenda* 6 (November 2001). Available at http://www.ciaonet.org/

Pillar, Paul R. "The Instruments of Counterterrorism." *U.S. Foreign Policy Agenda* 6 November 2001. Available at http://www.ciaonet.org/

______. *Terrorism and U.S. Foreign Policy.* Washington, D.C.: Brookings Institution Press, 2001.

Regan, Tom. "When Terrorists Turn to the Internet." *Christian Science Monitor,* July 1, 1999.

Rodgers, Paul. "Protecting America against Cyberterrorism." *U.S. Foreign Policy Agenda* 6 November 2001. Available at http://www.ciaonet.org/

Rothkopf, David J. "Business versus Terror." *Foreign Policy,* May–June 2002.

Schweitzer, Glenn E., and Carole Dorsch Schweitzer. *A Faceless Enemy: The Origins of Modern Terrorism.* New York: Perseus Press, 2002.

Schweitzer, Glenn E., and Carole C. Dorsch. *Superterrorism: Assassins, Mobsters, and Weapons of Mass Destruction.* New York: Plenum Trade, 1998.

Senate Treaty Approval relevant to terrorism. Available at http://www.senate.gov/legislative/legis_act_treaties_approved.html

Sofaer, Abraham D., et al. "A Proposal for an International Convention on Cyber Crime and Terrorism." The Hoover Institution, The Consortium for Research on Information Security and Policy (CRISP), and The Center for International Security and Cooperation, Stanford University (CISAC), August 2000. Available at http://www.ciaonet.org/

SysAdmin, Audit, Network, Security (SANS) Institute. Available at http://www. sans.org

The RMA Debate: A gateway to full-text online resources about the Revolution in Military Affairs, information war, and asymmetric warfare: Terrorism and Counter-terrorism. Available at http://www.comw.org/rma/fulltext/terrorism.html

Talbott, Strobe, and Nayan Chanda, eds. *The Age of Terror: America and the World After September 11.* New York: Basic Books, 2002.

Thachuk, Kimberly L. "Terrorism's Financial Lifeline: Can It Be Severed?" *Strategic Forum,* May 2002. Available at http://www.ndu.edu/inss/strforum/sf191.html

Tomisek, Steven J. "Homeland Security: The New Role for Defense," *Strategic Forum,* February 2002. Available at http://www.ndu.edu/inss/strforum/sf189.htm

Tucker, Jonathan B. "Chemical and Biological Terrorism: How Real a Threat?" *Current History,* April 2000.

U.S. Commission on National Security/21st Century's "Road Map for National Security: Imperative for Change" (Hart-Rudman Commission). Washington, D.C.: USCNS, 2001. Available at http://www.nssg.gov/Reports/reports.htm

U.S. Department of State. *Background Information on Terrorist Groups.* Available at http://www.state.gov/s/ct/rls/pgtrpt/2000/2450.htm (accessed 23 July 2002). Offers a report with each group's aliases, decisions, activities, strength, location, and external aid from the U.S State Department's Office of Counterterrorism.

Vatis, Michael A. "Cyber Attacks During the War on Terrorism: A Predictive Analysis." Hanover, N.H.: Institute for Security Technology Studies at Dartmouth College, September 22, 2001. Available at: http://www.ists.dartmouth.edu/

______. Director, National Infrastructure Protection Center, Federal Bureau of Investigation. "Statement for the Record," Before the Senate Judiciary Committee, Subcommittee on Technology and Terrorism, Washington D.C., October 6, 1999.

NOTES

1. Paul, Johnson, "The Seven Deadly Sins of Terrorism," Chapter 6 in Charles W. Kegley Jr., ed., *International Terrorism: Characteristics, Causes, Controls* (New York: St. Martin's Press, 1990), p. 64.
2. Some parts of this chapter were being written when these events were barely a week old. A chronology of these events can be found at CNN NEWS at: http://www.cnn.com/2001/US/09/11/chronology.attack/index.html

3. George W. Bush, "Executive Order 13224—Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten to Commit, or Support Terrorism," September 2001; available at http://www.treasury.gov/terrorism.html
4. As quoted by Ivan Eland, "Does U.S. Intervention Overseas Breed Terrorism?: The Historical Record," Foreign Policy Briefing, no. 50, Cato Institute, December 17, 1998. Available at http://www.ciaonet.org/ (accessed 11 February 2001 through CIAO).
5. See the *Patterns of Global Terrorism* website. This site contains annual State Department reports of patterns of global terrorism since 1995. Available at http://www.usis.usemb.se/terror (accessed on 3 November 2001) and http://www.state.gov/s/ct/rls/pgtrpt/2001/html/ for the 2001 report.
6. Andrew J. Bacevich, "Terrorizing the Truth," *Foreign Policy,* July–August 2001, 74–75.
7. Center for Defense Information. "List of Known Terrorist Organizations," Updated 28 May 2002,*Terrorism Project;* available at http://www.cdi.org/terrorism/terrorist-groups.cfm (accessed 20 July 2002).
8. Ehud Sprinzak, "The Great Superterrorism Scare," *Foreign Policy,* Fall 1998.
9. Ehud Sprinzak, "Revisiting the Superterrorism Debate," *Foreign Policy*, September–October 2001.
10. *Patterns of Global Terrorism: 2000.*
11. Sprinzak, "Revisiting the Superterrorism Debate,"114–115.
12. Bruce Hoffman, "Is Europe Soft on Terrorism?" *Foreign Policy*, Summer 1999. Bruce Hoffman has been an advisor on terrorism to the Bush Jr. administration.
13. Office of Counterterrorism of the U.S. Department of State. Available at http://www.state.gov/s/ct/ (accessed 30 September 2001).
14. Hoffman, "Is Europe Soft on Terrorism?" 2.
15. Hoffman, 2.
16. Bacevich, "Terrorizing the Truth," 74–75.
17. For a broader discussion of these groups, see Benjamin Netanyahu, *Fighting Terrorism: How Democracies Can Defeat Domestic and International Terrorists* (New York: Farrar, Straus Giroux, 1995), 59–63.
18. *Patterns of Global Terrorism: 2000,* 2.
19. *Patterns of Global Terrorism: 2000.*
20. Stephen Zunes, "In Focus: International Terrorism," *Foreign Policy in Focus,* November 1998. Revised article, September 2001, available at http://www.fpif.org/briefs/vol3/v3n38terr_body.html
21. Bacevich, "Terrorizing the Truth," 74.
22. Romesh Ratnesar, "All for One . . . For Now," *Time Europe*, October 1, 2001 (accessed through Lexis-Nexis 20 October 2001).
23. "Deficit Warning Sounded Over Post-Attack Spending," *CNN News;* available at http://www.cnn.com/2001/US/09/25/gen.america.under.attack/index.html (accessed 31 October 2001).
24. *Patterns of Global Terrorism: 2000,* 2.
25. Jamie McIntyre, "Army's Controversial 'School of the Americas' to Close Friday," *CNN News,* December 12, 2000; available at http://www.cnn.com/2000/WORLD/americas/12/12/school.americas/index.html (accessed 30 September 2001).
26. Zunes, "In Focus: International Terrorism," 1.
27. *CNN News,* "Deficit Warning Sounded."

28. Zunes, "In Focus: International Terrorism."
29. David Lamb, *The Arabs: Journeys Beyond the Mirage* (New York: Random House, 1987), 89. See 2nd edition of 2002 for more recent information.
30. Lamb, 90.
31. Paul Johnson, "Seven Deadly Sins of Terrorism," 63.
32. Bacevich, "Terrorizing the Truth," 75.
33. *Combating Terrorism: Issues in Managing Counterterrorist Program*, Statement of Norman J. Rabkin, Director National Security Preparedness Issues, National Security and International Affairs Division, before the Subcommittee on Oversight, Investigations and Emergency Management, Committee on Transportation and Infrastructure, House of Representatives (GAO/T-NSIAD-00-145).
34. *Combating Terrorism.*
35. Report of the Advisory Panel to Assess Domestic Response Capabilities for Terrorists Involving Weapons of Mass Destruction: Toward a National Strategy for Combating Terrorism. Second Annual Report, December 15, 2000. Chairman James S. Gilmore III, Governor of Virginia; available at http://www.rand.org/nsrd/terrpanel/ (accessed 23 July 2002).
36. Brian M. Jenkins, "International Terrorism: The Other World War," Chapter 1 in Charles W. Kegley Jr., ed., *International Terrorism: Characteristics, Causes, Controls* (New York: St. Martin's Press, 1990), 36.
37. Quoted in "Information Warfare: An Old Operational Concept with New Implications," by Abe Singer and Scott Rowell, National Defense University, Institute for National Strategic Studies, December 1996. Available at http://www.ndu.edu/inss/strforum/forum99.html (accessed 15 October 2001).
38. James Lindsay and Gregory Michaelidis, "Bush's Flair for Unilateralism Not Boosting International Ties," *Philadelphia Inquirer,* August 3, 2001. Available at http://www.brook.edu/dybdocrootviews/op-ed/lindsay/200108003.htm (accessed 7 August 2001).
39. Philip Gordon and Justin Vaisse, "All Treaties Are Not Equal," *Le Monde* (France), 8 September 2001 (accessed 2 January 2002 through Lexis-Nexis).
40. Azadeh Moaveni, "We Need to Work Together," *Time Europe,* September 26, 2001 (accessed 2 January 2002 through Lexis-Nexis).
41. U.S. Department of Defense, *Terrorist Group Profiles* (Washington, D.C.: March 1989), viii.
42. Department of Defense, *Terrorist Group Profiles.* See also *Patterns of Global Terrorism,* Annual Reports for 1998 and 1999, accessed through the U.S. State Department website.
43. Non-state actors are private groups that have the capacity to influence international events and interact on the world stage. These include terrorist organizations, national liberation movements, multinational corporations, and international public interest groups.
44. Peter A. Chalk, "'Grey Area Phenomena' and Human Security," Chapter 8 in William T. Tow, Ramesh Thakur, and In-Taek Hyun, eds., *Asia's Emerging Regional Order: Reconciling Traditional and Human Security* (New York: United Nations University, 2000), available at http://www.ciaonet.org/ (accessed 20 August 2001).
45. Chalk, 127.
46. Peter C. Sederberg, "Responses to Dissident Terrorism: From Myth to Maturity," Chapter 28 in Kegley, *International Terrorism;* and Peter C. Sederberg, *Terrorist Myths: Illusion, Rhetoric, and Reality* (Englewood Cliffs, N.J.: Prentice Hall, 1989).

47. Sederberg, *Terrorist Myths.* 51.
48. Sederberg, 53.
49. Eland, "U.S. Intervention."
50. Sederberg, *Terrorist Myths,* 53–56.
51. Sederberg, 64.
52. Sederberg, 65.
53. Michael Stohl, "Demystifying the Mystery of International Terrorism," in Kegley, *International Terrorism,* 86.
54. "What Terrorists Want," *The New Yorker*, October 29, 2001.
55. Kshitij Prabha, "Defining Terrorism," *Strategic Analysis: A Monthly Journal of the IDSA,* April 2000, 125–135.
56. Stohl, "Demystifying International Terrorism," 86.
57. Stohl, 86.
58. Stohl, 86.
59. Prabha, "Defining Terrorism," 125–135.
60. Prabha, 86.
61. Prabha.
62. Prabha, 7.
63. John Deutch, "Terrorism," *Foreign Policy*, Fall 1997; see chart on p. 16 of this article, which shows statistics on casualties of international terrorists, 1991–1996.
64. "Bin Laden denies role in New York, Washington Slaughter," *CNN News,* September 16, 2001; Available at http://www.cnn.com (accessed 20 September 2001).
65. "Taliban given three days to hand over bin Laden," *CNN News,* September 16, 2001. http://www.cnn.com (accessed 30 September 2001).
66. Azadeh Moaveni, "We Need to Work Together," *Time Europe,* September 26, 2001.
67. "White House Reviewing Rules Governing CIA," *CNN News,* September 16, 2001; available at http://www.cnn.com/2001/US/09/16/gen.powell.cia/index.html (accessed 23 July 2002).
68. *Report: Clinton Targeted Bin Laden,* CBS *60 Minutes* Correspondent Lesley Stahl, September 16, 2001; available at http://www.cbsnews.com/stories/2001/09/16/national/main311490.shtml (accessed 23 July 2002).
69. Zunes, "In Focus: International Terrorism," 3.
70. Zunes, 2.
71. Zunes, 2.
72. Sederberg, *Terrorist Myths,* 133.
73. "Bush Vows to Rid World of 'Evil-Doers'," CNN News, September 16, 2001.
74. Sederberg, "Responses to Dissident Terrorism," 262–263.
75. "Chronology of State Use and Biological and Chemical Weapons Control," *Chemical and Biological Weapons Resource Page*, Center for Nonproliferation Studies, Monterey Institute of International Studies. Available at http://cns.miis.edu/research/cbw/pastuse.htm (accessed 2 February 2002).
76. "Chronology."
77. "Plague War," *PBS Frontline Series.* Available at http://www.pbs.org/wgbh/pages/frontline/shows/plague/etc/cron.html (accessed 5 March 2002).

78. Nadine Gurr and Benjamin Cole, *The New Face of Terrorism: Threats from Weapons of Mass Destruction* (New York: I. B. Taurus, 2000).

79. United Nations, United Nations Special Commission (UNSCOM), "Latest Six-Monthly Report," April 16, 1998. Available at http://www.un.org/Depts/unscom/s98-332.htm (accessed 5 May 2001).

80. Richard A. Falkenrath, Robert D. Newman, and Bradley A. Thayer, *America's Achilles' Heel: Nuclear, Biological and Chemical Terrorism and Covert Attack* (Cambridge, Mass.: MIT Press, 1998), 17–21.

81. Falkenrath, Newman, and Thayer, 14.

82. Gurr and Cole, *New Face of Terrorism,* 14–16.

83. Laura Beers, "New Non-Proliferation Initiative Zeros in on Non-Nuclear Threat," *Weekly Defense Monitor,* Center for Defense Information, June 17, 1999.

84. For an extensive and interesting elaboration on these conventions, see Laura K. Donahue, "In the Name of National Security: U.S. Counterterrorist Measures, 1960–2000." BCSIA Discussion Paper 2001-6, ESDP Discussion ESDP-2001-04, John F. Kennedy School of Government, Harvard University, August 2001.

85. Donahue, 9.

86. Donahue, 10.

87. Donahue.

88. Ron Purver, "Chemical and Biological Terrorism: New Threat to Public Safety?" *Conflict Studies* 295 (December 1996–January 1997): 20.

89. Gurr and Cole, *New Face of Terrorism,* 8.

90. Phil Williams and Ernesto Savona, eds., *The UN and Transnational Organized Crime* (London: Frank Cass, 1996), 142.

91. "U.S. Foils Spate of bin Laden Bomb Attacks," *The Times,* 25 February 1999.

92. For a more complete discussion of the case, see Falkenrath, Newman, and Thayer, *America's Achilles' Heel,* 40–41.

93. Gurr and Cole, *New Face of Terrorism,* 215–218.

94. Gurr and Cole, 221.

95. Thomas J. Badey, "U.S. Anti-Terrorism Policy: The Clinton Administration," *Contemporary Security Policy,* August 1998, 60–61.

96. To learn more about these specific conventions see John F. Murphy, "Co-operative International Arrangements: Prevention of Nuclear Terrorism and the Extradition and Prosecution of Terrorists," in *Preventing Nuclear Terrorism: The Report and Papers of the International Task Force on Prevention of Nuclear Terrorism*, Paul A. Leventhal and Yonah Alexander, eds. (New York: Free Press, 1987). For an updated version of this book with links after 11 September 2001 http://www.nci.org/nci-nt.htm

97. Gurr and Cole, *New Face of Terrorism,* 227.

98. Donohue, "In the Name of National Security," 10.

99. NIPC, "Cyber Protests: The Threat to the U.S. Information Infrastructure, October 2001;" available at http://www.nipc.gov/publications/nipcpub/nipcpub.htm (accessed 24 July 2002).

100. Michael Vatis, "Cyber Attacks During the War on Terrorism: A Predictive Analysis" (Hanover, N.H.: Institute for Security Technology Studies, Dartmouth College, September 21, 2001), 6–7.

101. Tom Regan, "When Terrorists Turn to the Internet," *Christian Science Monitor,* July 1, 1999.
102. "China–U.S. Cyber War Escalates," CNN.com/World, May 1, 2001.
103. NIPC, "Cyber Protests Related to the War on Terrorism: The Current Threat," p. 1; available at: http://www.nipc.gov/publications/nipcpub/nipcpub.htm (accessed 24 July 2002).
104. Regan, "When Terrorists Turn to the Internet," 17.
105. Regan.
106. Dan Kuehl, "Defining Information Power," *Strategic Forum*, Institute for National Strategic Studies, National Defense University, June 1997; available at http://ndu.edu/inss/strforum/forum115.html (accessed 10 October 2001).
107. Joseph Pitts, "Electronic Warfare in the Information Age," *Journal of Electronic Defense,* July 2000; available at http://www.jedonline.com/ (accessed 9 August 2001).
108. Kopp, Carlo, "The Electronic Bomb—a Weapon of Electrical Mass Destruction," available at http://www.airpower.maxwell.af.mil/airchronicles/kopp/apjemp.html (accessed 20 July 2002).
109. Martin Libicki, "Rethinking War: The Mouse's New Roar?" *Foreign Policy,* Winter 1999–2000.
110. James Adams, Cyberthreat: Protecting U.S. Information Networks, "Information Warfare: Challenge and Opportunity," *USIA Electronic Journal* 3, (November 1998); available at http://usinfo.state.gov/journals/itps/1198/ijpe/pj48adam.htm (accessed 2 August 2001).
111. Adams, 1.
112. John Arquilla, "Screen Saver," *The New Republic,* May 1, 2000, 16–18.
113. Adams, "Information Warfare," 1–4.
114. Dan Verton, "False Sense of Cybersecurity: A Costly Problem for U.S.," *Federal Computer Week,* 22 June 2000 CNN.com. Available at http://www.cnn.com/2000/TECH/computing/ 06/20/false.cybersecurity.idg/index.html (accessed 25 July 2002).
115. Christopher W. Herrick, Interview with Michael Vatis, Director, Institute for Security Technology Studies, Dartmouth College, July 12, 2002.
116. Vatis interview.
117. Vatis interview.
118. Taken from "Fact Sheet: Protecting America's Critical Infrastructure", available at http://www.usinfo.state.gov/journals/itps/1198/ijpe/pj48wpfx.htm (accessed 20 June 2001).
119. Vatis interview.
120. Vatis interview.
121. Vatis interview.
122. This action has involved increased security in the financial industry and in the health care industry (Vatis interview).
123. Vatis interview.
124. "Fighting Cybercrime," Statement of Chris Klaus before the Senate Judiciary Committee, July 25, 2001. FDH Congressional Testimony, Item No. 32Y20019200001577.
125. "Fighting Cybercrime."
126. Major Robert D. Critchlow, "Whom the Gods Would Destroy," *Naval War College Review* (Summer 2000): 21.

127. Critchlow, 21. See also Ben Venzke, "Expert Ben Venzke on the 'Code Red' Worm," *CNN.com,* July 31, 2001.

128. *Patterns of Global Terrorism: 2000,* 2.

129. Available at http://www.treasury.gov/terrorism.html (accessed 3 November 2001).

130. Bruce Hoffman, "Is Europe Soft on Terrorism?" *Foreign Policy,* Summer 1999.

131. *BBC News,* "Flight to Disaster," April 21, 2000; available at http://news.bbc.co.uk/hi/english/world/newsid_721000/721674.stm (accessed 5 September 2001).

132. Center for Defense Information, "President Bush Proposes New Homeland Security Department," CDI Terrorism Project, June 11, 2002; available at: http://www.cdi.org/terrorism/hsdepartment-pr.cfm See also "The National Strategy for Homeland Security: Office of Homeland Security" issued September 20, 2002, available at http://www.whitehouse.gov/homeland/book/index.html and an analysis and evaluation of Bush Jr.'s national strategy for homeland security from the Brookings Institution, Ivo H. Daadler, James M. Lindsay, and James B. Steinberg, "The Bush National Security Strategy: An Evaluation," 4 October 2002; available at http://www.brookings.edu (accessed 4 October 2002). This analysis will later be published as a policy brief.

133. See, for example, Anne Kohnen, "Responding to the Threat of Agroterrorism: Specific Recommendations for the United States Department of Agriculture," International Security Program, Belfer Center for Science and Intergovernmental Affairs (BCSIA), Harvard University, October 2000 (accessed 1 May 2002 through CIAO).

134. Michael Dobbs, Cdr. USN, "Establishing a CINC for Homeland Security," *Journal of Homeland Security* (October 2001); available at http://www.homelandsecurity.org/journal/Articles/Dobbs_Oct01.htm. See also Center for Defense Information, "New Homeland Unified Command's Establishment Full of Difficulties," CDI Terrorism Project, April 8, 2002, available at http://www.cdi.org/terrorism/homeland-command-pr.cfm (accessed 5 May 2002).

To counter terrorism, the FBI's top investigative priority, we use our investigative and intelligence capabilities to neutralize domestic extremists and help dismantle terrorist networks worldwide.Â Protecting the United States from terrorist attacks is the FBIâ€™s number one priority. The Bureau works closely with its partners to neutralize terrorist cells and operatives International terrorism is a post-cold war phenomenon when forces driven by religious sentiments and factional sub-nationalism appeared in the aftermath of bi-polarity. State sponsored terrorism received a fillip due to advanced military hardware. Terrorism acquired a different face during 1990â€™s. They started taking advantage of the openness of information technology and easy availability of sophisticated weapons not-with-standing the use of computers and access to chemical and biological agents. Terrorism encompasses a range of complex threats. We focus on identifying terrorists and preventing their activities.Â Terrorist groups incite individuals, often young people, to leave their communities across the world and travel to conflict zones, primarily in Iraq and Syria and increasingly in Libya.