STRATEGY RESEARCH PROJECT



# REVIEW AND ASSESSMENT OF UNITED STATES STRATEGY TO COMBAT TERRORISM

BY

COMMANDER RICHARD A. RAINER JR.
United States Navy



USAWC CLASS OF 2002

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

# REVIEW AND ASSESSMENT OF UNITED STATES STRATEGY TO COMBAT TERRORISM

by

CDR Richard A. Rainer Jr.
United States Navy

LTC Antulio J. Echevarria II
Project Advisor



U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

## ABSTRACT

AUTHOR: Commander Richard A. Rainer Jr., USN

TITLE: REVIEW AND ASSESSMENT OF UNITED STATES STRATEGY TO COMBAT TERRORISM

FORMAT: Strategy Research Project

DATE: 09 April 2002 PAGES: 66 CLASSIFICATION: Unclassified

The striking difference between the terrorism on September 11, 2001 (9/11), and previous terrorist events was the magnitude and success of these attacks in a society where it never happened before. In response, the Bush administration is leading a worldwide campaign against terrorism. Using unclassified sources, this research project reviews and assesses United States strategy to combat terrorism. The strength in evolving U.S. strategy to combat terrorism lies in its dependence on all elements of national power ranging from diplomacy, international cooperation and constructive engagement to economic sanctions, covert action, physical security enhancement and military force. These initiatives should be continued. This paper will discuss the strengths and deficiencies of selected elements in U.S. counter-terrorism policy and recommend changes to increase effectiveness of U.S. strategy to combat terrorism. Overall, the U.S. strategy appears to be effective. However, specific elements in U.S. strategy — organizations to combat terrorism, diplomatic policy to strike at roots of terrorism anti-Americanism, intelligence collection, allied and coalition involvement in counter-terrorism, use of the military, border controls, the media, and WMD nonproliferation — must be improved in order to make it more effective.

TABLE OF CONTENTS

## LIST OF ILLUSTRATIONS

## REVIEW AND ASSESSMENT OF UNITED STATES STRATEGY TO COMBAT TERRORISM

> The exertions which a nation is prepared to make to protect its individual representatives or citizens from outrage is one of the truest measures of its greatness as an organized State.
>
> — Winston S. Churchill, 3 September 1918

The striking difference between the terrorism on September 11, 2001 (9/11), and previous terrorist events was the magnitude and success of these attacks in a society where it never happened before. On 9/11, terrorists attacked something and people that had nothing to do with the state. For that reason, the U.S. has been drawn into a new era of terrorist activity. In the almost prophetic words of William Cohen, former Secretary of Defense: "Welcome to the grave New World of terrorism."[1]

In response, the Bush administration leading a worldwide campaign against terrorism. Key administration officials, particularly President Bush, Secretary of Defense Donald Rumsfeld, and Secretary of State Colin Powell, have emphasized that their long-term objective is the destruction of terrorism — a goal to be achieved by the death or apprehension of terrorists, the destruction of their infrastructure and support base, and retaliation against states that aid or harbor terrorists. Using unclassified sources, this paper reviews evolving U.S. strategy to combat terrorism, assesses select elements of our strategy, and provides recommendations for improvement.

The President established the Office of Homeland Security as a mechanism by which to coordinate more than 50 Federal agencies that have a role in combating terrorism. The head of this new office's most important task will be to develop a comprehensive national strategy to combat terrorism and other emerging threats. The strength in evolving U.S. strategy to combat terrorism lies in its dependence on all elements of national power ranging from diplomacy, international cooperation and constructive engagement to economic sanctions, covert action, physical security enhancement and military force. These initiatives should be continued.

Overall, the U.S. strategy appears to be effective. The world seems to be responding favorably to U.S. leadership in the fight against terrorism, and coalescing around a common desire for international stability and prosperity — that which terrorism seeks to disrupt. However, specific elements in U.S. strategy — organizations to combat terrorism, diplomatic policy to strike at roots of terrorism anti-Americanism, intelligence collection, allied and coalition involvement in counter-terrorism, use of the military, border controls, themedia, and WMD nonproliferation — must be improved in order to make it more effective.

## DEFINITIONS

Terrorism is variously defined by different organizations, governments, and cultures according to the frame of reference and point of view of the one doing the defining. However, all definitions seem to share one common element: politically motivated behavior.[2] Broadly defined, terrorism is politically motivated violence, perpetrated against noncombatant targets by sub-national groups or agents, usually intended to influence an audience.[3] The term "international terrorism" is generally used to describe terrorism involving the territory or the citizens of more than one country. A "terrorist group" is any group that practices, or has significant subgroups that practice international terrorism. Antiterrorism involves all defensive measures employed to protect personnel and facilities against terrorist incidents. Counter-terrorism refers to offensive measures to deter, preempt and resolve a terrorist act.[4]

## THE THREAT OF TERRORISM

Approximately 47% of all terrorist incidents in 2000 were committed against U.S. citizens.[5] During his tenure as Secretary of Defense, William Cohen declared that terrorism would present the main strategic threat to the U.S. in the 21st century. The National Intelligence Council predicts the U.S. will face an increase in asymmetric threats and the potential unconventional delivery of WMD in the near future — a future in which our adversaries avoid direct confrontation and concentrate on strategies, tactics and weapons to exploit our weaknesses.[6] In a study of future sources of terrorism, Dr. Ian O. Lesser (a RAND analyst and former member of the U.S. State Department's Policy Planning Staff) identified six possible forces behind future terrorism: [7]

- The emergence of terrorism from non-traditional agendas and regions.
- Terrorists (and their victims) will have increasingly more to do with non-state, private, and criminal concerns.
- The U.S. revolution in military affairs will drive adversaries toward asymmetric strategies.
- Emergence of new ideological struggles.
- Terrorism carried out by the defeated or contained.
- Growing tendency toward terrorism divorced from any coherent political agenda.

In a discussion panel structured to examine issues that will shape future American defense policy, Ambassador Robert Oakley asserted that "future crisis will evolve from the rising number of failed states" along with nations disgruntled over the disparity of wealth between them and advanced countries.[8] In the past, small highly centralized groups, defined by a set of

common political, social or economic objectives, practiced terrorism in selective and discriminate acts of violence.[9]

What we are seeing now is a rise in terrorist organizations with "less-comprehensible nationalist or ideological motivations" and more "diffuse structure and leadership."[10] Beginning in the 1980s, a significant share of terrorist groups has been motivated at least partly by religion.[11] Extremist Islamic fundamentalist groups are seen as a particular threat to U.S. foreign policy goals and objectives.[12]

Dr. Lesser reasons the more universal actions of "new terrorism" carry profound lethal implications.[13] "The destruction of the World Trade Center and the severe damage to the Pentagon . . . may indicate a desire to inflict higher casualties on what are generally less protected civilian targets."[14] In fact, although the total volume of terrorist incidents worldwide has been declining, the percentage of terrorist incidents resulting in fatalities has grown.[15] Bruce Hoffman, RAND analyst and co-author of *Countering The New Terrorism*, attributes at least part of this rising lethality on terrorism's changing characteristics.[16] "Inflicting pain on the 'enemy' seems often to be the terrorists' goal, rather than drawing publicity to a cause."[17]

Additional factors account for this new lethality. Some terrorists may believe that ever more spectacular acts are necessary to capture public attention. The proliferation of "lethal technology" via open sources has also increased the terrorist's lethality. The loose knit nature of emerging terrorist organizations is also making terrorism harder to anticipate and terrorists harder to track, creating an environment where terrorist organizations can tolerant greater risk taking.

## REVIEW OF U.S. STRATEGY TO COMBAT TERRORISM

President G. W. Bush characterized the incidents of 9/11 as acts of war. He also stressed that the U.S., in responding to the attacks of 9/11, "will make no distinction betweenthe terrorists who committed these acts and those who harbor them."[18] In an interview with Peter Jennings of ABC News on 14 January 2002, Secretary of State Colin Powell was asked about the war on terrorism. He made the following comment: "Rather than look for a specific country to go after, we're going after terrorism. We're going to go after terrorism wherever it is located."[19]

Shortly after the attacks on 9/11, National Security Advisor Condoleezza Rice, stated:

> The President has made it clear from the outset that our campaign against terrorism will be fought across a very broad front. There is a diplomatic component, a law enforcement component, an intelligence component, a financial component and a military component as well. All of these facets, all of

them, have to operate together in a very tightly coordinated fashion. It will require close coordination among many, many government agencies.[20]

American strategy for fighting terrorism will focus on detection, preparedness, prevention, protection, response and recovery, and incident management.[21] The basic objectives of U.S. strategy are isolation of countries and groups that support terrorism; disruption of terrorist planning and operations; sharing of information [with partners throughout the world]; and the apprehension and trial of perpetrators.[22]

## FRAMEWORK

Presidential Directives issued during the Clinton administration have become the central blueprint for U.S. policy in combating terrorism. In the years since 1995, nine principles have evolved: [23]

- Make no concessions to terrorists and strike no deals.
- Bring terrorists to justice for their crimes.
- Isolate and apply pressure on states that sponsor and support terrorism to force them to change their behavior.
- Support nations that cooperate in combating terrorism.
- Address terrorism as both a crime and a national security threat.
- Protect U.S. personnel, facilities, and interests.
- Preempt threats and respond to attacks.
- Prepare now to manage and mitigate the effects of a terrorist incident.
- Focus on both state sponsors and also non-state actors in analyses and information gathering.

## ORGANIZATION

Figure 1 depicts how the Bush administration has organized for the fight against terrorism.[24] On 8 October 2001, President Bush established the Office of Homeland Security, responsible for developing and coordinating the implementation of a comprehensive national strategy to secure the U.S.

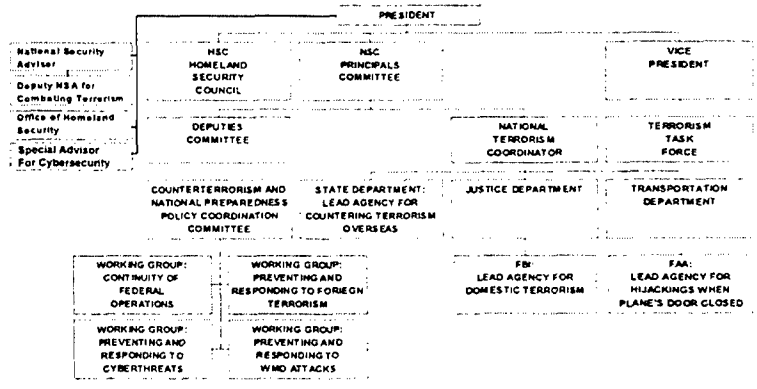


FIGURE 1. U.S. ORGANIZATION FOR COMBATING TERRORISM

from terrorist threats or attacks. "The President established the Office of Homeland Security and the Homeland Security Council to coordinate, and implement the Executive Branch's efforts to detect, prevent, protect against, respond to, and recover from terrorist attacks within the United States."[25] The Head of the Office of Homeland Security ("Assistant to the President for Homeland Security"), Thomas Ridge, will need to harmonize the activities of more than 50 federal offices and agencies, and hundreds of state, local and private organizations. The Homeland Security Council is responsible for ensuring coordination of homeland security-related activities of executive departments and agencies, and for effective development and implementation of homeland security policies.[26]

The President also designated a Deputy National Security Advisor for Combating Terrorism and selected a Special Advisor to the President for Cyberspace Security. The Deputy National Security Advisor for Combating Terrorism will be the President's principal advisor on matters related to combating global terrorism, including all efforts designed to detect, disrupt, and destroy global terrorist organizations and those who support them. He will report to the Assistant to the President for National Security Affairs, and also to the Assistant to the President for Homeland Security with respect to matters relating to global terrorism inside the United States.[27]

The President's Special Advisor for Cyberspace Security will coordinate interagency efforts to secure information systems. In the event of a disruption, the Special Advisor will coordinate efforts to restore critical systems. He will be the President's principal advisor on matters related to cyberspace security and report to the Assistant to the President for Homeland Security and to the Assistant to the President for National Security Affairs. The Special Advisor will also serve as chairman of a government-wide board that will coordinate the protection of critical information systems.[28] The advisory committee for cyber security is a public/private partnership responsible for protection of America's key infrastructures.[29]

The Vice President is currently heading a task force charged to determine how best to respond to major terrorist incidents.

## ELEMENTS OF U.S. STRATEGY TO FIGHT TERRORISM

"Available policy options range from diplomacy, international cooperation and constructive engagement to economic sanctions, covert action, physical security enhancement, and military force."[30]

### Diplomatic

The U.S. is a party or signatory to twelve international conventions and treaties relating to terror and its victims.[31] Since 9/11, the U.S. has also built an impressive worldwide coalition for the war against terrorism:[32]

- 136 countries have offered a range of military assistance.
- The U.S. has received 46 multilateral declarations of support from organizations.
- OAS and ANZUS (Australia, New Zealand and the U.S.) invoked their treaty obligations to support the United States.
- 142 countries have issued orders freezing the assets of suspected terrorists and organizations.
- 89 countries have granted over-flight authority for U.S. military aircraft.
- 76 countries have granted landing rights for U.S. military aircraft.
- 23 countries have agreed to host U.S. forces involved in offensive operations.

Additionally, NATO implemented Article V of the NATO treaty — considering the attacks on September 11th as an attack against all NATO members.[33]

**Economic**

The Secretary of State maintains a list of countries that support terrorism. Listed counties are subject to strict U.S. export controls, particularly of dual-use technology, and selling military equipment to them is prohibited. Indirect state sponsorship is addressed in a second terrorist category that prohibits the sale of arms to nations not fully cooperating with U.S. antiterrorism efforts and withholds foreign assistance to nations providing lethal military aid to countries on the list of state sponsors. Countries currently on the terrorism list are Cuba, Iran, Iraq, Libya, North Korea, and Sudan.[34]

U.S. economic sanctions fall into six general categories: restrictions on trading, technology transfer, foreign assistance, export credits and guarantees, foreign exchange and capital transactions, and economic access.[35] On 25 September 2001, President Bush signed an Executive Order freezing the assets of 27 organizations known to be affiliated with Usama bin Ladin's network and giving the Treasury's secretary board powers to impose sanctions on banks around the world that provide these organizations access to the international financial system.[36] There are now 168 such groups, entities, and individuals covered by the Executive Order.[37]

In December, the Bush Administration also ordered the freezing of assets of three organizations linked to the militant Palestinian organization Hamas. One of the groups, the 'Holy Land Foundation' is reported to be one of the largest Muslim charities in the U.S.[38] Since

9/11, the assets of at least 153 known terrorists, terrorist organizations, and terrorist financial centers have been frozen in the U.S. financial system; and more than $33 million in assets of terrorist organizations has been blocked.[39] The U.S. has also created three new organizations -- the Foreign Terrorist Asset Tracking Center (FTAT), Operation Green Quest, and the Terrorist Financing Task Force. These new organizations will help facilitate information sharing between intelligence and law enforcement agencies and encourage other countries to identify, disrupt, and defeat terrorist financing networks.[40]

Internationally, the United Nations Security Council passed resolution 1373 that requires all nations to keep their financial systems free of terrorist funds, and the G-20 (an international forum of finance ministers and central bank governors from 19 countries, the European Union and the World Bank), and International Monetary Fund (IMF) member countries have agreed to make public the list of terrorists whose assets are subject to freezing, and the amount of assets frozen.[41]

**Homeland Security**

The 2001 Quadrennial Defense Review defines Homeland Security as:

> The prevention, deterrence, and preemption of, and defense against aggression targeted at U.S. territory, sovereignty, population, and infrastructure as well as the management of the consequences of such aggression and other domestic emergencies. It includes Homeland Defense: the prevention, deterrence, preemption of, and defense against direct attacks aimed at U.S. territory, population, and infrastructure; and Civil Support: DOD support to civilian authorities for natural and manmade domestic emergencies, civil disturbances, and designated law enforcement efforts.[42]

Crisis Management and Consequence Management are generally defined as:

> Crisis management is predominantly a law enforcement function and includes measures to identify, acquire, and plan the use of resources needed to anticipate, prevent, and/or resolve a threat or act of terrorism. Consequence management is predominantly an emergency management function and includes measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism.[43]

The following primary Federal agencies will provide the core Federal response to a terrorist threat or incident within the U.S.:

- Department of Justice (DOJ) / Federal Bureau of Investigation (FBI).
- Federal Emergency Management Agency (FEMA).
- Department of Defense (DOD)
- Department of Energy (DOE)

- Environmental Protection Agency (EPA)
- Department of Health and Human Services (DHHS)

The FBI is the lead agency for crisis management and FEMA is the lead agency for consequence management for terrorist incidents occurring in the U.S.. The U.S. Agency for International Development (USAID) assists with consequence management for terrorist incidents occurring outside the U.S..

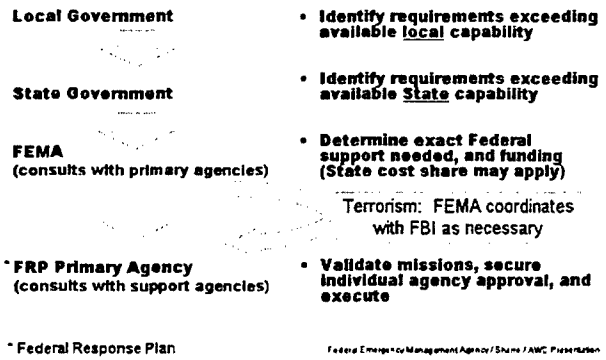


FIGURE 2. FEMA REQUEST PROCESS[44]

FEMA's organizational structure is built around four functions of mitigation, preparedness, response, and recovery. State emergency management agencies usually mimic FEMA in function. Most of the "heavy lifting in a terrorist attack falls on first responders — the local emergency services of firemen, police, ambulance crews, and emergency room crews."[45] "FEMA is charged with coordinating the federal effort only, although its role can expand if a disaster exceeds local and state capabilities and federal assistance is requested and approved."[46] One federal initiative under consideration, based on the concerns of local officials, is the National Domestic Preparedness Office. "The Office will function as an interagency forum to coordinate federal policy and program assistance for state and local emergency responders."[47]

Initiatives in addition to the new Office of Homeland Security include:[48]

- Over $20 billion has been applied to promote homeland security, including funds to upgrade intelligence and security, provide recovery assistance to disaster sites, help victims' families, and increase numbers of law enforcement personnel.
- New airline security standards that tighten background checks for airline screeners and workers, expands the federal air marshal program, creates new baggage security requirements, and tightens security in all airports.
- The FDA has enhanced the food screening process of imported foods.
- The Department of Health and Human Services created the Office of Public Health Preparedness, to coordinate the national response to public health emergencies.

**Humanitarian Aid**

U.S. foreign aid has a twofold purpose of furthering America's foreign policy interests while improving the lives of the citizens of the developing world. The strategy is that

humanitarian aid will remove openings that extremist groups might otherwise exploit. In 1961, President Kennedy signed the Foreign Assistance Act and created the U.S. Agency for International Development (USAID) by executive order. USAID receives overall foreign policy guidance from the Secretary of State and works to advance foreign policy objectives by supporting economic growth; global health; and, democracy and humanitarian assistance.

USAID works in close partnership with private voluntary organizations, indigenous organizations, universities, U.S. businesses, international agencies, other governments, and other U.S. government agencies.

**Intelligence**

The Director of Central Intelligence is charged with coordinating Intelligence Community issues and sharing information through the Counter-terrorist Center and the Interagency Intelligence Committee on Terrorism (IICT).[49] The Intelligence Community is a group of 13 government agencies and organizations that carry out the intelligence activities of the United States Government. The Director of Central Intelligence (DCI), who also leads the Central Intelligence Agency (CIA), heads the Community.[50] Resources for these organizations are tied together in the National Foreign Intelligence Program. The budget for these national activities, which support political, economic, and military decision makers, is developed by the DCI and presented to the Congress annually. Intelligence activities that are more narrowly focused and intended to support tactical military forces are funded separately in two programs within the Department of Defense. These programs — the Joint Military Intelligence Program and the Tactical Intelligence and Related Activities aggregation — fall under the Deputy Secretary of Defense.[51]

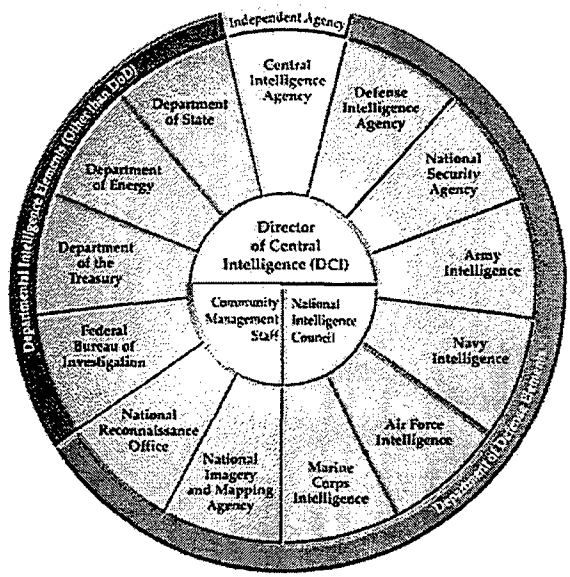


FIGURE 3. U.S. INTELLIGENCE COMMUNITY

"The future purpose of [intelligence gathering, infiltration of terrorist groups, and military operations] will be to destroy terrorist cells and facilities that may produce or store weapons of mass destruction."[52]

**Legislation and Law Enforcement**

Passed in the wake of the World Trade Center bombing in 1993 and the Oklahoma City bombing in 1995, the 1996 Antiterrorism and Effective Death Penalty Act makes it a crime to provide support to terrorist organizations and denies their members entry visas into the United States.[53] "Other major laws that can be used against countries supporting terrorism are the Export Administration Act, the Arms Export Control Act, and specific items or provisions of foreign assistance legislation."[54] Additionally, U.S. code establishes policy for military assistance to civilian authorities on a wide range of issues, from domestic disaster relief to special events.[55]

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act is part of the Congressional response to 9/11. The Act consists of ten titles which, among other things:[56]

- Give federal law enforcement and intelligence officers greater authority (at least temporarily) to gather and share evidence particularly with respect to wire and electronic communications;
- amend federal money laundering laws, particularly those involving overseas financial activities;
- create new federal crimes, increase the penalties for existing federal crimes, and adjust existing federal criminal procedure, particularly with respect to acts of terrorism;
- modify immigration law, increasing the ability of federal authorities to prevent foreign terrorists from entering the U.S., to detain foreign terrorist suspects, to deport foreign terrorists, and to mitigate the adverse immigration consequences for the foreign victims of 9/11; and
- authorize appropriations to enhance the capacity of immigration, law enforcement, and intelligence agencies to more effectively respond to the threats of terrorism.

"To date, the United States has joined with the world community in developing all of the major antiterrorism conventions, which impose on their signatories as obligation either to prosecute offenders or extradite them to permit prosecution for a host of terrorism-related crimes."[57]

**Military**

In 1999, Secretary of Defense Cohen outlined the core values guiding DOD efforts to prepare against terrorism at home:

- Military assistance in the wake of a domestic attack must be in support of the appropriate federal civilian authority (either DOJ or FEMA).

- An unequivocal chain of authority and accountability for that support must exist.
- Military assistance should not come at the expense of the primary mission — fighting and winning our nation's wars.
- Military response efforts will be grounded primarily in the National Guard and Reserve.
- We will not trample on American lives and liberties in the name of preserving them.

DOD's role in combating terrorism at home is part of a coordinated U.S. government interagency team response. No single agency possesses the authorities, response mechanisms and capabilities to effectively deter or resolve terrorist incidents. The DOD, as authorized by law, plays a supporting role in assisting lead federal agencies in their response to terrorist incidents. Department of State is the lead agency for coordination of counter-terrorism policy and operations abroad. Department of Justice, through the FBI, is the lead agency for countering terrorism in the U.S..[59] "Domestically, DOD supports the law enforcement efforts of the DOJ, including the FBI, and the Federal Emergency Management Agency (FEMA) for consequence management."[60]

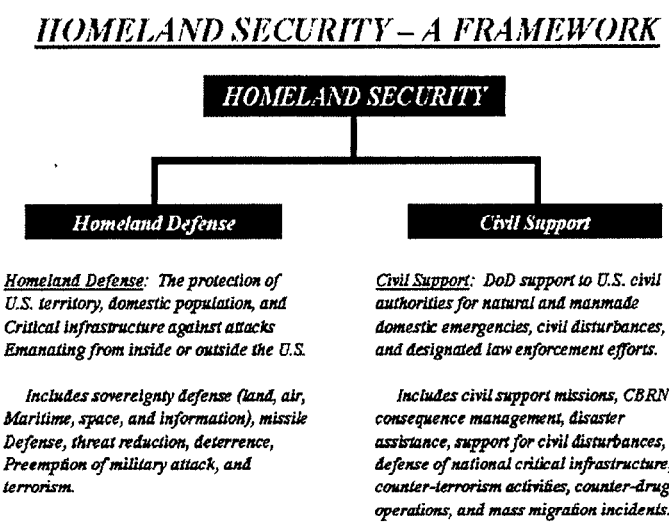


FIGURE 4. MILITARY ROLE IN HOMELAND SECURITY [58]

DOD assistance includes threat assessment; Domestic Emergency Support Team participation and transportation; technical advice; operational support; tactical support; support for civil disturbances; custody, transportation and disposal of a WMD device; and other capabilities including mitigation of the consequences of a release.[61] DOD has many unique capabilities for dealing with a WMD and combating terrorism, such as the U.S. Army Medical Research Institute for Infectious Diseases, Technical Escort Unit, and U.S. Marine Corps Chemical Biological Incident Response Force. These and other DOD assets may be used in responding to a terrorist incident if requested by the Lead Federal Agency (LFA) and approved by the Secretary of Defense.[62] DOD also provides Rapid Response Teams to provide essential support for state and local first responders early in a crisis. Ten rapid response teams have been created and are located in each of the ten FEMA regions.

**Special Programs**

Additional administration programs aimed specifically at combating terrorism include:[63]

- Antiterrorism Assistance Program. This program provides training and equipment to foreign countries working to improve their antiterrorism capability.
- Assistance to victims programs designed to compensate victims of terrorism.
- Counter-terrorism Research and Development Program. Jointly funded by the Departments of State and Defense, this program supports research and development of technology to counter increasingly sophisticated equipment used by terrorists.
- Diplomatic Security Program. This program funds construction of hardened facilities, physical security, and counter-intelligence abroad.
- The Rewards for Justice Program. Under the 1984 Act to Combat International Terrorism, the State Department offers rewards of up to $5 million to anyone providing information that would prevent or resolve an act of international terrorism against U.S. citizens or property, or that leads to the arrest or conviction of terrorists. The USA Patriot Act authorizes rewards greater than $5 million, if it is determined that a greater amount is necessary to combat terrorism or defend the U.S. against such acts.

## ASSESSMENT OF U.S. STRATEGY TO COMBAT TERRORISM

The challenge our government faces is to establish executable links that cut across mission areas and agencies:

### ORGANIZATION TO COMBAT TERRORISM

One of the biggest challenges facing the current administration will be the coordination of antiterrorism efforts. "Unlike the concept of jointness of command built into the U.S. national military establishment, the civilian side of the U.S. government functions more as a hierarchy of committees."[64] Even in the White House, the President has divided leadership and coordination responsibilities for combating terrorism between the NSA and the OHS, with various advisors that report either directly to the President, Vice-President, specific cabinet members, or a combination thereof. Efficiency of government may breakdown when stressed by issues that are interdisciplinary and intertwined.[65] Figure 5 represents the "situation" Governor Ridge will have to grapple with.

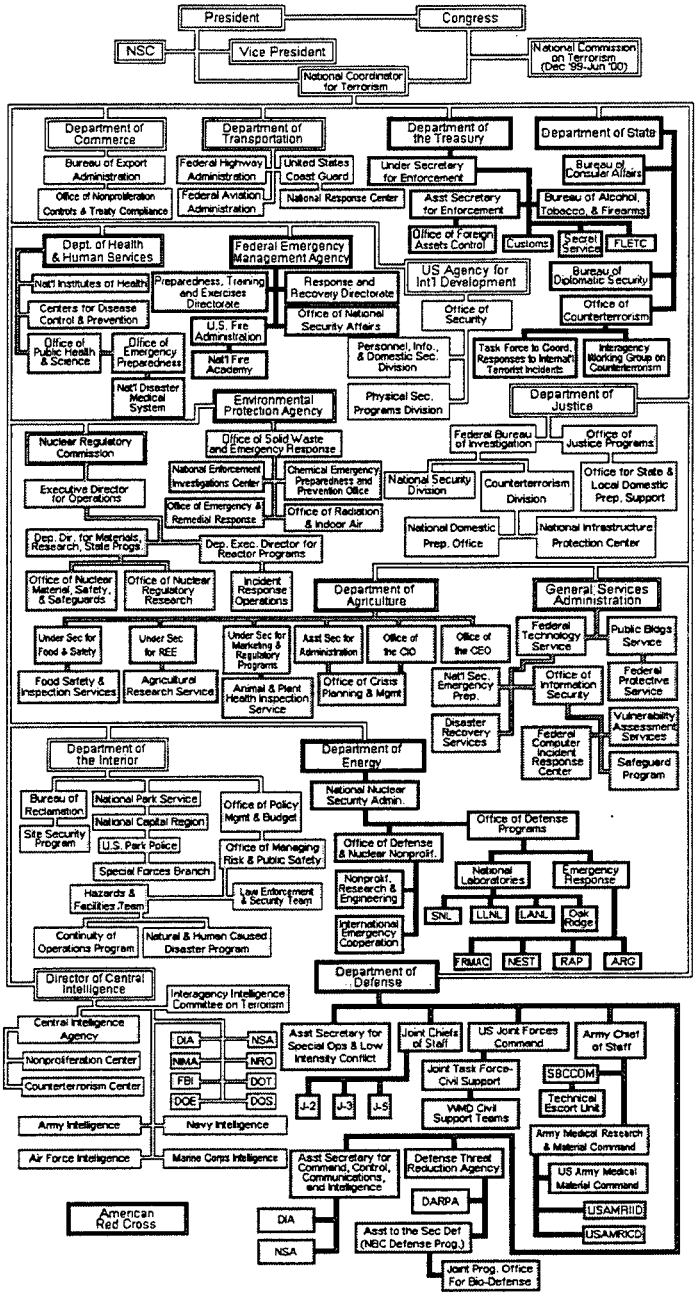


FIGURE 5. ORGANIZATIONAL CHART FOR FIGHTING TERRORISM[66]

## ELEMENTS OF U.S. STRATEGY TO FIGHT TERRORISM

### Diplomatic

Many in the United States were shocked and horrified by the images of Palestinians rejoicing over the news of the 9/11 attacks. Equaly hard to fathom was the lack of unanimous and unqualified condemnation of these events on the international scene.[67] The antipathy and

ambivalence expressed by some towards the U.S. lends moral support to those whose hatred of America drives them to commit violence against us — "one person's terrorist is another's freedom fighter." Various roots seem to fuel anti-American sentiment: political-economic, historical, religious cultural, and/or psychological. *Global Trends 2015* predicts most anti-U.S. terrorism in the future will be based on perceived ethnic, religious or cultural grievances.[68]

The global economy — globalization — is being driven by rapid and almost unrestricted flows of information, ideas, cultural values, capital, goods and services, and people; but its reach and benefits will not be universal. "Terrorism shows the dark side [of globalization]."[69] America's extensive commercial reach exports our views and realities that citizens of other countries find offensive, "stoking anxiety and anger about cultural invasion."[70] The prosperity of the west, particularly the U.S., while people in most developing countries and economies struggle to maintain meager standards of living leads to intense frustration and psychological anti-Americanism. This hatred is fueled by what we are vice what we do. "Regions, countries, and groups feeling left behind will face deepening economic stagnation, political instability, and cultural alienation. They will foster political, ethnic, ideological, and religious extremism."[71]

Dr. Steven Metz of the U.S. Army War College suggests western notions of civil rights, personal liberties, and civil-military relationships may not be culturally compatible in non-western societies.[72] Charismatic leaders (particularly those in the Islamic culture (who are neither representative of Islam nor approved by Islam) exploit the challenges to Islamic fundamentalism posed by the secular and materialistic culture of the west in their appeal to recruited followers. From North Africa to the Philippines, there are over populated and economically stressed societies that have yet to come to terms with modernity.[73]

As perception of U.S. hegemony grows, so will resistance to U.S. economic, political, and cultural influence. "Political-economic anti-Americanism represents reaction to current U.S. foreign policies."[74] Examples include our support for Israel, our continued embargo on Iraq, and our international economic policies. Historical anti-Americanism stems from past U.S. behavior, such as our support of military coups in South America during the 70's and perceived exploitation of poor nations by the rich nations. Militant Islamists and fundamentalists, who view the U.S. as the great Satan and morally corrupt, most vocally express religious anti-Americanism.

**Economic**

"In the past, use of economic sanctions was usually predicated upon identification of a nation as an active supporter or sponsor of international terrorism."[75] However, "sanctions

usually require the cooperation of other countries to make them effective, and such cooperation is not always forthcoming."[76] Three of the countries on the State Department terrorism list (Iraq, Iran, and Libya) supplied 11% of the world's oil needs in 1999, 35% of Europe's oil imports, and 10.8% of Japan's oil imports, which complicates universal acceptance for U.S. led sanctions.[77] Numerous countries, with which the U.S. has strategic relationships, also sell dual-use technology to terrorist list countries — complicating efforts to gain international cooperation for U.S. led sanctions.[78]

"Critics of the State Department [States Supporting Terrorism] list argue it has become too politicized and that nations are retained on the list as Cold War carryovers or for other grounds not directly related to active state support of terrorism, such as religious persecution, drug trafficking, counterfeiting, or other criminal activity."[79] However, removing a country from the list may result in confrontation with Congress based on a past history of terrorism support. Historically, the trend seems to be "to maintain the status quo, or add to the list, but not to delete from it."[80] "A desire to punish a state for supporting international terrorism may also be subject to conflicting foreign policy objectives."[81]

**Homeland Security**

"Local agencies range from volunteer and part-time coordinators with few resources and little authority to large, highly professional organizations with state-or-the-art information technology and staffs with extensive training and experience."[82] In addition to the local, state, and federal emergency management and disaster response agencies, an increasingly broad network for other public, nonprofit, and for-profit organizations are involved in the national emergency management system. Coordinating the activities of volunteer and other nonprofit, and for-profit organizations and individuals, and government agencies is complex and difficult.

Without a uniform command and control protocol in place, local first responders are concerned about potential problems if the federal government tries to take over a state and/or local response already in progress.[83] The concerns over ambiguity are "exacerbated by the separation of crisis management and consequence management."[84] In most terrorist response situations, its probable that crisis and consequence activities will take place concurrently. Command and control issues will be complicated if half the response (crisis management) is led by the federal government, and half of the response (consequence management) is led by the state or local government.[85]

Perhaps the most serious danger emanating from the 9/11 attacks may have been the exposure of "the soft underbelly of globalization."[86] Global integration is only sustainable if we

improve the systems designed to facilitate legitimate cross-border movements while stopping illegitimate and dangerous ones.[87]

The INS has only about 5,000 inspectors to process more than five hundred million inspections at our port of entries every year, and only about 2,000 investigators and intelligence agents available to keep track of more than 30 million foreign people in the U.S.[89]. Congress has focused most of its attention on the thousands of illegal migrants who annually cross the 2,000-mile border with Mexico, where most INS agents are posted. Only 334 agents are assigned to patrol the 4,000-mile border with Canada.[90] The Customs Service, which is responsible for inspecting all goods entering the country, inspects fewer than 2 percent of the 340,000 vehicles and 58,000 cargo shipments that cross the country's borders or are unloaded in U.S. ports every day.[91]

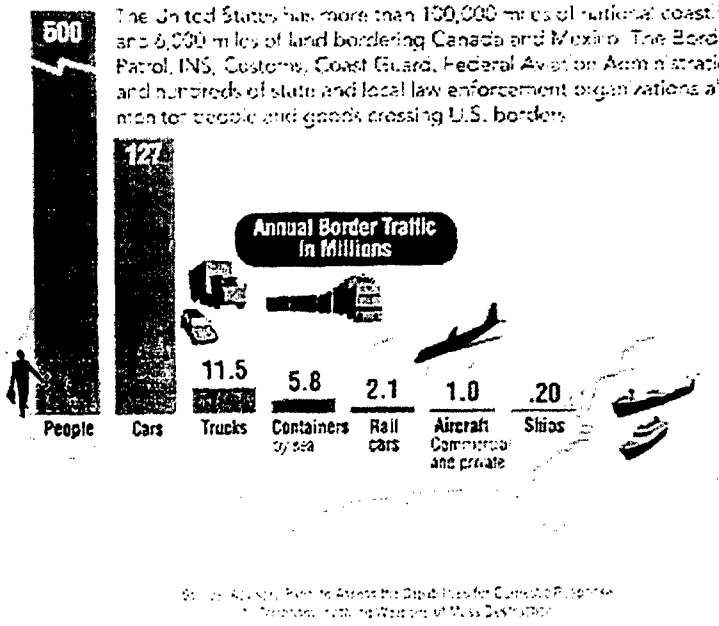


FIGURE 6. ANNUAL U.S. BORDER TRAFFIC [88]

Much of the information processed by the INS is done by hand, on old technology platforms, and with independent systems that do not share common databases. Entry and exit data is provided to the INS in paper form, which must be transferred by hand into an electronic database — a process that takes weeks and months to accomplish and prevents access to data in real time. To help inspectors identify persons who are inadmissible to the U.S., databases maintained by the INS, Customs Service and the State Department's Bureau of Consular Affairs have been made available in a shared database program called the Interagency Border Inspection System (IBIS). Unfortunately, officers (through IBIS) can only access criminal history data from the National Crime Information Center (NCIC) to check for wanted persons at only two ports of entry.[92]

**Intelligence**

To understand the perceived failure of U.S. intelligence with respect to the terrorist acts of 9/11, it is important to first understand the constraints the intelligence community operates under. The framework under which the intelligence community was created envisioned enemies to be nation-states and was designed to provide for protection of citizen's rights. This resulted in the creation of "organizations and authority based on distinctions of domestic versus foreign threats, law enforcement versus national security concerns, and peacetime versus wartime."[93] The FBI is primarily responsible for law enforcement and domestic issues, and the CIA (together with the NSA, DIA, and other intelligence agencies) is responsible for foreign threats and national security concerns. "Law enforcement's focus is to collect evidence *after* a crime is committed in order to support prosecution... the CIA collects and analyzes information in order to forewarn the government *before* an act occurs."[94] Two former CIA officials believe this contradictory focus creates an inherent reluctance to share information between intelligence agencies. Those focused on law enforcement need to protect their information for fear of compromising future court action, and those focused on forewarning the government protect their information for fear of revealing their sources and methods in court. To address this apparent fragmented approach to intelligence gathering and sharing, these officials reason that intelligence reform will revolve around the question of how to establish a "proper balance between national security and law enforcement goals."[95]

This fragmentation also impairs covert action. "Current law requires both a presidential finding and reporting to Congress of all CIA covert action. No such rule governs covert military operations."[96] Joint operations between the CIA and military special operations units could be slowed or hampered due to the differing approval and reporting requirements of these organizations.

Secondly, it is important to understand the different kind of threat we are facing. Jeffrey White, of the Defense Intelligence Agency, uses the term "irregular warfare" to capture the concepts of non-traditional threats.[98] Robert Steele, author of *On Intelligence: Spies and Secrecy in an Open World,* predicts four future threat types: "high tech brutes fighting conventional wars, low tech brutes engaged in low intensity conflict, high tech seers focused on information warfare, and low tech seers engaged in

| Contrasting Dimensions of War | |
|---|---|
| **Modern** | **Irregular** |
| Organized | Informal |
| Advanced technology | At-hand technology |
| Logistics-dependent | Logistics-independent |
| National direction | Local direction |
| Coherent doctrine | Ad hoc doctrine |
| Decisive battle | Raids and skirmishes |
| Soldier | Warrior |
| Allies | Accomplices |
| Segregation | Integration |

FIGURE 7. ASYMMETRIES BETWEEN CONVENTIONAL WARFARE AND TERRORISM [97]

jihad."[99] Equally focused opponents will not necessarily engage in conflicts. U.S. adversaries will increasingly apply asymmetric strategies and tactics in attempts to counter and avoid our strengths.[100] In an essay on problems of warfare in the 20th century, Mr. White makes an argument that practitioners of irregular warfare remain "confoundingly unaffected by changes in technology", and "sociology, psychology, and history will have more to say about the nature of the conflict, including its persistence and intensity."[101] The operational environment of the irregular warrior includes geography, ecology, history, ethnicity, religion, and politics. The Intelligence Community has historically focused on analysis of forces similar to us. However, "'the gray zones' . . . where there is no real representation of democratic countries or international agencies, turns these regions into a kind of intelligence vacuum, where terrorist organizations can find a safe-haven and a basis for future activity."[102] Dissimilar foes, — the irregular warriors, or terrorists — need to be looked at with equal skill. The kinds of data our high-tech intelligence gathering systems provide against modern conventional adversaries may be much harder to collect against loosely organized and more socially integrated terrorist organizations.

**Legislation**

The 1996 Anti-terrorism and Effective Death Penalty Act (AEDPA) illustrates a dilemma of fighting terrorism in a constitutional democracy. Inappropriately balancing counter-terrorism legislation and the rights of citizens that legislation aims to protect will equate to "cooperation" with the terrorist — by deteriorating our freedom.[103] Passed in the wake of the 1993 WTC bombing and the Oklahoma bombing, critics view the bulk of its counter-terrorism titles as unconstitutional — citing problems with the suspension of due process, limits on habeas corpus, and a restriction on First Amendment activities.

Under the AEDPA, it is illegal to provide material support to a group designated a terrorist organization and also makes it a crime to provide support for the non-violent/non-criminal acts of terrorist organizations. Critics also argue that had this law been in effect earlier, it would have been illegal to provide aid and funds to Nelson Mandela and the African National Congress, designated a terrorist organization in the 1980s.

Critics most vehemently disagree with the provisions of the AEDPA Title IV. Arguments against this provision center mostly around its liberal rules for deportation of aliens based on classified evidence (that defense attorneys are prohibited from seeing) and the exclusion of individuals based on ideological beliefs and association with terrorist organizations. Essentially, opponents of the AEDPA argue it is "blatantly unfair and in violation of the habeas corpus

tradition of face your accusers and the right to a fair hearing to require aliens to defend against evidence they cannot see and sit in jail until they can [defend themselves]."[104]

**Military Force**

"Although not without difficulties, military force, particularly when wielded by a superpower such as the United States, can carry substantial clout."[105] The U.S. decisive edge in both information technology and weapons development ensures its strong position as a dominant military power. So much so, that potential adversaries are forced to pursue asymmetric capabilities against U.S. forces and interests —abroad and at home. It is hard to envision U.S. opponents seeking direct conflict with the U.S. on its terms.[106]

"The United States so outstrips its allies that technology actually inhibits effective military cooperation with allies and friends, exposing the U.S. to more strident global criticism and leading to an increasingly unhealthy division of labor."[107] The driving force behind this disparity is the superiority of U.S. air power — in numbers of aircraft and in capabilities. "Only the U.S. possesses sizable airlift and tanker fleets and stealth aircraft. Additionally, no one possesses the number and sophistication of U.S. satellites, and only the U.S. has the secure command and control network to manage these air and space assets in near real-time."[108] These inequalities are making joint operations and exercises between the U.S., its allies, and coalition partners increasingly difficult to manage. "When working effectively, efficiently, and safely with allied air arms becomes too hard, the U.S. will be tempted to go it alone."[109]

As the U.S. shoulders greater responsibility as a force provider, allies and friends may become less inclined to invest in advanced technologies that would give the U.S. more of an incentive to include them in military planning. Ironically, our increasingly dominant role in the air campaign stems from a technological ability driven by a shared desire by all allied and coalition partners to wage relatively bloodless war. Yet, there are significant potential political costs for the U.S. as we are increasingly perceived to be the only nation doing the shooting.

In addition to the increased risk of alienating world opinion, other drawbacks to the use of military force against terrorism include possible casualties to innocents and friendly forces, the creation of terrorist "martyrs", and increased asymmetrical warfare. The asymmetrical challenges we face from terrorist organizations stem at least partly from that fact that terrorist groups lack the ability to confront us in direct combat. These risks lead many to believe it would be a mistake to combat terrorism through military means alone. One proponent of this view argues "terrorism is not fundamentally a military problem; it is a political, social and economic problem."[110] Hence, the "military . . . is not suitably structured, trained or equipped to defeat

terrorism. . . . The military may be able to contribute to the fight against terrorism, but it should not lead the way." [111]

**Special Programs**

U.S. spending on development aid has fallen significantly over time and is quite low now compared with levels relative to what other industrialized nations provide. The U.S. devotes resources equal to only 0.1 percent of the U.S. economy to development aid (discounting the aid earmarked for just Afghanistan). This represents the smallest share of national resources devoted to development aid in the post-World War II era. Compared to the 1980s, the share of the economy dedicated to development aid has fallen by half.[113]

| | 1980s Average | In 2002 under Administration's Budget | Comment on 2002 Figures |
|---|---|---|---|
| Inflation-adjusted level (in 2002 dollars) | $13.4 billion | $10.9 billion | Significantly below historic average |
| As a share of the economy | 0.20% | 0.10% | Post-World War II low |
| As a share of the budget | 0.92% | 0.56% | Post-World War II low |

FIGURE 8. U.S. SPENDING ON DEVELOPMENT AND HUMANITARIAN AID [112]

**Technology**

The worldwide availability of potentially harmful information and technology is increasingly elevating the national security dimension of terrorism.[114] Most experts agree that the U.S. will maintain a global advantage in the field of information technology (IT) over the foreseeable future. However, as rich nations take advantage of the rapid advances in IT, older technologies will become more affordable and shift into new markets . This will benefit U.S. allies, but will also benefit adversaries interested in acquiring early generation technology capable of being used for WMD. [115] The National Intelligence Council's report on global trends submits that terrorists will take advantage of IT to become more integrated.[116] Thomas Homer-Dixon, director of the Center for the Study of Peace and Conflict at the University of Toronto, suggests the attacks of 9/11 illustrate "the rise of complex terrorism."[117] He believes:

> Modern societies face a cruel paradox: Fast paced technological and economic innovations may deliver unrivalled prosperity, but they also render rich nations vulnerable to crippling, unanticipated attacks. By relying on intricate networks and concentrating vital assets in small geographic clusters, advanced Western nations only amplify the destructive power of terrorists — and the psychological and financial damage they can inflict.[118]

Essentially, the growing technological capacity of small groups coupled with our increasing reliance on high-tech in social economic systems facilitates the potential for violence on a mass

scale — complex terrorism. The U.S. now depends upon a complex, interdependent network of critical infrastructure systems that are essential to our national and economic security. These networks include information systems in the government, telecommunications, banking and finance, transportation, energy, manufacturing, water, health and emergency services networks. Most of this infrastucture "lies unprotected or is equiped with security sufficient to deter only amateur vandals, thieves, or hackers."[119]

The growing technological capacity (i.e. destructive capacity) of small groups results from advances in weapons and communications technology, and increased opportunities to "divert non-weapon technologies to destructive ends."[120] The global economy is bringing with it open borders and the enhanced movement of goods, people, and services — enabling the ability of terrorist organizations to operate in an unregulated environment.[121] Improved and readily available light weapons make it easier for fewer people to kill more people, advanced communication technologies allow organizations to coordinate activities and share encrypted information on a global scale, and modern society provides a host of inviting targets in the form of concentrated energy sources, combustibles, and poisons.

Vulnerabilities in our society's complex and interconnected networks (i.e. energy and information grids, transportation systems, water processing and food production, and healthcare) add to our risk of catastrophic terrorism. Critical information and communication infrastructures are targets for terrorists because of the broad economic and operational consequences a shutdown can inflict. Consider the economic disruption caused on 9/11:[122]

- Financial markets were shut down for over a week as companies struggled to restore communications and recover important IT assets;
- Trading was halted on principal stock exchanges for nearly a week;
- Telecommunications networks in and around New York City were so congested that first responders were unable to use cellular services;
- Widespread uncertainty that communications systems would be unavailable;
- Insurance sector's resources have been severely strained, raising concerns about their ability to provide sufficient levels of protection for cyber-based attacks in the future.

These systems are becoming more tightly coupled, increasing the possibility that a disruption in one node will affect others throughout the system — potentially in a non-linear fashion where a small shock produces a disproportionately large disruption.[123] Terrorists need only be clever enough to identify and exploit these weaknesses, and then attack the right nodes

in the right networks at the right time. An obvious example is the terrorist use of box cutters as "keys to convert a high-tech means of transport into a high-tech weapon of mass destruction."[124] The less redundancy built into a system, the greater its vulnerability to catastrophic attack. An accident in a railway tunnel in Baltimore during the summer of 2001 tied up rail transportation for weeks because the resulting fire was so difficult to defeat and the tunnel represented a non-redundant link in the east coast rail system. What lesson might have been drawn by an observant terrorist organization?

Terrorists are also exploiting computer and communication networks to organize themselves into new, less hierarchical networks — sponsored by secret, private backers. Enabled by the information revolution, this recent phenomena makes detecting, preventing, and responding to terrorist activity more difficult than ever before.[125] Studies of terrorist organizations in the Middle East also suggest that the most active and lethal groups make extensive use of information techniques.[126]

In a discussion of networks, net-war, and information age terrorism, researchers John Arquilla, David Ronfeldt, and Michele Zanini reason future terrorism may increasingly feature information disruption rather than physical destruction.[127] They found that many terrorist entities are moving from hierarchical toward information-age network designs. "In the future, as the information age brings the further empowerment of non-state and transnational actors, 'stateless' versions of the terrorist war may spread."[128] Terrorists will continue using advanced information technology to support these organizational structures. More effort will go into building arrays of transnational inter-netted groups than stand-alone organizations, and this is likely to make terrorism harder to fight.

The use of a WMD technology by terrorists may be the threat for which the U.S. is least prepared. Information on nuclear, chemical, and biological weapons is readily available on the Internet and how-to guides. There is increasing evidence of illegal trafficking in nuclear materials. In addition, a number of countries hostile to the U.S. are known to be developing WMD capabilities, and some of them are known to support terrorist groups.[129]

**RECOMMENDATIONS**

"Most experts agree that the most effective way to fight terrorism is to gather as much intelligence as possible; disrupt terrorist plans and organizations before they act; and organize multinational cooperation against terrorists and countries that support them."[130] While speaking at the U.S. Army War College shortly after the attacks on 9/11, General Sir Rupert Smith

outlined four important reasons for states to pursue operations (including those against terrorism) in a multi-national coalition:[131]

- Individual states may not have the resources to act alone.
- Member nations gain moral, political, material and geographical support.
- Risk is spread.
- Being an ally gains a share in the "reward" of achieving the objective.

Ultimately, reducing terrorism rests on our commitment to improved organization and diplomatic / intelligence efforts as a first line of defense, prevention of attacks through deterrence or interdiction, WMD defense, and consequence management of terrorist attacks whenever and wherever they happen.

ORGANIZATION

Six countries studied by the Congressional Research Service (Canada, France, Germany, India, Israel, and the U.K.) share common structural elements in their approach to terrorism. These include: [132]

- Centralization of decision making with coordinating mechanisms.
- Guidelines for clear designation of agency in charge during a terrorist incident.
- Strategies with a strong intelligence component.
- Executive branch oversight mechanisms.

In crafting an organization to fight terrorism, the administration appears to have blended elements of these common structural elements with some of the elements of the U.S. "Drug Czar" concept. Under the current structure, the Assistant to the President for Homeland Security (APHS) is not specifically in charge of all elements of the U.S. strategy to combat terrorism, he is a coordinator. Like the Head of the Office of National Drug Control Policy (Drug Czar), the APHS acts as a coordinator in the Executive Office to merge international and domestic responsibilities in bringing together the law enforcement, intelligence, foreign policy/national policy, and domestic first responder communities. Like the Drug Czar, the APHS also has no budget authority. He exercises budget review authority, which ideally wields considerable clout in terms of policy input and integration. However, this will only hold true as long as the occupant of the office is "a strong personality with strong backing from the President . . . changes in leadership could significantly impair or enhance the effectiveness of a national leadership effort."[133] "What is now needed is a comprehensive effort to knot together . . . the

formidable array of capabilities and instruments that the U.S. can bring to bear in the struggle against terrorism."[134]

The APHS should have stronger budgetary authority. Retired Army Gen. Barry McCaffrey (drug czar under President Clinton) agrees: ". . . he will need a substantial, capable staff, and the authority to approve the budgets of all agency counter-terrorism programs . . . if he ends up with a small staff and a secretary and simply generates ideas, he will be nothing but a speakers' bureau on terrorism."[135] This would entail an expansion of responsibility and consolidation of power in one decision-making body responsible for coordinating all mechanisms to be employed in the fight against terrorism, but could ensure coordination and consistency in inter-agency efforts against terrorism.[136]

A CRS Report for Congress, "Homeland Security: The Presidential Coordination Office", reviews the Office of Homeland Security and suggests its success may be guided by the experience of the Office of War Mobilization (OWM) created in 1943. A participant-observer who served on the OWM staff attributed its success to seven guiding principles:[137]

- Institutional status in the President's Office recognized by statutory law;
- Jurisdiction over all agencies;
- Restriction to top policy and program issues;
- Non-involvement in normal function of individual departments;
- Maintenance of reasonable control — director had authority to resolve conflicts;
- Experience and public respect of the program coordinator; and
- Small high-level staff.

There are some obvious implications for the Homeland Security Office. First, the OHS is not a permanent institution because it was created by presidential directive. Institutionalizing the office "could reduce congressional reluctance to appropriate funds to an agency subject to having its mission, responsibilities, and administration readily modified by presidential order."[138]

Secondly, the executive order is not specific. Therefore, the jurisdiction of the OHS is not clearly understood and its authority over other agencies is uncertain. The executive order also created a 10 member Homeland Defense Council, to be chaired by the President (the DOHS is a member). Unfortunately, the relationship between the functions of the OHS and the HSC are unclear. Similarly, so is the relationship between OHS and the national director for combating terrorism on the staff of the NSC.

ELEMENTS

**Diplomatic**

The economies of most terrorist producing states (Sub-Saharan Africa, the Middle East and some in Latin America) are failing to respond effectively to the effects of globalization. These are regions where modernizing governments are threatened by a traditionalist backlash, characterized by confrontation between the secular material values of the west and theistic, land-based, and traditional culture.[139] Future U.S. policy and strategy must promote five factors to ensure the widest possible spread of economic growth:[140]

- Increase political pressure for higher living standards.
- Exercise political and economic clout to force improved macroeconomic policies.
- Continue trade liberalization policies to promote international trade and investment.
- Promote expansion of the IT revolution through promotion of education, infrastructure development, and standardization.

The U.S. should also integrate the goal of combating anti-Americanism as an important element of its foreign policies. "Recognizing the various types of anti-Americanism is an essential first step in combating them."[141] Anti-Americanism is not a necessary by-product of our status as a super power, and the stemming of negative world opinion should be "in the mind-set of the State Department, Pentagon, Intelligence Community, and Congress."[142] Cultivating positive world opinion of the U.S. is ultimately less costly, and less painful, thenthe ill will generated by actions that generate anti-American sentiment. "In the long term, and as a core objective, the U.S. should strike at the social, economic, and political roots of terrorism by coordinating global economic and political reforms, intensifying diplomatic initiative, and remaining prepared for military engagements."[143]

Regarding reforms to the State Department's terrorism list, "a strategy might be to 'focus' the current list."[144] One option may be to consider splitting the list into two —"an active supporters list and a list of dormant states that have approved of terrorism in the past and still could be doing more to stop it," subject to modified sanctions.[145] Another approach would be for Congress to codify a "portfolio of sanctions" that could be used selectively by the Administration in a graduated fashion dictated by the level of support that nation renders to terrorist activity.[146]

**Homeland Security**

Several improvements are warranted in intergovernmental relations between federal, state and local governments. Except in cases where a terrorist attack occurred on a federal property, local first responders would be initially in charge. If the federal government tries to take over a state and/or local response already in progress, there needs to be a uniform command and control protocol.[147]

Additionally, regular conduct of intergovernmental exercises can work to clarify command and control issues by:[148]

- Familiarization between agencies and their personnel.
- Increasing skill/confidence of responders
- Creation of lessons learned
- Validating procedures
- Testing capabilities

The U.S. Government Accounting Office has reviewed the programs of various federal agencies and recommends the government adopt a "risk management approach."[150] Essentially, the Risk Management Approach would require each agency to first conduct a threat assessment to evaluate the likelihood of terrorist activity against a given asset. Next, a vulnerability assessment would be conducted to identify weaknesses in areas that may be exploited by terrorists, potentially suggesting ways to eliminate or mitigate those weaknesses. Finally, a criticality assessment would be conducted to prioritize "important assets and infrastructure in term of their importance to national security, economic activity, and public safety."[151] After the assessment process is completed, better decisions can be made with respect to key actions necessary to better prepare against potential threats. "Without a risk management approach, there is little assurance that programs to combat terrorism are prioritized and properly focused."[152]

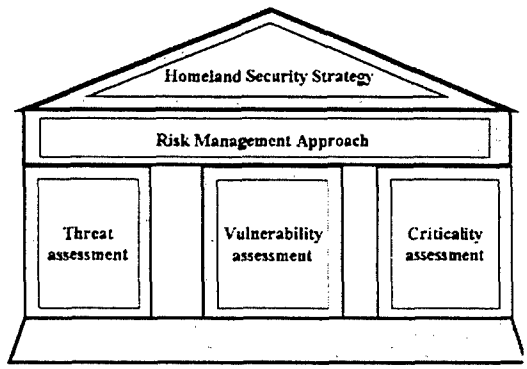


FIGURE 9. RISK MANAGEMENT APPROACH TO HOMELAND SECURITY[149]

With respect to U.S. borders, measures that are required to improve security fall into five general categories: border patrol, inspections, info-technology, personnel, and policy.[153] The ratio of border inspections performed per year to the number of available inspectors is staggering. The security measures enacted after 9/11 increased inspection requirements without increasing the number of inspectors. Funding needs to be provided for more Border Patrol agents and Port Inspectors, and upgraded equipment and technology available for their use. Types of emerging technologies that could be incorporated in the war on terrorism include:[154]

- Face recognition technology at airports;
- Digital finger printing and hand recognition;
- Electron beam irradiation of mail and luggage;

- Advanced air filtration systems in public buildings and institutions; and
- Explosives detection at airports and public buildings.

To assist in preventing known or suspected terrorists, criminals, and inadmissible passengers from boarding transportation bound for the U.S., carriers need to be required to submit advance passenger information to the INS— who should make this information available real-time to law enforcement agencies. Such a measure would "enhance the ability to identify potential threats prior to departure from or arrival in the U.S., as well as to prevent the departure of individuals who may have committed crimes while in the U.S."[155] Additionally, the U.S. needs to improve the infrastructure and integration of all law enforcement data systems, including making available the National Crime Information Center Interstate Identification Index at all ports of entry. This will ensure data from all sources on aliens is accessible to all appropriate agents and agencies in real-time.[156]

Concurrently, U.S. visa requirements need to be evaluated to ensure proper passport policies are in place. An initiative under consideration by the INS that needs to be implemented is the elimination of the Transit Without Visa Program (TWOV) to prevent inadmissible international passengers from entering the U.S. INS is implementing an improved student visa program (Student Exchange Information Visitor System — SEVIS), but needs to also review and revise the process by which foreign students gain admission to the U.S.

**Intelligence**

Operationally, there appears to be a redefinition of the battlefield: from one that has been defined in terms of space, to one that is defined in terms of people. As General Sir Rupert Smith put it, "[in the past, war was] fought on an open battlefield [by identifiable armies], the trend is to conduct war and conflict among the people."[157] As terrorist organizations become less centralized and more diffuse, the terrorist will depend more and more upon the general population for protection and concealment. This trend demands the use of greater and greater "precision" against our adversaries — with highly accurate weaponry. As much as possible, we have to hit only the enemy when we strike in order to sustain popular support for our efforts by our own population and reduce damage to the people among which our enemies operate. The need for greater precision creates a greater need for intelligence.

By strengthening our intelligence efforts and improving the quality of shared information, we may also improve our ability to determine the intentions of terrorist organizations.[158] Intelligence is important not only to prevent terrorist attacks but can also aid in understanding how the terrorist organizations work and how their decision making processes can be affected.

In so doing, we will move closer towards removing the terrorist's ability to operate easily among the people. By keeping terrorists on the move and increasing their need and frequency of communication, they will become increasingly vulnerable to counter-attack.

Institutionally, the efforts of the different elements of the U.S. Intelligence Community are often fragmented and cross-focused. The Director of Central Intelligence (DCI), who also serves as head of the CIA, leads the community. "His position should be 'separated from the position of head of CIA [just as the secretary of defense sits above the individual services], and given budgetary, planning, and management authority over the agencies that are responsible for national-level intelligence."[159]

The CIA and FBI maintain separate counter-terrorism centers, which help to perpetuate a fragmented approach to counter-terrorism by the U.S. intelligence community. A single National Counter-Terrorism Center that plans intelligence collection for all agencies and produces analysis derived from all sources of intelligence should be created under the management of the Director of Central Intelligence. Additionally, each major U.S. intelligence agency maintains separate agreements with foreign counterpart organizations to obtain information. These efforts should be coordinated under a DCI with authority and responsibility to plan, monitor, and approve such arrangements — the goal being eliminated duplication of effort and streamlined collection, synthesis, and dissemination of information.

The law requiring presidential finding and reporting to congress of all CIA covert action should be changed to eliminate the artificial distinctions between military and CIA covert actions. "In the fight against terrorists, the CIA and the military will be called to conduct joint covert operations."[160] As the distinction between military special operations and CIA-sponsored covert actions diminishes, we should consider the establishment of a permanent planning staff responsible for counter-terrorism covert action. Membership would include all appropriate intelligence agencies, headed by one department. Former DCI, John Deutch, suggests secretary of defense ownership of such a staff.[161]

Understanding the conflict against terrorism "requires a deep appreciation of the society in which it occurs."[162] The national intelligence gathering systems are still need to face conventional threats, and will be of value against terrorism, but what is required to gather important information is human intelligence (HUMINT). Counter-terrorism expertise, cultural knowledge, and language aptitudes of HUMINT officers — attachés, embassy officials and HUMINT collectors sensitive to the local operational environment and adept at interpreting terrorist agendas and ideological programs — should be improved.[163]

**Military**

"Not only does bombing solo reinforce America's image as a hegemonic bully in places like Pakistan and Iran, but it undermines support in countries that back U.S. goals."[164] If going it alone is not the answer, neither is holding back technological development and implementation in our armed forces — waiting for our allies (and potential adversaries) to catch up. America's friends and allies need to invest in the technology to modernize their military forces. The U.S. cannot force the issue, but can provide incentives for modernization by making U.S. technology easier to acquire through loosened export controls and lend/lease programs. Additionally, we can reduce the increasing worldwide perception of American hegemony and the resulting backlash of wavering allied support if we "sacrifice some control and decision making dominance to our allies, trading a degree of military efficiency for political inclusion."[165] Admittedly, this type of policy will only be as effective as our ability to prevent proliferation of our own technology in order to prevent its use against us.

Military action should not be any nation's automatic response to a terrorist incident. As long as the possibility exists that terrorism may be prevented or perpetrators brought to justice by means of law enforcement activity, economic sanction, or other legal means, these options should be examined and employed to the fullest reasonable extent. In those instances where terrorist groups or supporting nations do not respond to these efforts, the military option may be considered. Military force, perceived or actual, is a valuable tool in the war against terrorism.

An interesting study published in *Terrorism and Political Violence* by Michele Malvesti attempts to identify the factors behind U.S. decisions to resort to overtmilitary force as a counter terrorism response. The factors were determined to be:[166]

- Relatively immediate positive perpetrator identification;
- perpetrator repetition;
- direct targeting of a U.S. citizen working in an official U.S. government related capacity:
- the fait accompli nature of the incident;
- flagrant anti-U.S. perpetrator behavior;
- the political and military vulnerability of the perpetrator; and
- maximization of casualties in an anti-U.S. terrorist incident.

Additionally, there appears to be a reliance on the use of "special forces" in our efforts so far against terrorism. General Sir Rupert Smith warned: "Be careful regarding who you think are 'special' in Special Forces."[167] "Growing forces" we can only use in limited fashion will result in the inefficient use of our entire force. The "average soldier" needs to be capable of operating in

the same environment we are now employing Special Forces. We need to "get the best out of the most, most of the time. Specialty should lie in secrecy and specialty of equipment, not in the competence implied in it."[168] Our military needs to be capable of "handling regional conflicts, crime, home defense, and intrastate problems" with equal adeptness.[169]

**Special Programs**

One of the factors heightening fear, panic, and economic disruption as a result of a terrorist attack is the "incessant barrage of sensational reporting and commentary by 24-hour news TV."[170] An industry based monitoring body, like the "circuit breakers" in the stock exchange, could be established to work with broadcasters to manage the flow and content of information. This body could ensure the telecasting of vital information while at the same time reducing the pressure of competition between broadcasters leading to sensationalized news.

"The media and the government have common interests in seeing that the media are not manipulated into promoting the cause of terrorism or its methods."[171] Neither the media nor policymakers want to see terrorism eroding constitutional freedoms including that of the press. This appears to be a dilemma which U.S. society will continually have to struggle. Improved cooperation between the media establishment and the government is essential if the U.S. is not to be embarrassed/damaged by a terror event and if freedom ofthe press is to be protected. Competition among the media is not conducive to self-restraint — they must recognize their power to affect public opinion and confidence in the government and possibly the outcome of a terrorist event.[172]

**Technology**

All of aspects of our society depend on a complex network of critical infrastructure and information systems. Protecting this infrastructure is critically important. The Director of Homeland Security, Thomas Ridge, put it succinctly:

> Disrupt, destroy or shut it down these information networks, and you shut down America as we know it and as we live it and as we experience it every day. We need to prevent disruptions; and when they occur, we need to make sure they are infrequent, short and manageable. This is an enormously difficult challenge. It is a technical challenge, because we must always remain one step ahead of the hackers. It's a legal challenge, because this effort raises cutting-edge questions of both privacy and civil liberties. It's a political challenge, because the government must act in partnership with the private sector, since most of the assets that are involved in this effort are owned by the private sector, which owns and operates the vast majority of America's critical infrastructure.[173]

"Terrorists can make connections between components of complex systems — such as between passenger airliners and skyscrapers — that few, if any, people have anticipated."[174] We must examine the systems critical to society and try to identify the weak links susceptible to attack. In so doing, we may be able to anticipate our vulnerabilities and reduce our risks. However, it would be naïve to think we could anticipate all the "exploitable unknown unknowns."[175] We must also take steps to "loosen the couplings in our complex economic and technological networks by building in buffering capacities and introducing 'circuit breakers' into our systems, and dispersing high-value assets so that they are less concentrated and less inviting targets."[176] Because 80% of the U.S. high technology and information infrastructure is owned and operated by the private sector, security against cyber attacks will require unprecedented cooperation between the private sector, and federal and state government agencies. America's critical technological and information assets must be identified, assessed for risk from terrorist attack, and then programs must be designed and implemented to minimize those risks.

As terrorist organizations become less hierarchical and increasingly networked, strategies that target "leadership" or charismatic members will become less effective. "Networked organizations rely on information flow to function, and disruption of the flows cripples their ability to coordinate actions."[177] An indication of an organization's susceptibility to info-war tactics is that organization's reliance on network technology to conduct its operations. Just as our reliance on networked technology can be used against us, "counter-terrorists" can adopt similar measures to defeat terrorist organizations. The key is proper identification of terrorist technological networks and the adoption of proper destructive and disruptive activities to overload them.[178]

To meet the challenges posed by WMD terrorism, the U.S. needs to accelerate and intensify nonproliferation efforts by emphasizing the following strategies:

- Persuade or induce proliferating governments to change course.
- Deny proliferators the supply of equipment, material, or technology from abroad.
- Continue programs to secure or eliminate Cold War WMD and missile capabilities.
- Strengthen existing international nonproliferation treaties, promote new ones that meet U.S. interests, and upgrade the means of verifying them.
- Continue development of a missile defense system.

The Livermore Study Group recommends and "end-to-end strategy to provide a multi-layered defense — from detection and prevention to reversal and response — in which all phases of a potential WMD terrorist attack can be addressed."[179]

| Intelligence and warning | Prevention | Crisis management | Consequence management | Retaliation |
|---|---|---|---|---|
| • Strategic warning<br>• Tactical warning | • Denial<br>• Demotivation<br>• Deterrence<br>• Elimination | • Detection<br>• Threat validation<br>• Location<br>• Weapon assessment<br>• Impact assessment<br>• Attribution<br>• Demotivation and deterrence<br>• Render safe | • Damage assessment<br>• Evacuation and protection<br>• Reconstitution<br>• Cleanup | • Attribution<br>• Prosecution<br>• Military response |

FIGURE 10. END-TO-END STRATEGY FOR RESPONDING TO WMD TERRORISM

In addition to policy, technology must be developed and applied to counter this threat. Current technologies under development that need to be refined for field use as soon as possible include:[180]

- Wide-Area Tracking System (WATS) for detecting and tracking a ground-delivered nuclear device.
- The Joint Biological Remote Early Warning System (JBREWS) for alerting U.S. field troops of an attack with biological agents.
- Portable radiation detectors designed to detect the isotopic signature of plutonium and uranium.
- Portable immunoassay and DNA recognition sensors for use in the field to identify specific biological warfare agents.

## CONCLUSION

In the post-cold war world, ethnic / religious / political problems previously held in check are surfacing with a vengeance. As the world's most influential economy and the only remaining superpower, the U.S. is a target of those forces which reject "our form" of modern culture, economics, and politics. Central to an understanding of the forces behind terrorism is the realization that globalization (and the complex interdependence it implies between modern nations) is accelerating a divide between "the haves" and the "have nots." The desired effects of the globalized economy — increased democracy, free trade, etc. — have not been dispersed, or accepted, equally throughout the world. An understanding of the "ideologies behind terrorism" will help focus our strategy and ensure we apply the most effective methods in fighting it.

We must streamline command and control in organizations responsible for combating terrorism, strengthen the interagency process, and integrate all elements of national power while remaining flexible enough to adapt rapidly to different environments.

The U.S. must include counter-terrorism as an underpinning of all diplomatic relations. Our strategy should include the implementation of tactics and technology designed to expose sponsors of terrorism; contain and prevent the emergence of terrorist safe havens; and target terrorist funding networks.

Additionally, the U.S. should implement measures designed to limit terrorist risks to our national interests and mitigate the effects of catastrophic attacks on those interests. Our information technology systems and intelligence related processes must also be improved in order to enhance the efficiency and effectiveness of our immigration service. Leaders and organizations that draw clout from ethnic, religious, and political unrest advance their agendas through asymmetric means, which includes terrorism. Terrorism's threat to the homeland has been magnified due to the proliferation of weapons and technology. Therefore, we have an acute need for intelligence and information in order to establish the plans of our opponents so we can devise our tactics for attack, deterrence, and coercion without aggravating our problem.

Therefore, a more effective U.S. strategy to combat terrorism depends upon:

- The Assistant to the President for Homeland Security must be granted stronger organizational control and budgetary authority.
- The Office of Homeland Security must be permanently established through congressional legislation.
- Future U.S. as an important element of foreign policy.
- Intergovernmental relations between federal, state, and local organizational responsible for homeland security must be improved.
- A single National Counter-Terrorism Center that plans intelligence collection for all agencies and produces analysis derived from all sources of intelligence should be created under the management of the Director of Central Intelligence.
- The U.S. should pursue policies and programs that promote greater allied and coalition involvement in the planning and execution of counter-terrorism.
- The military should ensure a greater percentage of U.S. forces are capable of operating effectively in environments traditional restricted to Special Forces.
- An industry based monitoring body should be established to work with broadcasters to manage the flow and content of information to prevent sensationalization of terrorism news coverage.
- The U.S. must strengthen efforts to protect its borders and critical infrastructures while accelerating and intensifying its WMD nonproliferation efforts.

This war can be won, but only if we apply our strategy correctly. Terrorists seek to exploit our weaknesses overseas and at home. Our strategy must effectively combine the efforts of all levels of government towards the goal of preventing additional attacks, mitigating the effects of attacks that do occur, and to identify, arrest and prosecute those who commit terrorism against us.

WORD COUNT: 11,841

## ENDNOTES

[1] William Cohen, "Preparing for a Grave New World," The Washington Post, 26 July 1999, sec A, p. 19.

[2] Raphael F. Perl, Terrorism, the Future, and U.S. Foreign Policy (Washington, D.C.: Congressional Research Service, The Library of Congress, 2001), 3.

[3] Title 22 of the US Code, Section 2656f(d).

[4] Congress, Senate, Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, Department of Defense and Combating Terrorism: Statement of Brian Sheridan, Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, 106th Cong., 24 March 2000; available from <http://www.defenselink.mil/ DODgc/lrs/docs/test00-03-24sheridan.rtf>; Internet; accessed 10 November 2001.

[5] Perl, Terrorism, the Future, and U.S. Foreign Policy, 2. For a complete list of significant terrorist incidents since 1961, see: U.S. Department of State, "Significant Terrorist Incidents, 1961-2001," 28 September 2001; available from <http://www.state.gov/r/pa/ho/ pubs/fs/index.cfm?docid=5902>; Internet; accessed 12 January 2002.

[6] National Intelligence Council, Global Trends 2015: A dialogue About the Future With Nongovernment Experts (Washington, D.C.: National Foreign Intelligence Board under the authority of the Director of Central Intelligence, 2000), 11.

[7] Ian O. Lesser et al., Countering the New Terrorism (Santa Monica, CA: Rand Corporation, 1999), 111.

[8] Conrad C. Crane, Alternative National Military Strategies for the United States, (Carlisle, PA: Strategic Studies Institute, 2000), 3.

[9] Lesser et al., Countering the New Terrorism, 8.

[10] Ibid., 9.

[11] Ibid., 12-28.

[12] Perl, Terrorism, the Future, and U.S. Foreign Policy, 3.

[13] Lesser et al., Countering the New Terrorism, 85-144.

[14] Perl, Terrorism, the Future, and U.S. Foreign Policy, 2.

[15] Lesser et al., Countering the New Terrorism, 7. Also in: U. S. Department of State, "Significant Terrorist Incidents, 1961-2001," 31 October 2001; available from <http:// www.state.gov/r/pa/ho/pubs/fs/index.cfm?docid=5902>; Internet; accessed 10 November 2001.

[16] Congress, House, Committee on Government Reform, Subcommittee on National Security, Veterans Affairs, and International Relations, Terrorism: Threat Assessment in a

Changing Global Environment: Statement of Raphael Perl, Specialist in International Affairs, Congressional Research Service, 106th Cong., 26 July 2000; available from <http://www.house.gov/reform/ns/hearing2/perl_jul_26.htm>; Internet; accessed 10 November 2001.

[17] Congress, House, Committee on Government Reform, Subcommittee on National Security, Veterans Affairs, and International Relations, Terrorism: Threat Assessment in a Changing Global Environment: Statement of Raphael Perl, Specialist in International Affairs, Congressional Research Service.

[18] Perl, Terrorism, the Future, and U.S. Foreign Policy, 4.

[19] U.S. Department of State, "America Responds: Building Global Freedom," 15 January 2001; available from <http://www.state.gov/s/ct/index.cfm?id=4291>; Internet; accessed 15 January 2002.

[20] The White House, "New Counter-Terrorism and Cyberspace Security Positions Announced," 9 October 2001, 1; available from <http://www.whitehouse.gov/news.releases/2001/10/print/20011009-4.html>; Internet; accessed 12 January 2002.

[21] The White House, "Frequently Asked Questions About the War on Terrorism at Home and Abroad." n.d., 1; available from <http://www.whitehouse.gov/response/faq-homeland.html>; Internet; accessed 12 January 2002.

[22] U.S. Department of State, "Statement Upon Release of Patterns of Global Terrorism 2000," 30 April 2001, 1; available from <http://www.state.gov/secretary/rm/2001/index.cfm?docid=2557>; Internet; accessed 12 January 2002.

[23] U.S. Department of State, "Press Release: United Against Terrorism," 7 November 2001; available form <http://www.state.gov/r/pa/rls/index.cfm?docid=5968>; Internet; accessed 10 November 2001. See also: Congress, Senate, Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, Department of Defense and Combating Terrorism: Statement of Brian Sheridan, Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict.

[24] Perl, Terrorism, the Future, and U.S. Foreign Policy, 11-12.

[25] U.S. Department of State, "The Global War on Terrorism: The First 100 Days," n.d., 10; available from <http://www.state.gov/s/ct/rls/rpt/index.cfm?docid=6947>; Internet; accessed 12 January 2002.

[26] The White House, "President Establishes Office of Homeland Security," 8 October 2001, 3; available from <http://www.whitehouse.gov/news/releases/2001/10/print/ 20011008.html>; Internet; accessed 12 January 2002.

The Council will have as its members the President, the Vice President, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Health and Human Services, the Secretary of Transportation, the Director of the Federal Emergency Management Agency, the Director of the Federal Bureau of Investigation, the Director of Central

Intelligence, the Assistant to the President for Homeland Security, and such other officers of the executive branch as the President may from time to time designate. The Chief of Staff, the Chief of Staff to the Vice President, the Assistant to the President for National Security Affairs, the Counsel to the President, and the Director of the Office of Management and Budget also are invited to attend any Council meeting. The Secretary of State, the Secretary of Agriculture, the Secretary of the Interior, the Secretary of Energy, the Secretary of Labor, the Secretary of Commerce, the Secretary of Veterans Affairs, the Administrator of the Environmental Protection Agency, the Assistant to the President for Economic Policy, and the Assistant to the President for Domestic Policy shall be invited to attend meetings pertaining to their responsibilities. The heads of other executive departments and agencies and other senior officials shall be invited to attend Council meetings when appropriate. The Council will meet at the President's direction.

[27] The White House, "Fact Sheet on New Counter-Terrorism and Cyberspace Positions," 9 October 2001, 1; available from <http://www.whitehouse.gov/news/releases/2001/10/print/20011009.html>; Internet; accessed 12 January 2002.

[28] Ibid

[29] U.S. Department of State, "The Global War on Terrorism: The First 100 Days," 11.

[30] Perl, Terrorism, the Future, and U.S. Foreign Policy, ii.

[31] U.S. Department of State, "International conventions and Other Treaties Relating to Terrorism," 13 November 2001; available from <http://www.state.gov/r/pa/ho/pubs/fs/index.cfm?docid=6093>; Internet; accessed 12 January 2002.

The United States is a party or signatory to the following international conventions and treaties relating to terrorism and its victims:

- 1963 Tokyo Convention on Offenses and Certain Other Acts Committed on Board Aircraft
- 1970 Hague Convention for the Unlawful Seizure of Aircraft
- 1971 Montreal Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation
- 1973 Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, Including Diplomatic Agents
- 1979 Convention Against the Taking of Hostages
- 1979 Convention on the Physical Protection of Nuclear Material
- 1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation (supplements the 1971 Montreal Convention)
- 1988 Rome Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation

- 1988 Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf (supplements the Rome Convention)
- 1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection
- 1997 Convention for the Suppression of Terrorist Bombings, signed by the United States on January 12, 1998, submitted to the Senate for advice and consent to ratification on September 8, 1999
- 1999 Convention for the Suppression of the Financing of Terrorism, signed by the United States on January 10, 2000 and submitted to the Senate for advice and consent to ratification on October 12, 2000

[32] U.S. Department of State, "The Global War on Terrorism: The First 100 Days," 4. See also: Perl, Terrorism, the Future, and U.S. Foreign Policy, 7.

[33] Lord Robertson, "Statement to the Press by NATO Secretary General, Lord Robertson, on the North Atlantic Council Decision On Implementation Of Article 5 of the Washington Treaty following the 11 September Attacks against the United States," 4 October 2001; available from <https://www.nato.int/docu/speech/2001/s011004b.htm>; accessed 9 March 2002.

Specifically, NATO agreed to:

- Enhance intelligence sharing
- Provide, as appropriate and according to ability, assistance to allies subject to terrorist threats as a result of their support for the campaign against terrorism
- Take necessary measures for the security for facilities of the U.S. and other allies on their territory
- Backfill selected allied assets in NATO's AOR that are required to directly support operations against terrorism
- Provide access for the U.S. and other allies to ports and airfields on the territory of NATO nations for operations against terrorism

[34] U.S. Department of State, "Patterns of Global Terrorism – 2000," 30 April 2001; available from <http://www.state.gov/s/ct/rls/pgtrpt/2000/>; Internet; accessed 12 January 2002.

[35] Perl, Terrorism, the Future, and U.S. Foreign Policy, 7.

[36] Ibid., 6. See also: U.S. Department of State, "Press Statement: Designation of 22 Foreign Terrorist Organizations Under Executive Order 13224," 2 November 2001; available from <http://www.state.gov/r/pa/prs/ps/2001/ index.cfm?docid=5885>; Internet; accessed 10 November 2001.

[37] U.S. Department of State, "Comprehensive list of Terrorists and Groups Identified Under Executive order 13224," 31 December 2001; available from <http://www.state.gov/s/ct/ rls/fs/2001/index.cfm?docid=6531>; Internet; accessed 15 January 2002.

Executive Order 13224, signed by President Bush on September 23, blocks the assets of organizations and individuals linked to terrorism. There are now 168 such groups, entities, and individuals covered by the Executive Order. Following is a complete listing:

- Original Annex: September 23, 2001:

Al-Qaida/Islamic Army*, Abu Sayyaf Group*, Armed Islamic Group (GIA)*, Harakat ul-mujahidin (HUM)*, Al-Jihad (Egyptian Islamic Jihad)*, Islamic Movement of Uzbekistan (IMU)*, Asbat al-Ansar, Salafist Group for Call and Combat (GSPC), Libyan Islamic Fighting Group, Al-Itihaad al-Islamiya (AIAI), Islamic Army of Aden, Usama bin Ladin ("Most Wanted" Terrorist), Muhammad Atif/Subhi Abu Sitta/Abu Hafs al-Masri ("Most Wanted" Terrorist – killed in Afghanistan), Sayf al-Adl ("Most Wanted" Terrorist), Shaykh Sa'id/Mustafa Muhammad Ahmad, Abu Hafs the Mauritanian/Mahfouz Ould al-Walid/Khalid al-Shanqiti, Ibn al-Shaykh al-Libi, Abu Zubaydah/Zayn al-Abidin Muhammad Husayn Tariq, Abd al-Hadi al-Iraqi/Abu Abdullah, Ayman al-Zawahiri ("Most Wanted" Terrorist), Thirwat Salah Shihata/Muhammad Ali, Tariq Anwar al-Sayyid Ahmad/Fathi/Amr al-Fatih, Muhammad Salah/Nasr Fahmi Nasr Hasanayn, Makhtab al-Khidamat/Al-Khifaf, Wafa Humanitarian Organization, Al-Rashid Trust, Mamoun Darkazanli Import-Export Company. (Note: Groups with asterisks are also designated as Foreign Terrorist Organizations under the Anti-terrorism and Effective Death Penalty Act)

- Designated on October 12, 2001

"Most Wanted" Terrorists: Abdullah Ahmed Abdullah, Muhsin Musa Matwalli Atwah, Ahmed Khalfan Ghailani, Ahmed Mohammed Hamed Ali, Fazul Abdullah Mohammed, Mustafa Mohamed Fadhil, Sheikh Ahmed Salim Swedan, Fahid Mohammed Ally Msalam, Anas al-Liby, Abdul Rahman Yasin, Khalid Shaikh Mohammed, Abdelkarim Hussein Mohamed al-Nasser, Ahmad Ibrahim al-Mughassil, Ali Saed bin Ali el-Hoorie, Ibrahim Salih Mohammed al-Yacoub, Ali Atwa, Hasan Izz-al-Din, Imad Fayez Mugniyah. Others: Rabita Trust, Jaish-e-Muhammad, Al-Hamati Sweets Bakeries, Al-Nur Honey Press Shops (aka: Al-Nur Honey Center), Chafiq bin Muhammad al-Ayadi, Dr. Amin al-Haq (Dr. Amin ul-Haq), Jamyah Taawun al-Islamia (aka: Society of Islamic Cooperation), Mohammad Zia, Mufti Rashid Ahmad Ladeyaznoy (Karachi, Pakistan), Muhammad al-Hamati (aka: Muhammad Hamdi Sadiq al-Ahdel), Omar Mahmoud Uthman (aka: Abu Qatada al-Filistini), Tohir Yuldashev, Mamoun Darkazanli, Saqar al-Jadawi, Ahmad Said al-Kadr, Sad al-Sharif, Bilal bin Marwan, Al-Shifa Honey Press for Industry and Commerce, Haji Abdul Manan Agha, Yasin al-Qadi (aka: Shaykh Yassin Abdullah Kadi), Riad Hijazi.

- Designated on November 2, 2001

Abu Nidal Organization (ANO), Aum Shinrikyo, Basque Fatherland and Liberty (ETA), Gama'a al-Islamiyya (Islamic Group), HAMAS (Islamic Resistance Movement), Hizballah (Party of God), Kahane Chai (Kach), Kurdistan Workers' Party (PKK), Liberation Tigers of Tamil Eelam (LTTE), Mujahedin-e Khalq Organization (MEK), National Liberation Army (ELN), Palestinian Islamic Jihad (PIJ), Palestine Liberation Front (PLF), Popular Front for the Liberation of Palestine (PFLP), PFLP-General Command (PFLP-GC), Real IRA, Revolutionary Armed Forces of Colombia (FARC), Revolutionary Nuclei (formerly ELA), Revolutionary Organization 17 November, Revolutionary People's Liberation Army/Front (DHKP/C), Shining Path (Sendero Luminoso, SL), United Self-Defense Forces of Colombia (AUC). (Note: All

22 groups are also designated as Foreign Terrorist Organizations under the Anti-terrorism and Effective Death Penalty Act)

- Designated on November 7, 2001

Aaran Money Wire Service, Inc., Al Baraka Exchange LLC, Al-Barakaat, Al-Barakaat Bank, Al-Barakat Bank of Somalia (BSS), Al-Barakat Finance Group, Al-Barakat Financial Holding Co., Al-Barakat Global Telecommunications, Al-Barakat Group of Companies Somalia Limited, Al-Barakat International (AKA Baraco Co), Al-Barakat Investments, Al-Barakat Wiring Service, Al Taqwa Trade, Property and Industry Company Limited, ASAT Trust, Bank al Taqwa Limited, Baraka Trading Company, Barakaat Boston, Barakaat Construction Company, Barakaat Enterprise, Barakaat Group of Companies, Barakaat International, Barakaat International Foundation, Barakaat International, Inc., Barakaat North America, Inc, Barakaat Red Sea Telecommunications, Barakaat Telecommunications Co Somalia, Barakat Bank and Remittances, Barakat Computer Consulting (BCC), Barakat Consuting Group (BCG), Barakat Global Telephone Company, Barakat International Companies (BICO), Barakat Post Express (BPE), Barakat Refreshment Company, Barakat Wire Transfer Company, Barakat Telecommunications Company Limited (BTELCO), Barako Trading Company, LLC, Global Services International, Heyatul Ulya, Nada Management Organization, Parka Trading Company, Red Sea Barakat Company Limited, Somalia International Relief Organization, Somali Internet Company, Somali Network AB, Youssef M. Nada & Co. Gesellschaft MBH, Youssef M. Nada, Hussein Mahmud Abdullkadir, Abdirasik Aden, Abbas Abdi Ali, Abdi Adulaziz Ali, Yusaf Ahmed Ali, Dahir Ubeidullahi Aweys, Hassan Dahir Aweys, Garad Jama, Ali Ghaleb Himmat, Albert Friedrich Armand Huber, Liban Hussein, Ahmed Nur Ali Jim'ale, Abdullahi Hussein Kahie, Mohamed Mansour, Zeinab Mansour-Fattouh, Youssef Nada.

- Designated on December 4, 2001

Holy Land Foundation, Beit El-Mal Holdings, Al-Aqsa Islamic Bank

- Designated on December 20, 2001

Lashkar e-Tayyiba (LET), Ummah Tameer e-Nau (UTN), Sultan Bashir-ud-Din Mahmood, Abdul Majeed, Mahammed Tufail

- Designated on December 31, 2001

Continuity Irish Republican Army (CIRA), Loyalist Volunteer Force (LVF), Orange Volunteers (OV), Red Hand Defenders (RHD), Ulster Defence Association/Ulster Freedom Fighters (UDA/UFF), First of October Antifascist Resistance Group (GRAPO)

- Designated on January 9, 2002

Afghan Support Committee (ASC), Revival of Islamic Heritage Society (RIHS) (NOTE:Only the Pakistan and Afghanistan offices of the entity have been designated.), Abd al-Muhsin al Libi, Abu Bakr al-Jaziri.

[38] Perl, Terrorism, the Future, and U.S. Foreign Policy, 1.

[39] U.S. Department of State, "The Global War on Terrorism: The First 100 Days," 5-6.

[40] Ibid.

[41] Ibid. G-20 Member countries include: Argentina, Australia, Brazil, Canada, China, France, Germany, India, Indonesia, Italy, Japan, Mexico, Russia, Saudi Arabia, South Africa, Korea, Turkey, the United Kingdom, and the United States. The IMF is an international organization of 183 member countries, established to promote international monetary cooperation, exchange stability, and orderly exchange arrangements; to foster economic growth and high levels of employment; and to provide temporary financial assistance to countries to help ease balance of payments adjustment.

[42] U.S. Department of Defense, Quadrennial Defense Review Report (Washington, D.C.: Department of Defense, September 2001), derived from 18 and 19.

[43] U.S. Department of Defense, CONPLAN : United States Government Interagency Domestic Terrorism Concept of Operations Plan, (Washington, D.C.: U.S. Department of Defense, 2001), 7.

[44] Federal Emergency Management Agency, "Responding to the Emergency Consequences of Terrorism," briefing slides used in a presentation to the Army War College class, Carlisle Barracks: U.S. Army War College, November 2001.

[45] George Melloan, "America's Federal Agencies Stake 'Homeland Defense' Claims," The Wall Street Journal, 27 November 2001, sec. A, p. 23.

[46] William L. Waugh Jr. and Richard T. Sylves, "Defending the Homeland: Institutionalism and the Politics of Weapons of Mass Destruction," 2 December 1999, 9; available from <http://bush.tamu.edu/pubman/papers/1999/waugh99.pdf>; Internet; accessed 11 December 2001.

[47] General Accounting Office, Combating Terrorism: Issues in Managing Counterterrorist Programs: Statement of Norman J. Rabkin, Director National Security Preparedness Issues, National Security and International Affairs Division (Washington, D.C.: U.S. General Accounting Office, 6 April 2000), 8.

[48] U.S. Department of State, "The Global War on Terrorism: The First 100 Days," 10-11.

[49] Central Intelligence Agency, "The War on Terrorism: DCI Counter-terrorist Center," 22 January 2002, 2; available from <http://www.cia.gov/terrorism/ctc.html>; Internet; accessed 16 February 2002.

[50] U.S. Intelligence Community, "Who We Are and What We Do," n.d., 1-2; available from <http://www.cia.gov/ic/functions.html>; Internet; accessed 16 February 2002.

[51] Ibid. See also John Deutch and Jeffery H. Smith, "Smarter Intelligence," Foreign Policy, January/February 2002, 66.

[52] Deutch and Smith, 66.

[53] Perl, Terrorism, the Future, and U.S. Foreign Policy, 6.

[54] Ibid., 7.

[55] MACA LAW AND POLICY. **Domestic Disaster Relief:** 31 US Code 1535, "Economy Act"; 33 US Code Sec 701, "Flood Control"; 41 US Code Sec 11, "Food and Forage Act"; 42 US Code Sec 5121, "Stafford Act Federal Response Plan"; Executive Order 12656, "Assignment of Emergency Preparedness Responsibilities," 18 Nov 88DOD Directive 3020.36, "Assignment of National Security Emergency Preparedness Responsibilities to DOD Components," Nov 88;DOD Directive 3025.1, "Military Support to Civil Authorities (MSCA)," 15 Jan 93; DOD Regulation 3025.1-M "DOD MANUAL FOR CIVIL EMERGENCIES," June 1994. **International Relief:** 10 US Code Sec 401, "Humanitarian Relief"; 10 US Code Sec 404, "Foreign Disaster Assistance". **Immigration Emergencies:** HSPD-2, "Combating Terrorism Through Immigration Policy"; 42 US Code Sec 5121, "Stafford Act Federal Response Plan". **Environmental Incidents:** 42 US Code Sec 5121, "Stafford Act Federal Response Plan"; 42 US Code Sec 9601-9675, "Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA)"; Title 40 Code of Federal Regulations, Part 300, "National Oil and Hazardous Substances Pollution Contingency Plan (NCP)"; 33 US Code Sec 1251-1386, "Federal Water Pollution Control Act"; DOD Directive 5030.41, "Oil and Hazardous Substances Pollution Prevention and Contingency Program," 1 Jun 77. **Weapons of Mass Destruction Accidents/Incidents:** PDD 39 US Policy on Counter Terrorism; 42 US Code 3151, "Stafford Act Federal Response Plan"; DOD Directive 3150.5, "DOD Response to Improvised Nuclear Device Threats,"24 Mar 87; DOD Directive 3150.8, "DOD Response to Radiological Accidents," 13 Jun 96. **Postal Augmentation:** DOD Directive 5030.50, "Employment of DOD Resources in Support of the U.S. Postal Service," 13 Apr 72;CJSC Instruction 3217.01, "Military Assistance to the US Postal Service," 30 May 95. **Civil Disturbances:** US Constitution Article 1 Section 8;10 US Code Sec 331-335, "Insurrection Act"; 18 US Code Sec 1385, "Posse Comitatus";DOD Directive 3025.12, "Military Assistance for Civil Disturbances (MACDIS)," 4 Feb 94; DOD Directive 5525.5, "DOD Cooperation with Civilian Law Enforcement Officials,"15 Jan 86; DOD Civil Disturbance Plan, "GARDEN PLOT," 15 Feb 91. **Critical Infrastructure Program:** PDD 62, "Combating Terrorism"; PDD 63, "Critical Infrastructure Protection"; DOD Directive 5160.54, "DOD Critical Asset Protection Program (CAAP)," 20 Jan 98. **Support to Law Enforcement:**10 US Code Sec 124. - Detection and monitoring of aerial and maritime transit of illegal drugs: Department of Defense to be lead agency; 10 US Code Sec 371, "Use of information collected during military operations"; 10 US Code Sec 372, "Use of Military Equipment and Facilities"; 10 US Code Sec 373, "Training and Advising"; 10 US Code Sec 374, "Operation of Equipment"; 10 US Code Sec 375, "Restriction on Direct Participation"; 10 US Code Sec 376, "Affect on Military Preparedness"; 10 US Code Sec 377, "Reimbursement"; 10 US Code Sec 380, "Annual Briefing to States"; 10 US Code Sec 381, "Procurement of Equipment"; 10 US Code Sec 382, "WMD Event"; 18 US Code Sec 1385, "Posse Comitatus"; 31 US Code Sec 1535, "Economy Act";PDD 39, "US Policy on Counter-terrorism"; PDD 62, "Combating Terrorism"; HSPD-1, "Combating Terrorism"; DOD Directive 5525.5, "DOD Cooperation with Civilian Law Enforcement Officials". **Continuity of Government (COG) Continuity of Operations (COOP):** PDD 67, "Enduring Constitutional Government". **Emergency Preparedness:** Executive Order 12656, "Emergency Preparedness Responsibilities". **Support to Secret Service:** DOD Directive 3025.13, "Defense Resources in Support of United States Secret Service". **Special Events:** 10 US Code Sec 2551 Equipment and barracks: national veterans' organizations; 10 US Code Sec 2552 Equipment for instruction and practice: American National Red Cross; 10 US Code Sec 2553 Inaugural; 10 US Code Sec 2554 Boy Scout Jamboree; 10 US Code Sec 2564 Sporting Events (Olympics, Goodwill, World Cup, etc).

[56] Charles Doyle, "Terrorism: Section by Section Analysis of the USA PATRIOT Act," CRS Report for Congress (Washington D.C.: Congressional Research Service, 2001), i; available from <http://www.fpc.gov/CRS_REPS/tssa1210.pdf>; Internet; accessed 9 March 2002.

[57] Perl, Terrorism, the Future, and U.S. Foreign Policy, 9.

[58] Cathy Condon, Special Assistant to the Secretary of the Army-Military Support, "Homeland Security Briefing," briefing slides used in a presentation to the Army War College class, Carlisle Barracks, U.S. Army War College, November 2001.

[59] U.S. Department of Defense, CONPLAN : United States Government Interagency Domestic Terrorism Concept of Operations Plan, 3.

[60] Congress, Senate, Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities, Department of Defense and Combating Terrorism: Statement of Brian Sheridan, Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict.

[61] U.S. Department of Defense, CONPLAN : United States Government Interagency Domestic Terrorism Concept of Operations Plan, 4.

[62] Ibid.

[63] Perl, Terrorism, the Future, and U.S. Foreign Policy, 12.

[64] Congress, House, Committee on Government Reform, Subcommittee on National Security, Veterans Affairs, and International Relations, Terrorism: Threat Assessment in a Changing Global Environment: Statement of Raphael Perl, Specialist in International Affairs, Congressional Research Service.

[65] Congress, House, Committee on Government Reform, Subcommittee on National Security, Veterans Affairs, and International Relations, Terrorism: Threat Assessment in a Changing Global Environment: Statement of Raphael Perl, Specialist in International Affairs, Congressional Research Service.

[66] Center for Nonproliferation Studies, Monterey Institute of International Studies, "Organizational Chart for Terrorism Response," 24 October 2001; available from <http://cns.miis.edu/research/cbw/domestic.htm>; Internet; accessed 13 January 2002.

[67] Moisés Naím, "Anti-Americanisms: A guide to hating Uncle Sam," Foreign Policy, January/February 2000, 104.

For example, the author sites "In Argentina, Hebe de Bonafini, an internationally known human rights activist and president of the Association of the Mothers of Plaza de Mayo said, "When the attack happened...I felt happiness." In France, the editor of Le Monde Diplomatic summarized his view of the world's reaction: "What's happening to [Americans] is too bad, but they had it coming."

[68] National Intelligence Council, 57.

[69] U.S. Department of State, "Statement Upon Release of Patterns of Global Terrorism 2000," 2.

[70] Naím, 103.

[71] National Intelligence Council, 10.

[72] Steven Metz, "Asymmetry and the Strategy of Osama bin Laden," briefing slides used in a presentation to the Army War College class, Carlisle Barracks, U.S. Army War College, October 2001.

[73] Michael Howard, "What's in a Name? How to Fight Terrorism," Foreign Affairs, January/February 2002, 12.

[74] Naím, 104.

[75] Perl, Terrorism, the Future, and U.S. Foreign Policy, 6.

[76] Ibid., 7.

[77] Ibid., 15.

[78] Ibid., 18.

[79] Ibid., 17.

[80] Ibid., 15.

[81] Ibid., 5.

[82] Waugh Jr., 6.

[83] General Accounting Office, Combating Terrorism: Issues in Managing Counterterrorist Programs: Statement of Norman J. Rabkin, Director National Security Preparedness Issues, National Security and International Affairs Division, 9.

[84] Ibid., 10.

[85] Ibid.

[86] Stephen E. Flynn, "America the Vulnerable," Foreign Affairs, January/February 2002, 61.

[87] Ibid., 62.

[88] Katherine McIntire Peters, "The War At Home: Federal Agencies Are Badly Organized to Protect Americans Against Terrorism," Government Executive, November 2001, 29.

[89] According to the year 2000 census.

[90] Ibid.

[91] Ibid.

[92] Congress, Senate, Judiciary Committee, Subcommittee on Immigration, Statement of James W. Ziglar, Commissioner, Immigration and Naturalization Service Regarding Effective Immigration Controls to Deter Terrorism, 107th Cong., 2001.

[93] Deutch and Smith, 64.

[94] Ibid.

[95] Ibid.

[96] Ibid., 66.

[97] White, 6.

[98] Jeffrey B. White, "A Different Kind of Threat: Some Thoughts on Irregular Warfare," 1996, 1; available from <http://www.cia.gov/csi/studies/96unclass/iregular.htm>; Internet; accessed 24 February 2002.

[99] Crane, 4.

[100] Ibid., 6.

[101] White, 1.

[102] Dr. Ely Karmon, "Intelligence and the Challenge of Terrorism in the 21st Century," 1-2 November 1998, 4-5; available from <http:/www.osp.state.or.us/oem/library/interesting %20reading/intelligence_and_the_challenge_of_terrorism_in_the_21st_century.htm>; Internet; accessed 16 December 2001. This paper was presented at the conference "A Counter-Terrorism Strategy for the 21st Century: The Role of Intelligence" at The Morris E. Curiel Center for International Studies of Tel Aviv University, on 1-2 November 1998.

[103] Perl, Terrorism, the Future, and U.S. Foreign Policy, 5.

[104] Matthew Oresman, "The Dilemma of Fighting Terrorism in a Constitutional Democracy: The 1996 Anti-Terrorism and Effective Death Penalty Act," 20 February 2001, 6; available from <http://www.nadn.navy.mil/nafac/delegates/papers/papers/u%20of%20penn/ matthew%20oresman%20u%20of%20penn.doc>; Internet; accesses 10 November 2001.

[105] Perl, Terrorism, the Future, and U.S. Foreign Policy, 9.

[106] National Intelligence Council, 56.

[107] Phillip S. Meilinger, "Force Divider: How military technology makes the United States even more unilateral," Foreign Policy, January/February 2002, 76.

[108] Ibid.

[109] Ibid., 77.

[110] Stephen H. Gotowicki, "Confronting Terrorism: New War Form or Mission Impossible," Military Review, May-June 1997, 61.

[111] Ibid. Lieutenant Colonel Gotowicki offers some compelling reasons why military capabilities alone would be ineffective in defeating terrorism:

- The asymmetries between conventional warfare and terrorism are profound.
- Terrorism's organizational structure is significantly below the "threshold of significance" typically addressed by conventional military forces.
- Identifying terrorist perpetrators is difficult.
- Terrorist doctrine is ad hoc and opportunistic.
- The terrorist chain of command is amorphous.
- Terrorist logistics are small scale.
- Intelligence requirements for dealing with terrorism differ significantly from those used in conventional conflicts.

[112] Isaac Shapiro, "In 2002, U.S. Aid to Poorer Nations Would Hit Post-WWII Lows as a Share of the Economy and the Budget," 18 June 2001; available from <http://www.cbpp.org/6-18-01bud-pr.htm>; Internet, accessed 10 march 2002. Figure Source: Center on Budget and Policy Priorities analysis of data from the Office of Management and Budget and USAID.

[113] Shapiro, Appendix 1.

[114] Congress, House, Committee on Government Reform, Subcommittee on National Security, Veterans Affairs, and International Relations, Terrorism: Threat Assessment in a Changing Global Environment: Statement of Raphael Perl, Specialist in International Affairs, Congressional Research Service.

[115] National Intelligence Council, 9.

[116] Ibid., 10.

[117] Thomas Homer-Dixon, "The Rise of Complex Terrorism," Foreign Policy, January/February 2002, 52.

[118] Ibid.

[119] Flynn, 63-64.

[120] Homer-Dixon, 54.

[121] Congress, House, Committee on Government Reform, Subcommittee on National Security, Veterans Affairs, and International Relations, Terrorism: Threat Assessment in a Changing Global Environment: Statement of Raphael Perl, Specialist in International Affairs, Congressional Research Service.

[122] Congress, House, Committee on Science, Hearing of the Committee on Science: Testimony of Governor James S. Gilmore, III, Governor of Virginia and Chairman of the Advisory Panel to Assess the Capabilities for Domestic Response to Terrorism Involving Weapons of Mass Destruction, 107th Congress, 17 October 2001, 3; available from <http://www.house.gov/science/full/oct17/gilmore.htm>; Internet; accesses 15 December 2001.

[123] Homer-Dixon, 56. Professor Homer-Dixon uses a stock market crash as an example, in which selling drives down prices, which begets more selling.

[124] Ibid.

[125] Lesser et al., Countering the New Terrorism, 41.

[126] Ibid., 87.

[127] Ibid., 39-68.

[128] Ibid., 70.

[129] Director of Central Intelligence, Unclassified Report to Congress on the Acquisition of Technology Relating to Weapons of Mass Destruction and Advanced Conventional Munitions, 1 January Through 30 June 2001 (Washington, D.C.: U.S. Central Intelligence Agency, 05 March 2001); available from < http://www.odci.gov/cia/publications/bian/ bian_jan_2002.htm#3>; Internet; accessed 27 February 2002. Evidence indicates determined Iranian efforts to acquire WMD related equipment, materials, and technology primarily from entities in Russia, China, North Korea, and Europe. Since the Gulf war, Iraq has rebuilt key portions of its chemical production infrastructure for industrial and commercial use, as well as its missile production facilities. It has also attempted to purchase numerous dual-use items for, or under the guise of, legitimate civilian use. This equipment could be diverted for WMD purposes.

[130] Perl, Terrorism, the Future, and U.S. Foreign Policy, 4.

[131] General Sir Rupert Smith, "Kermit Roosevelt Lecture, 2001," Lecture, Carlisle Barracks, PA, U.S. Army War College, 25 September 2001. Cited with permission of General Sir Rupert Smith, British Army. One of the most outstanding officers of his generation, General Sir Rupert Smith became DSACEUR after commanding the British Army in Northern Ireland between 1996 and 1998 and UNPROFOR in Bosnia and Herzegovina in 1995. Since November 1998, he was Deputy Supreme Allied Commander Europe from November 1998 to September 2002.

[132] General Accounting Office, Combating Terrorism: How Five Foreign Countries Are Organized to Combat Terrorism (Washington, D.C.: U.S. General Accounting Office, April 2000), 4. Also: Congress, House, Committee on Government Reform, Subcommittee on National Security, Veterans Affairs, and International Relations, Terrorism: Threat Assessment in a Changing Global Environment: Statement of Raphael Perl, Specialist in International Affairs, Congressional Research Service.

[133] Congress, House, Committee on Government Reform, Subcommittee on National Security, Veterans Affairs, and International Relations, Terrorism: Threat Assessment in a Changing Global Environment: Statement of Raphael Perl, Specialist in International Affairs, Congressional Research Service.

[134] Bruce Hoffman, "Reorganize to Meet Today's Threats," RAND Review, Fall 2001, 19.

[135] Peters, 28.

[136] General Accounting Office, Combating Terrorism: Selected Challenges and Related Recommendations (Washington, D.C.: U.S. General Accounting Office, September 2001). See chapter 2 for further discussion.

[137] Harold C. Relyea, "Homeland Security: The Presidential Coordination Office," CRS Report for Congress (Washington D.C.: Congressional Research Service, 10 October 2001), 4-6; available from <http://www.fpc.gov/crs_reps/crs.hsec. pdf>; Internet; accessed 11 December 2001.

[138] Ibid., 6.

[139] Howard, 13.

[140] National Intelligence Council, 34.

[141] Naím, 103.

[142] Ibid.

[143] Ian O. Lesser, "Strike at the Roots of Terrorism," RAND Review, Fall 2001, 14.

[144] Perl, Terrorism, the Future, and U.S. Foreign Policy, 17.

[145] Perl, Terrorism, the Future, and U.S. Foreign Policy, 17.

[146] Ibid.,18.

[147] General Accounting Office, Combating Terrorism: Issues in Managing Counterterrorist Programs: Statement of Norman J. Rabkin, Director National Security Preparedness Issues, National Security and International Affairs Division, 9.

[148] Ibid., 10. See also: General Accounting Office, Combating Terrorism: Selected Challenges and Related Recommendations (Washington, D.C.: U.S. General Accounting Office, September 2001), chapter 4 and 5.

[149] General Accounting Office, Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts: Statement of Raymond J. Decker, Director, Defense Capabilities and Management (Washington, D.C.: U.S. General Accounting Office, October 2001), 8.

[150] General Accounting Office, Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts: Statement of Raymond J. Decker, Director, Defense Capabilities and Management, 4.

[151] Ibid., 11.

[152] Ibid., 12.

[153] Congress, Senate, Judiciary Committee, Subcommittee on Immigration, Statement of James W. Ziglar, Commissioner, Immigration and Naturalization Service Regarding Effective Immigration Controls to Deter Terrorism.

[154] Alexander A. C. Gerry, "War on Terrorism Spawns New Technologies," ROA National Security Report, December 2001, 29-30. See also: John D. Woodward Jr., "Use Biometrics to Protect America," RAND Review, Fall 2001, 12-23.

[155] Congress, Senate, Judiciary Committee, Subcommittee on Immigration, Statement of James W. Ziglar, Commissioner, Immigration and Naturalization Service Regarding Effective Immigration Controls to Deter Terrorism.

[156] Ibid. Also: Flynn, 68.

[157] General Sir Rupert Smith, "Kermit Roosevelt Lecture, 2001".

[158] Gotowicki, 66. Lieutenant Colonel Gotowicki uses the following example: None of the national or local intelligence agencies detected the preparations or intentions of the two or three perpetrators of the Oklahoma City bombing. A proper intelligence focus against terrorism would be on group identification and intention. Intelligence should track the movements of very small quantities of weapons and explosives (because terrorist capabilities could reasonably consist of no more than a few rifles and several pounds of explosives), determine local political alignments and alliances, discern terrorist goals and objectives, identify and monitor disaffected and radicalized individuals and assess the influence of local religious leaders.

[159] Deutch and Smith, 66.

[160] Ibid., 66.

[161] Ibid., 66.

[162] White, 10.

[163] Ibid., 12. See also Karmon, 6.

[164] Meilinger, 77.

[165] Ibid.

[166] Michele L. Malvesti, "Explaining the United States' Decision to Strike Back at Terrorists," Terrorism and Political Violence, Summer 2001, 100.

[167] General Sir Rupert Smith, "Kermit Roosevelt Lecture, 2001".

[168] Ibid.

[169] Crane, 5.

[170] Homer-Dixon, 61.

[171] Raphael, F. Perl, "Terrorism, The Media, and The Government: Perspectives, Trends, and Options for Policymakers," CRS Issue Brief (Washington D.C.: Congressional Research Service, 22 October 1997), 9; available from <http://www. fas.org/irp/crs/crs-terror.htm>; Internet; accessed 10 November 2001.

[172] Robert H. Kupperman, and Deborah van Opstal, Terrorism, the Strategic Tool: A Glimpse at Tomorrow (Washington D.C.: Center for Strategic and International Studies, 1982), 8.

[173] The White House, "New Counter-Terrorism and Cyberspace Security Positions Announced," 2.

[174] Homer-Dixon, 61.

[175] Ibid.

[176] Ibid. For example, Professor Homer-Dixon suggests moving away from just-in-time production processes, increased autonomy of local and regional food production, increasing inventories of feedstock and parts, and the increased use of circuit breakers in systems modeled after the circuit breakers built into the New York Stock Exchange which halt trading if the market plunges more than a certain percentage in a particular period of time. These measures would undoubtedly decrease economic efficiency for the sake of increased security. However, he argues market forces will drive the implementation of these measures anyway if terrorist attacks continue.

[177] Lesser et al., Countering the New Terrorism, 80.

[178] Lesser et al., Countering the New Terrorism, 81. See also Karmon, 8.

[179] Lauren de Vore, "A National Strategy Against Terrorism Using Weapons of Mass Destruction," Science & Technology Review, January-February 1998, 25.

[180] Ibid., 26.

## BIBLIOGRAPHY


Betts, Richard K. "Fixing Intelligence." Foreign Affairs, January/February 2002, 43-59.

Biddle, Stephan. "War Aims and War Termination." Defeating Terrorism – Strategic Issue Analysis. Carlisle Barracks: U.S. Army War College, Strategic Studies Institute, December 2001. Available from < http://carlisle-www.army.mil/usassi/waraims.pdf>. Internet. Accessed 17 December 2001.

Center for Nonproliferation Studies, Monterey Institute of International Studies. "Organizational Chart for Terrorism Response." 24 October 2001. Available from <http://cns.miis.edu/research/cbw/domestic.htm>. Internet. Accessed 13 January 2002.

Central Intelligence Agency. "The War on Terrorism: DCI Counter-terrorist Center." 22 January 2002. Available from <http://www.cia.gov/terrorism/ctc.html>. Internet. Accessed 16 February 2002.

Cohen, William. "Preparing for a Grave New World." The Washington Post, 26 July 1999, sec A, p. 19.

Collins, Jim. "The Industrial Base from the Terrorist perspective - Dilemmas and Problems to Solve." Briefing slides. Pentagon: NAVAIR 3.2E, 9 October 2001.

Condon, Cathy, Special Assistant to the Secretary of the Army-Military Support. "Homeland Security Briefing." Briefing slides used in a presentation to the Army War College class. Carlisle Barracks: U.S. Army War College, November 2001.

Congress, House, Committee on Government Reform, Subcommittee on National Security, Veterans Affairs, and International Relations. "Terrorism: Threat Assessment in a Changing Global Environment." Statement of Raphael Perl, Specialist in International Affairs, Congressional Research Service. 106th Congress, 26 July 2000. Available from <http://www.house.gov/reform/ns/hearing2/perl_jul_26.htm>. Internet. Accessed 10 November 2001.

_____, Committee on Science. Hearing of the Committee on Science: Testimony of Governor James S. Gilmore, III, Governor of Virginia and Chairman of the Advisory Panel to Assess the Capabilities for Domestic Response to Terrorism Involving Weapons of Mass Destruction. 107th Congress, 17 October 2001. Available from <http://www.house.gov/science/full/oct17/gilmore.htm>. Internet. Accesses 15 December 2001.

Congress, Senate, Committee, on Armed Services, Subcommittee on Emerging Threats and Capabilities. "Department of Defense and Combating Terrorism." Statement of Brian Sheridan, Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict. 106th Congress, 24 March 2000. Available from <http://www.defenselink.mil/DODgc/lrs/docs/test00-03-24sheridan.rtf>. Internet. Accessed 10 November 2001.

_____, Judiciary Committee, Subcommittee on Immigration. Statement of James W. Ziglar, Commissioner, Immigration and Naturalization Service Regarding Effective Immigration Controls to Deter Terrorism. 107th Congress, 2001.

Cordesman, Anthony. "A New Strategy for Counter-Terrorism and Asymmetric Warfare." Defending America: Redefining the Conceptual Borders of Homeland Defense. Washington, D.C.: Center for Strategic and International Studies, 19 September 2001. Available from <http://www.csis.org/burke/hd/reports/New%20US%20Strategy%20for %20Terror%209-20.pdf>. Internet. Accessed 18 January 2002.

Crane, Conrad C. Alternative National Military Strategies for the United States. Carlisle, PA: Strategic Studies Institute, 2000.

de Vore, Lauren. "A National Strategy Against Terrorism Using Weapons of Mass Destruction." Science & Technology Review, January-February 1998, 24-26.

Deutch, John, and Jeffery H. Smith. "Smarter Intelligence." Foreign Policy, January/February 2002, 64-69.

Director of Central Intelligence. Unclassified Report to Congress on the Acquisition of Technology Relating to Weapons of Mass Destruction and Advanced Conventional Munitions, 1 January Through 30 June 2001. Washington, D.C.: U.S. Central Intelligence Agency, 05 March 2001. Available from < http://www.odci.gov/cia/publications/bian/ bian_jan_2002.htm#3>. Internet. Accessed 27 February 2002.

Doyle, Charles. "Terrorism: Section by Section Analysis of the USA PATRIOT Act." CRS Report for Congress. Washington D.C.: Congressional Research Service, 10 December 2001. Available from <http://www.fpc.gov/CRS_REPS/tssa1210.pdf>. Internet. Accessed 9 March 2002.

Federal Emergency Management Agency. "Responding to the Emergency Consequences of Terrorism." Briefing slides used in a presentation to the Army War College class. Carlisle Barracks: U.S. Army War College, November 2001.

Flynn, Stephen E. "America the Vulnerable." Foreign Affairs, January/February 2002, 60-74.

General Accounting Office. "Combating Terrorism: Issues in Managing Counterterrorist Programs." Statement of Norman J. Rabkin, Director National Security Preparedness Issues, National Security and International Affairs Division. Washington, D.C.: U.S. General Accounting Office, 6 April 2000.

_____. "Homeland Security: A Risk Management Approach Can Guide Preparedness Efforts." Statement of Raymond J. Decker, Director, Defense Capabilities and Management. Washington, D.C.: U.S. General Accounting Office, October 2001.

_____. Combating Terrorism: How Five Foreign Countries Are Organized to Combat Terrorism. Washington, D.C.: U.S. General Accounting Office, April 2000.

_____. Combating Terrorism: Selected Challenges and Related Recommendations. Washington, D.C.: U.S. General Accounting Office, September 2001.

Gerry, Alexander A. C.. "War on Terrorism Spawns New Technologies." ROA National Security Report, December 2001, 29-30.

Gotowicki, Stephen H. "Confronting Terrorism: New War For or Mission Impossible." Military Review, May-June 1997, 61-66.

Grossman, Elaine M. "Key Review Offers Scant Guidance On Handling '4th Generation' Threats." Inside The Pentagon, 4 October 2001, 1. Available from <http://www.d-n-i.net/fcs_folder/itp_qdr.htm>. Internet. Accessed 16 October 2001.

Harmon, Christopher C.. Terrorism Today. Portland, Oregon: Frank Cass Publishers, 2000.

Hoffman, Bruce. "Reorganize to Meet Today's Threats." RAND Review, Fall 2001, 19-20.

Homer-Dixon, Thomas. "The Rise of Complex Terrorism." Foreign Policy, January/February 2002, 52-62.

Howard, Michael. "What's in a Name? How to Fight Terrorism." Foreign Affairs, January/February 2002, 8-13.

Karmon, Dr. Ely. "Intelligence and the Challenge of Terrorism in the 21st Century." 1-2 November 1998. Available from <http:/www.osp.state.or.us/oem/library/interesting%20reading/intelligence_and_the_challenge_of_terrorism_in_the_21st_century.htm>. Internet. Accessed 16 December 2001. This paper was presented at the conference "A Counter-Terrorism Strategy for the 21st Century: The Role of Intelligence" at The Morris E. Curiel Center for International Studies of Tel Aviv University, on 1-2 November 1998.

Kelly, Terrence. "An Organizational Framework for Homeland Defense." Parameters, Autumn 2001: 105-16.

Kupperman, Robert H. and Deborah van Opstal. Terrorism, the Strategic Tool: A Glimpse at Tomorrow. Washington D.C.: Center for Strategic and International Studies, 1982.

Lesser, Ian O., Bruce Hoffman, John Arquilla, David Ronfeldt, and Michele Zanini. Countering the New Terrorism. Santa Monica, CA: Rand Corporation, 1999.

Lesser, Ian O.. "Strike at the Roots of Terrorism." RAND Review, Fall 2001, 14-15.

Malvesti, Michele L. "Explaining the United States' Decision to Strike Back at Terrorists." Terrorism and Political Violence, Summer 2001, 85-106.

Masci, David and Kenneth Jost. "War on Terrorism." The CQ Researcher, 12 October 2001, 817-48.

Meilinger, Phillip S. "Force Divider: How military technology makes the United States even more unilateral." Foreign Policy, January/February 2002, 76-77.

Melloan, George. "America's Federal Agencies Stake 'Homeland Defense' Claims." The Wall Street Journal, 27 November 2001, sec. A, p. 23.

Metz, Steven. "Asymmetry and the Strategy of Osama bin Laden." Briefing slides used in a presentation to the Army War College class. Carlisle Barracks: U.S. Army War College, October 2001.

_____. "Which Army After Next? The Strategic Implications of Alternative Futures." Parameters, Autumn, 1997, 15-26. Available from <http://carlisle-www.army.mil/usawc/parameters/97autumn/metz.htm>. Internet. Accessed 10 November 2001.

Naím, Moisés. "Anti-Americanisms: A guide to hating Uncle Sam." Foreign Policy, January/February 2000, 103-104.

National Commission on Terrorism. Countering the Changing Threat of International Terrorism: Report of the National Commission on Terrorism. 7 June 2000. Available from <http://www.fas.org/irp/threat/commission.html>. Internet. Accessed 10 November 2001.

National Intelligence Council. Global Trends 2015: A dialogue About the Future With Nongovernment Experts. Washington, D.C.: National Foreign Intelligence Board under the authority of the Director of Central Intelligence, December 2000.

Netanyahu, Benjamin. Fighting Terrorism: How Democracies Can Defeat the International Terrorist Network, 2001 Edition. New York: Farrar, Straus, and Giroux, 2001.

Oresman, Matthew. "The Dilemma of Fighting Terrorism in a Constitutional Democracy: The 1996 Anti-Terrorism and Effective Death Penalty Act." 20 February 2001. Available from <http://www.nadn.navy.mil/nafac/delegates/papers/papers/u%20of%20penn/matthew%20oresman%20u%20of%20penn.doc>. Internet. Accesses 10 November 2001.

Perl, Raphael F. "Terrorism, the Future, and U.S. Foreign Policy." CRS Issue Brief for Congress. Washington D.C.: Congressional Research Service, 2 November 2001. Available from <http://www.fpc.gov/crs_reps/tff.1102.pdf>. Internet. Accessed 11 December 2001.

_____. "Terrorism, The Media, and The Government: Perspectives, Trends, and Options for Policymakers." CRS Issue Brief. Washington D.C.: Congressional Research Service, 22 October 1997. Available from <http://www. fas.org/irp/crs/crs-terror.htm>. Internet. Accessed 10 November 2001.

Peters, Katherine McIntire. "The War At Home: Federal Agencies Are Badly Organized to Protect Americans Against Terrorism." Government Executive, November 2001, 27-31.

Relyea, Harold C. "Homeland Security: The Presidential Coordination Office." CRS Report for Congress. Washington D.C.: Congressional Research Service, 10 October 2001. Available from <http://www.fpc.gov/crs_reps/crs.hsec. pdf>. Internet. Accessed 11 December 2001.

Robertson, Lord. "Statement to the Press by NATO Secretary General, Lord Robertson, on the North Atlantic Council Decision On Implementation Of Article 5 of the Washington Treaty following the 11 September Attacks against the United States." 4 October 2001. Available from <https://www.nato.int/docu/speech/2001/s011004b.htm>. Accessed 9 March 2002.

Shapiro, Isaac. "In 2002, U.S. Aid to Poorer Nations Would Hit Post-WWII Lows as a Share of the Economy and the Budget." 18 June 2001. Available from <http://www.cbpp.org/6-18-01bud-pr.htm>. Internet, Accessed 10 march 2002.

Smith, James M. and William C. Thomas, Eds. The Terrorism Threat and U.S. Government Response: Operational and Organizational Factors. Colorado Springs, CO.: USAF Academy, USAF Institute for National Security Studies, 2001.

Smith, Rupert. "Kermit Roosevelt Lecture, 2001." Lecture. Carlisle Barracks, PA, U.S. Army War College, 25 September 2001. Cited with permission of General Sir Rupert Smith, British Army.

Stein, Fred. "Homeland Defense Definitions, etc." Briefing Slides. Arlington, Virginia: MITRE Corporation, 9 February 2002. MITRE is a not-for-profit national technology resource that provides systems engineering, research and development, and information technology support to the government. It operates federally funded research and development centers for the DOD, the FAA, and the IRS.

The Gilmore Commission. Advance Executive Summary: Third Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. 31 October 2001. Available from <http://www.rand.org/organization/nsrd/terrpanel>. Internet. Accessed 14 December 2001.

_____. First Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction I. Assessing the Threat, 15 December 1999. Available from <http://www.rand org/nsrd/terrpanel/terror.pdf>. Internet. Accessed 11 November 2001.

_____. Second Annual Report of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction II. Toward A National Strategy for Combating Terrorism, 15 December 2000. Available from <http://www.rand org/nsrd/terrpanel/terror2.pdf>. Internet. Accessed 12 November 2001.

_____. Third Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction III. For Ray Downey, 15 December 2001. Available from <http://www.rand org/nsrd/terrpanel/terror3-screen.pdf>. Internet. Accessed 15 December 2001.

The White House. "Executive Order Establishing Office of Homeland Security." 8 October 2001. Available from <http://www.whitehouse.gov/news/releases/2001/10/print/ 20011008-2.html>. Internet. Accessed 12 January 2002.

_____. "Fact Sheet on New Counter-Terrorism and Cyberspace Positions." 9 October 2001. Available from <http://www.whitehouse.gov/news/releases/2001/10/print/ 20011009.html>. Internet. Accessed 12 January 2002.

_____. "Fact Sheet on Terrorist Financing Executive Order." 24 September 2001. Available from <http://www.whitehouse.gov/news/releases/2001/09/20010924-2.html>. Internet. Accessed 10 November 2001.

_____. "Frequently Asked Questions About the War on Terrorism at Home and Abroad." n.d. Available from <http://www.whitehouse.gov/response/faq-homeland.html>. Internet. Accessed 12 January 2002.

_____. "Homeland Security Presidential Directive–1: Organization and Operation of the Homeland Security Council." 29 October 2001. Available from <http://www.whitehouse.gov/news/releases/2001/10/print/20011030-1.html>. Internet. Accessed 10 November 2001.

_____. "Homeland Security Presidential Directive–2: Combating Terrorism through Immigration Policies." 29 October 2001. Available from <http://www.whitehouse.gov/news/releases/2001/10/print/20011030-2.html>. Internet. Accessed 10 November 2001.

_____. "New Counter-Terrorism and Cyberspace Security Positions Announced." 9 October 2001. Available from <http://www.whitehouse.gov/news.releases/2001/10/print/20011009-4.html>. Internet. Accessed 12 January 2002.

_____. "President Establishes Office of Homeland Security." 8 October 2001. Available from <http://www.whitehouse.gov/news/releases/2001/10/print/20011008.html>. Internet. Accessed 12 January 2002.

U.S. Department of Defense. CONPLAN : United States Government Interagency Domestic Terrorism Concept of Operations Plan. Washington, D.C.: U.S. Department of Defense, January 2001.

_____. Quadrennial Defense Review Report. Washington, D.C.: Department of Defense, September 2001.

U.S. Department of State. "America Responds: Building Global Freedom." 15 January 2001. Available from <http://www.state.gov/s/ct/index.cfm?id=4291>. Internet. Accessed 15 January 2002.

_____. "Comprehensive list of Terrorists and Groups Identified Under Executive order 13224." 31 December 2001. Available from <http://www.state.gov/s/ct/rls/fs/2001/index.cfm?docid=6531>. Internet. Accessed 15 January 2002.

_____. "International conventions and Other Treaties Relating to Terrorism." 13 November 2001. Available from <http://www.state.gov/r/pa/ho/pubs/fs/index.cfm?docid=6093>. Internet. Accessed 12 January 2002.

_____. "Patterns of Global Terrorism - 2000." 30 April 2001. Available from <http://www.state.gov/s/ct/rls/pgtrpt/2000/>. Internet. Accessed 12 January 2002.

_____. "Statement Upon Release of Patterns of Global Terrorism 2000." 30 April 2001. Available from <http://www.state.gov/secretary/rm/2001/index.cfm? docid=2557>. Internet. Accessed 12 January 2002.

_____. "The Global War on Terrorism: The First 100 Days." n.d.. Available from <http://www.state.gov/s/ct/rls/rpt/index.cfm?docid=6947>. Internet. Accessed 12 January 2002.

_____. "2001 Report on Foreign Terrorist Organizations." 5 October 2001. Available from <http://www.state.gov/s/ct/rls/rpt/fto/2001/index.cfm?docid=5258>. Internet. Accessed 11 November 2001.

_____. "Briefing on the Rewards For Justice Program." 13 December 2001. Available from < http://www.state.gov/secretary/rm/2001/dec/6844.htm>. Internet. Accessed 16 December 2001.

_____. "Overview of State-Sponsored Terrorism: Patterns of Global Terrorism –2000." April 2001. Available form <http://www.state.gov/s/ct/rls/pgtrpt/ 2000/index.cfm?docid=2441>. Internet. Accessed 10 November 2001.

_____. "Press Release: United Against Terrorism." 7 November 2001. Available form <http://www.state.gov/r/pa/rls/index.cfm?docid=5968>. Internet. Accessed 10 November 2001.

_____. "Press Statement: Designation of 22 Foreign Terrorist Organizations Under Executive Order 13224." 2 November 2001. Available form <http://www.state.gov/r/pa/prs/ps/2001/index.cfm?docid=5885>. Internet. Accessed 10 November 2001.

_____. "Significant Terrorist Incidents, 1961-2001." 31 October 2001. Available from <http://www.state.gov/r/pa/ho/pubs/fs/index.cfm?docid=5902>. Internet. Accessed 10 November 2001.

_____. "Significant Terrorist Incidents, 1961-2001." 28 September 2001. Available from <http://www.state.gov/r/pa/ho/pubs/fs/index.cfm?docid=5902>. Internet. Accessed 12 January 2002.

_____. "U.S. Humanitarian Aid and War Against Terrorism Go Hand in Hand." 30 October 2001. Available from <http://usembassy.state.gov/Tokyo/ wwwhse0585.html>. Internet. Accessed 10 March 2002.

U.S. Intelligence Community. "Who We Are and What We Do." n.d. Available from <http://www.cia.gov/ic/functions.html>. Internet. Accessed 16 February 2002.

U.S. Joint Chiefs of Staff. Joint Tactics, Techniques, and Procedures for Antiterrorism: Joint Pub 3-07.2. Washington D.C.: Joint Staff, 17 March 1998.

Waugh Jr., William L. and Richard T. Sylves. "Defending the Homeland: Institutionalism and the Politics of Weapons of Mass Destruction." 2 December 1999. Available from <http://bush.tamu.edu/pubman/papers/1999/waugh99.pdf>. Internet. Accessed 11 December 2001.

White, Jeffrey B. "A Different Kind of Threat: Some Thoughts on Irregular Warfare." 1996. Available from <http://www.cia.gov/csi/studies/96unclass/iregular.htm>. Internet. Accessed 24 February 2002.

Woodward Jr., John D.. "Use Biometrics to Protect America." RAND Review, Fall 2001, 21-23.

THE END