UNITED STATES SENATE COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM,

AND GOVERNMENT INFORMATION

SENATOR JON KYL, CHAIRMAN

CRIME, TERROR, & WAR: NATIONAL SECURITY & PUBLIC SAFETY IN THE INFORMATION AGE

SUBCOMMITTEE ACCOMPLISHMENTS IN THE 105TH CONGRESS

REPORT SUBMITTED BY MAJORITY STAFF

NOVEMBER 1998

INTRODUCTION

During the Cold War, the source and nature of threats to the United States were well understood. The Soviet strategic nuclear threat ordered American defense and intelligence planning. The offensive posture of the Warsaw Pact and Soviet regional subversion were answered by the strength of the NATO Alliance and the determination of the Reagan Doctrine, and a U.S. military that was designed and ready for force projection anywhere in the world.

There were more lives lost in hostilities during this so-called Cold War than at any comparable period in history. But for the most part, Americans felt safe at home. We lived with the horrible threat of mutual assured destruction for decades, before public opinion and Presidential leadership insisted upon real strategic defense (a goal that remains politically elusive even today). At the same time, civil defense, a common part of state and local planning in the 1950s, gradually became relegated to dusty contingency plans and late night TV jokes. Bomb shelters became wine cellars. The military not did not train to defend our shores, because there was no enemy poised to attack.

Today, however, the assumption that we Americans can rest in our island nation secure from foreign threats is not so comfortably obvious. It no longer takes a superpower to threaten the American homeland, as the spread of technology—especially weapons technologies—has lowered the threshold for what is needed to do serious harm. The 1998 Rumsfeld Commission report on the ballistic missile threat to the United States points out that lesser nations are developing capabilities to launch ballistic missiles that can reach Americans at home[1]. Many terrorists groups have a newfound interest in weapons that can cause a great number of casualties, such as biological and chemical weapons, and more sweeping social objectives for their terrorist campaigns. And the amazing tools of the Information Age, while giving tremendous advantage to every aspect of national life and expanding personal choices, also import vulnerabilities that may be exploited by America's adversaries.

In the face of these threats, we are coming to reexamine the meaning of national security, and the traditional ways in which government has provided for the common defense. When national security threats transcend our borders, it is clear that domestic tranquillity cannot be the exclusive province of law enforcement agencies. Nor can the military confine itself to defending against threats that arise only abroad.

For guardians of the nation's security, and defenders of the Constitution, I believe there is an important dividing line that we need to ponder: Where does national security leave off, and domestic security begin? What are the threats to our safety and security, and how can would-be aggressors be deterred? How can we defend against new adversaries who would exploit the weapons of the information age? What is the right national security strategy to protect America today? And what are the policies, plans, and programs needed to carry out that strategy? These questions are affecting the responsibilities we assign defense agencies, the intelligence community, and law enforcement agencies, and the relationships among them.

In hearings on U.S. counter-terrorism strategy, national preparedness to deal with potential acts of terrorism, and the protection of the nation's critical information infrastructure, the Subcommittee on Technology, Terrorism, and Government Information has explored these issues in the 105th Congress, in an effort to help develop insights and broaden understanding for meeting the national security and public safety needs of the 21st century. This is a report of our findings.

I would like to acknowledge and thank the members of the majority staff who participated in writing this report. They are: Michelle Van Cleave, staff director and chief counsel; Janice Kephart-Roberts, counsel; and professional staff members Paul Nicholas, Brian Parr, David Stephens, and Rick Wilson.

Sincerely,

JON KYL

Chairman
Subcommittee on Technology, Terrorism,
and Government Information

CONTENTS

CHANGING NATURE OF SECURITY THREATS IN THE 21ST CENTURY

Coming out of World War II, Americans understood national security largely in military terms: what forces are required to counter the military threats arrayed against us? What resources do we need to support those forces? National policy was directed at containment of the Soviet Union, the reconstruction of Western Europe and Japan, and the protection of our interests in the Third World. And the United States was more than modestly successful in these pursuits.

But the job of ensuring national security capabilities adequate to post Cold War needs will be more challenging than it was during the Cold War, given the profound differences between the world we are entering and the world we are leaving.

Clearly the strategic nuclear threat to the United States has been sharply reduced by reason of the vast political changes in Russia and the breakup of the Soviet empire. Forces are dispersed, and coherence of command and control is uncertain. At the same time, previously negligible dangers have actually increased sharply: the potential for unauthorized or accidental missile launch, as well as the concern that one or more of these weapons could be diverted to a third party, either through sale or theft. Moreover, the former Soviet Union has not become a prosperous, capitalist democracy overnight, nor given the political patchwork of the present government is it obviously moving in that direction; indeed, the political evolution of Russia and the other newly independent states is the central strategic variable for the future.

The end of the Cold War has not meant the end of conflict or evil in the world. The peoples of Eastern Europe are struggling with the wrenching social and economic costs imposed by imperial Communist control, trying to build nations amidst the ruins of the present and the unsettled scores of the past. The failure of the communist model in the Soviet Union has not lessened the willingness of communist regimes in China, Cuba, Southeast Asia, North Korea and elsewhere forcibly to maintain power and control. And an American military presence has been needed in disparate regions at a pace and scale far in excess of the assumptions of the Pentagon's six-year budget plans. Who would have predicted that American troops would go to Somalia, Haiti, Rwanda, Bosnia, or Kosovo? Or that U.S. embassies in East Africa would be destroyed by terrorist bombs, resulting in the deaths of hundreds of Americans and Africans caught under the rubble? In this post Cold War era, American lives are on the line all over the world.

The spread of weapons technologies presents an additional set of national security concerns.[2] The proliferation of weapons of mass destruction is dispersed geographically, carried out against a backdrop of global commercial activities the great majority of which are lawful and non-threatening, involving actors of widely varying national background and methods of operation. Intelligence needs to work hand in glove with law enforcement to stop unlawful technology transfer; and other operations to interdict or disrupt weapons programs—should they be authorized and implemented—require tailored operational and intelligence capabilities.

The face of terrorism has also been changing dramatically over the past decade. In the 1970s and early 1980s, terrorist organizations

typically had discrete and immediate political objectives—the release of compatriots from prison, the political independence of ethnic region or state, or the withdrawal from a conflict. To further these goals, terrorists engaged in kidnapping, hijacking, small-scale hostage-taking, and other operations involving relatively low levels of violence. As summed-up by a leading expert in terrorism: traditional "terrorists want a lot of people watching, not a lot of people dead."[3]

Today's "post-modern" terrorists have eschewed unconstrained or modulated violence[4]. Many of these individuals and groups seek nothing but the wholesale collapse of societies and nations which they deem evil. These terrorists often embrace religious or quasi-religious ideologies based on ethnic or racist hate, fanaticism or apocalyptic "millenialism"; and because they believe their actions are justified to please a higher authority, the ability to kill large numbers of individuals only reinforces the correctness of their actions. Nation-states which oppose U.S. policies may cynically use these groups to advance their own nationalist, anti-American agendas, and provide safe haven and other logistical support to such terrorists.

The 1993 terrorist bombing at the World Trade Center brought these new threats closer to home. The blessings of our free and open society also can provide cover for acts of terror and violence; and penetrating terrorist networks to defeat their plans is an intelligence and law enforcement challenge of the first order.

Loss of Sanctuary

Indeed, perhaps the most surprising and disturbing feature of the post Cold War strategic setting is what defense planners are calling "the loss of sanctuary", i.e., new and growing strategic vulnerabilities of the United States.

Potential adversaries have been brought up short by the impressive showing of America's conventional military capabilities in the Persian Gulf War. One lesson learned is the futility of challenging the overwhelming military force of the United States and the West by conventional means. But potential adversaries may also have learned that attacking our vulnerabilities, rather than our strengths, might prove more effective.

Recent high level policy interest, as well as public concern, has focused on conventional terrorist threats to U.S. infrastructure targets, in the wake of such horrors as the bombings at the World Trade Center and the Oklahoma City Federal Building. Single point physical destruction is obviously a real threat and a serious concern.

But even more disturbing scenarios, involving infrastructure coordinated attacks or advanced unconventional weapons, are not out of the range of possibility. The proliferation of advanced technological capabilities has created a new and more diverse set of potential adversaries. The harm that can be caused by non-state actors also is potentially wider, deeper, and more tailored than previously seen. The abilities of hostile states to exploit information warfare (IW) techniques or other emerging categories of special technologies (for example, many of the so-called "non-lethal" technologies) are poorly understood. Indeed, the U.S. intelligence community is not able today to answer even the first order questions about the IW or special weapons capabilities of potential adversaries, much less perform the traditional but now much more sophisticated work of strategic and tactical indications and warning (I&W) of attack.

A complicating factor is that increasing awareness or perception by potential adversaries of broad vulnerabilities in the national support infrastructure gives rise to concerns that strategic threats may be induced by the very existence and reach of perceived strategic vulnerabilities. In the past, the sheer volume of dispersed information required by an adversary to understand and target critical U.S. infrastructure assets was a source of protection. But today, information technology tools enable focused intelligence collection about vulnerabilities previously available only to the major adversary. Expensive investment in intelligence collection is no longer required; indeed, in some cases, potential adversaries may be able to simply sit back and let others do their research for them. Unfortunately, many infrastructure vulnerabilities are now routinely sought out, collated, and described in great detail on the Internet by individuals apparently attracted by the ease of wide communication with like-minded persons and the virtual "lawlessness" of the forum itself. On the other hand, the nature of these technology-enabled threats may not be nearly as well understood by U.S. planners charged with their protection.

Technology blurs the distinction between a criminal act and an act of war.

Together, these new developments have helped produce a situation in which the cornerstone of defense policy, U.S. deterrence strategy, once so apparently clear and mission-defining during the Cold War, has become uncertain. The U.S. position as the only remaining superpower does not, by itself, guarantee protection from these threats. Nor is the U.S. national security process presently configured to handle foreign threats that exploit the U.S. homeland as a base for operations.

In the security environment of the 21st century, the distinction between criminal activities and acts of war is becoming increasingly blurred. What may appear to be an instance of a hacker breaking into a national security system may be indistinguishable from the precursors to a planned information warfare attack. And if the result were to be the same—the disruption of U.S. military defense capabilities at a critical point in an on-going conflict—should this be treated as simply a criminal act in the traditional sense? If a terrorist with established links to a hostile foreign adversary were to detonate a chemical or biological weapon in a major U.S. city, would this constitute an act of war by proxy? Such questions suggest that a new class of criminal activity may be emerging—perhaps best described as "strategic crime"—that by its very nature and scope can threaten the foundations of the nation. Developing effective strategies and policies to combat these "strategic crimes"—which may fall between the seams of traditional law enforcement activities and national defense efforts—is an urgent requirement for our government.

Recent Experience

Unfortunately, the threats and vulnerabilities we face are neither hypothetical nor abstract.

In the area of information and infrastructure security, there has been a soaring number of penetrations into commercial, military and infrastructure-related computer systems. FBI Director Louis Freeh has told Congress that FBI cases have been doubling every year[5]. Our

individual and personal freedoms have become more vulnerable in the face of advances in computing and software that have lowered the barriers to theft of personal information, such as birth dates, social security numbers, and credit information. Armed with such information, criminals can steal the identity of individuals, creating ruinous financial and legal situations for innocent victims.

For this reason, Senator Kyl championed a bill to make identify theft a federal crime. "The Identity Theft and Assumption Deterrence Act" (S. 512 which later became H.R.4151) was signed into law in October, 1998. The Act makes is unlawful to steal personal information, and enhances penalties against identity thieves. It recognizes victims by giving them the ability to seek restitution for all costs involved in restoring lost credit and reputation. And it establishes a centralized complaint and education service at the Federal Trade Commission[6].

Looking beyond threats to the individual, vulnerabilities in our critical infrastructures could be used to disrupt our national life and threaten our security. For example, several telecommunications firms were recently penetrated by an U.S.-based international hacker ring. Attorney General Reno has testified that this penetration "suggests that [the perpetrators] could have disrupted telecommunications on a national basis had they so desired."[7] In October of last year, an incident occurred where a former Pacific Gas & Electric Co. worker caused a widespread power outage in the San Francisco region.

Even more worrisome is an event that occurred in Spring of this year, in which Defense Department networks experienced their most widespread and systematic attacks to date. Over 20 major installations' networks were compromised. The timing of the attacks—dubbed "Solar Sunrise"—is noteworthy. They occurred while the military was trying to deploy forces to the Persian Gulf in response to Iraqi provocations. For over 4 days, the defense community and law enforcement agencies struggled to understand the nature of the attacks and identify the threat. The attacks were launched from computers within the United States and overseas. As it turned out, this incident involved a couple of California teenagers. But "Solar Sunrise" demonstrated an enormous vulnerability in our *unclassified* computer systems which nevertheless play a critical role in managing and moving U.S. armed forces all over the globe.

The threat of chemical and biological weapons (CBW) use against the United States is also growing. Terrorist interest in CBW is clearly on the rise. The Aum Shinrikyo cult's use of sarin gas in the Tokyo subway seared forever in our consciousness the vulnerability of our open societies to CBW terrorist attack. Terrorists operating in the United States have shown both the capability and possibly the intent to commit similar acts here. Investigations into the 1993 bombing of the World Trade Center revealed Ramzi Yousef's interest in using chemical weapons in that attack—which he abandoned only for lack of money.

In 1997, the FBI conducted over 100 criminal investigations involving chemical, biological and radiological weapons.[8] And the pace this year continues unabated. In February of this year, the FBI arrested two individuals in Las Vegas who were experimenting with strains—luckily harmless—of anthrax. Weeks later, an individual threatened the use of anthrax against a debt collection in Phoenix, causing a major disruption to city activities. And more recently, the

FBI arrested three men in Brownsville with threatening the use of biological weapons against the President and other federal officials.

Terrorists are not our only concern. Rogue states—such as Libya, Iraq, and North Korea—as well as Russia are aggressively pursuing CBW. We suspect that some of these countries' Special Forces are trained in the use of chemical and biological weapons. Simple CBW devices can be constructed with little difficulty and used for extremely lethal effect. They could be delivered by missile from ships not far from our shores, or delivered by terrorist proxies. Our intelligence community knows far too little about how rogue states intend to employ such weapons—a glaring shortfall in our capacity to devise effective strategies to prevent and deter the use of CBW against the U.S.

Significant uncertainties remain about how threats posed by new information technologies, information warfare capabilities and chemical and biological weapons will evolve. But we cannot afford to wait and let these emerging threats crystallize before developing effective strategies and policies to prevent, deter and defend the U.S. against such threats. Then, it will be too late.

Gaps in National Policy and Strategy

Defending the American homeland against possible cyber-assaults, physical attacks against our critical infrastructures, and chemical and biological weapons attack presents a new challenge for the United States. Consistent with the values and structures established by our Constitution, we need to refine the roles and responsibilities we assign law enforcement, intelligence agencies, and the military[9], to ensure they can work together, in their proper spheres, to provide for public safety and our nation's defense.

To address the full range of these issues, the Subcommittee held over a dozen hearings in the 105th Congress. The next part of this report describes Subcommittee objectives during those hearings, the principal issues addressed, Subcommittee findings, and resulting Subcommittee work. There was some encouraging news to emerge from parts of this 18-month inquiry. But unfortunately, in too many cases, the Subcommittee found a lack of understanding at the national level about the nature of the threats and challenges confronting the U.S.; a related absence of consensus on national strategies to respond to these challenges; and self-defeating policies and programs that increase our vulnerabilities. Much work remains to be done.

COUNTER-TERRORISM STRATEGY

Issues and Objectives

The August 7, 1998 car bomb attacks against U.S. embassies in Nairobi, Kenya and Dar es Salaam, Tanzania are a tragic reminder of the continuing threat posed to Americans by foreign terrorists. These attacks—which killed 12 U.S. citizens and over 250 others—make clear that the United States will continue to be targeted by terrorists who oppose our values and way of life. Equally clear is that the challenge of protecting Americans and American interests against terrorists requires a coherent national counter-terrorism strategy, one that is consistently implemented and relates resources and means to well-conceived objectives.

Against the backdrop of the embassy attacks, and the U.S. military response on August

20, 1998 against terrorist targets in Afghanistan and Sudan, the Judiciary Committee held a public hearing on September 3, 1998 on the subject of U.S. counter-terrorism strategy and its effectiveness. At Senator Kyl's initiation, the purpose of the hearing was to examine the objectives of U.S. strategy for combating terrorism and to consider the adequacy of national policies and resources in achieving these objectives.

In exercising its oversight of counter-terrorism policy, the Committee was particularly interested to learn whether the U.S. military response to the embassy attacks represented a change in the Administration's counter-terrorism strategy. Tomahawk cruise missile attacks against terrorist training camps in Afghanistan and a suspected chemical weapons production facility outside Khartoum, Sudan appeared to represent a new emphasis on the use of armed force to deter and defeat terrorism. At the same time, the Committee raised questions about the strategic objective of the targets selected. Related questions examined at the hearing included the roles envisioned for the intelligence community, law enforcement authorities, and the U.S. military in combating terrorism. In addressing these questions, the Committee examined in detail the bombings in East Africa, including the investigation and response, with an eye toward identifying needed improvements to our counter-terrorism strategy, policies, and capabilities.

Observations & Findings

Since the 1993 bombing of the World Trade Center in New York City and the 1995 bombing of the federal building in Oklahoma City, the United States government has taken important steps to improve its counter-terrorism capabilities. The U.S. is currently spending about $7 billion a year in the fight against terrorism.[10] Since 1995, Congress has more than doubled the counter-terrorism budget for the Federal Bureau of Investigation (FBI), from $118 million to $286 million.[11] The FBI now has its own Counter-terrorism Center to coordinate its activities and operations with all federal agencies, including the U.S. intelligence community; it employs more than 2500 agents worldwide who are dedicated to terrorism issues. And the U.S. Congress has provided increased legislative authorities to the FBI in recent years, including a 1994 law providing extraterritorial jurisdiction for the murder of U.S. citizens abroad with a weapon of mass destruction[12], such as the car-bomb used in both the Nairobi and Dar es Salaam embassy attacks.

These investments are producing results. The swift apprehension and rendering into U.S. custody of the suspects in the African bombings is the most recent and dramatic example of effective law enforcement action. Another example was the successful effort by the FBI, working through the inter-agency Joint Terrorism Task Force, to disrupt plans by Sheik Rahman and his followers to bomb several New York City landmarks in 1995, including the United Nations building and the Lincoln and Holland Tunnels. Classified briefings to Congress have described many other successes which the U.S. government has had in stopping more than a few terrorist plots each year.

In testifying before the Committee, FBI Director Louis Freeh observed that the expansion of the number of Legal Attaché offices around the world has had a "significant impact on the FBI's ability to track terrorist threats and bring investigative resources quickly to bear on cases where quick response is critical."[13] Most recently, the presence of FBI agents in African

capitals enabled the rapid start of the investigation into the East African embassy bombings, and laid the foundation for the quick apprehension of several suspects.

But alongside these considerable successes, our hearing uncovered significant weaknesses not only in our counter-terrorism capabilities, but in our strategic approach to battling terrorists as well. For example, the crisis response to the embassy bombings demonstrated that the U.S. is not yet sufficiently prepared to respond quickly to attacks on foreign soil; and the challenge of responding to multiple attacks is even more daunting. Contingency planning for the overseas deployment or U.S. medical, rescue, and investigative personnel was clearly insufficient. U.S. flights to Kenya and Tanzania were delayed 48 hours. There was confusion about which personnel and equipment should be transported first and three of the four flights experienced mechanical difficulties en route.

Current counter-terrorism efforts lack consistency and coherence.

The United States also needs better operational intelligence to help prevent terrorist attacks in the first place. This means improving our intelligence capabilities to identify potential terrorists, detect their plans, and to provide a basis for preemptive actions against them. James Woolsey, former Director of the Central Intelligence Agency, emphasized that there is no substitute for human intelligence, especially in an era of declining defense budgets. Such intelligence is expensive, hard to achieve, and often involves unsavory individuals—but is nevertheless essential for combating terrorism.

Having intelligence in hand, however, is only useful if the nation's leadership is prepared to act on it. In the case of Usama bin Laden, who is head of a vast global terrorist network that perpetrated the attacks against our embassies in August, the U.S. has long possessed credible and substantial information concerning his previous involvement in terrorist attacks against Americans and plans for future such attacks. For example, in February of this year, the Subcommittee uncovered a "fatwa" issued by bin Laden that called on supporters to attack Americans worldwide. And within six months, bin Laden and his followers carried out the threat by attacking our embassies in East Africa. This raises questions about how senior Administration policy makers put to use intelligence information provided to them, and whether they have identified the threshold that must be met to trigger vigorous preemptive action on the part of the United States.

The Subcommittee found a lack of consistency and coherence in the Administration's counter-terrorism efforts, especially in our dealings with the state sponsors of terrorism. On the one hand, the U.S. struck forcefully against elements of bin Laden's support infrastructure following attacks on our embassies, and is following through with arrests of key members of his organization. On the other hand, the Clinton Administration has been unwilling to confront Saddam Hussein—a principal sponsor of terrorism. While it was apparent that the chemical plant in Sudan was one source of precursor chemicals for the production of VX gas, it is may not have been the only source. A far more extensive supply and production network for chemical weapons can be found in Iraq; and yet, United Nations weapons inspectors have had their work cut short, as the Clinton Administration

has adopted a preference for avoiding confrontation. A counter-terrorism strategy that goes after the tail but leaves the body intact is doomed to fail.

No effective counter-terrorism strategy can ignore countries that provide safe haven, safe transit, and other support to terrorists. In this regard, current strategy is deficient. For example, U.S. policy toward Afghanistan, the site of extensive terrorist training camps, is woefully vague and erratic. Without the essential services and support that can be provided only by nation states, international terrorism cannot thrive. To be successful, our counter-terrorism and foreign policies must hold state supporters of terrorism accountable for their actions, and help them see that facilitating or tolerating terrorist operations is not in their interest.

Finally, as former United Nations Ambassador Jeane Kirkpatrick reminded the Committee, terrorist organizations derive their strength from the sponsorship of radical states. Accordingly, the first principle of a coherent counter-terrorism strategy is to ensure that no more governments succumb to radical, anti-western forces. (Pakistan is an immediate and pressing example of this concern.) We also need a coherent foreign policy adjunct that provides U.S. support to governments that work with us.

Subcommittee Initiatives

Based on the success in capturing terrorists through the offering of rewards, Senator Kyl is preparing legislation to increase the current $2 million limit on bounties, to provide enhanced incentives for turning in more wealthy terrorists like Usama bin Laden. The Congress also enacted an emergency supplemental request for improvements to embassy security, intelligence capabilities, and other measures needed in light of the August embassy bombings. And, as discussed later in this report, we have been working to ensure that intelligence and law enforcement agencies have the ability to gain access to encrypted communications and data so that we improve our chances of disrupting terrorist networks and defeating their plans.

FOREIGN TERRORIST ACTIVITIES IN THE UNITED STATES

Issues & Objectives

Coincident with the five-year anniversary of the World Trade Center bombing, the Subcommittee held hearings to review the status of U.S. efforts to counter foreign terrorism in the United States. Chairman Kyl sought to gain an understanding of the nature and extent of foreign terrorist activities within the United States, to serve as a basis for improving our national policies and laws to prevent, deter and, if need be, prosecute and punish terrorists.

The Subcommittee hearing on foreign terrorist activities in the U.S., held February 24, had several objectives:

- Determine the lessons learned in the four World Trade Center bombing prosecutions to build a more complete public understanding of foreign terrorist operations in the United States, including those that were involved with the World Trade Center case.

- Examine U.S INS policies to assess their efficacy in excluding terrorists from entering the United States.

- Review the effectiveness of the 1996 Antiterrorism Act, with a special focus on provisions seeking to limit foreign terrorist organization fundraising in the United States.

- Lay the foundation for the development of more effective national laws and policies.

Observations & Findings

Foreign terrorist organizations' activities in the United States continue to grow, focused mainly on recruitment and fundraising. According to the FBI, Hamas, Iranian-backed Hizballah, and Egyptian al-Gamat, all have an active presence in the United States.[14] One of most well documented fundraising and recruitment enterprises occurs in the radical Muslim community, where annual conferences held throughout the United States take in thousands of dollars that are diverted to foreign terrorist activities.[15]

Foreign terrorist organizations are active throughout the U.S.

Of note is that foreign terrorist organizations are also using the Internet to raise funds and recruit, as well as for communications. In a quick check of Internet sites, the Subcommittee located at least nine foreign terrorist organizations' homepages promoting their agenda and disseminating information, including Peru's Shining Path, the Tamil Tigers of Sri Lanka, and Hamas and Hizballah. And encryption is used by terrorists to hide data and communications. There are at least five known instances in which terrorists have used encryption to communicate and protect operational plans, including Ramzi Yousef's use of encryption to conceal his plan to blow up eleven U.S. airliners.[16] These concerns are discussed more fully in the section on Encryption Policy, below.

A second finding is that state sponsors of terrorism and foreign terrorist organizations are known to use U.S. universities as a base to educate, as well as recruit supporters and solicit money. For example, at least one Iraqi and three Iranians responsible for participating in the development of their respective countries' nuclear weapons programs were educated at U.S. universities.[17] The FBI states that there are currently a few hundred radical Iranian students in the United States who provide low-level intelligence and technical expertise to the Iranian government.[18] At the University of South Florida, a professor associated with the Islamic Jihad organized numerous "conferences" that were actually thinly disguised fund-raising efforts. At least one conference featured Sheik Rahman[19], who is now serving a life sentence for his involvement in the World Trade Center bombing.

Third, Subcommittee witnesses observed that the porosity of U.S. borders complicates our efforts to combat foreign terrorist activities within the U.S. Moreover, terrorists often violate immigration laws and procedures that we do have in place, by submitting false statements and obtaining fraudulent passports and visas. The State Department's Visa Waiver Pilot Program further complicates U.S. counter-terrorism efforts by providing opportunities for terrorists to enter the U.S. by passport alone, through any of 29 visa waiver countries where they may have entered the country fraudulently.

Clearly then, the Immigration and Naturalization Service has a central role to play in the U.S. counter-terrorism effort, but the Subcommittee found that neither the INS nor the inter-agency community has yet to fully recognize the need for INS to have a seat at the table—and funding for—counterterrorism activities. Only recently, at Senator Kyl's urging, has the INS appointed a counterterrorism coordinator. However, the counter-terrorism coordinator at the INS lacks the staff, budget, and access to intelligence and database information necessary to ensure that the counter-terrorism mission is fully embedded into its operations.

Finally, the Subcommittee found that key provisions of the 1996 Antiterrorism Act are having little effect.[20] For example, one of the best known provisions of the Act—the designation of foreign terrorist organizations to prohibit their transactions here—remains an unproven tool in the effort to curtail foreign terrorist fundraising in the U.S. No foreign terrorist assets have been seized under the new law. At the same time, it is difficult to assess what deterrent effect the law may be having. The Alien Terrorist Removal Court, created by the Act, has yet to have a case referred to it by the Department of Justice due mostly to the Court's politically controversial status and the availability of other, more traditional legal avenues.

Foreign Terrorist Organizations

1. Abu Nidal Organiz ation
2. Abu Sayyaf Group
3. Armed Islamic Group
4. Aum Shinrikyo
5. Euzkadi Ta Askat asuna
6. Democratic Front for the Liberation of Palestine - Hawatmeh Faction
7. HAMAS
8. Harakat ul-Ansar
9. Hizbollah
10. Gama'a al-Islamiyya
11. Japanese Red Army
12. al-Jihad
13. Kach
14. Kahane Chai
15. Khmer Rouge
16. Kurdistan Workers' Party
17. Liberation Tigers of Tamil Eelam
18. Manuel Rodriguez Patriotic Front Dissidents
19. Mujahedin-e Khalq Organization
20. National Liberation Army
21. Palestine Islamic Jihad - Shaqaqi Faction
22. Palestine Liberation Front - Abu Abbas Faction
23. Popular Front for the Liberation of Palestine
24. Popular Front for the Liberation of Palestine - General Command
25. Revolutionary Armed Forces of Colombia
26. Revolutionary Organization 17 November
27. Revolutionary People's Liberation Party/Front
28. Revolutionary People's Struggle
29. Shining Path
30. Tupac Amaru Revolutionary Movement

Source: State Department. Members of named groups many not enter U.S., nor transact business/solicit funds here. Contributions, business dealings with these groups are prohibited by law.

Terrorists have learned that they can exploit the blessings of our free and open society to raise money, recruit supporters, meet with their followers, and move about relatively free of scrutiny. But a free society is not defenseless in the face of terrorism. We have far reaching abilities to defeat terrorist objectives, to protect ourselves, and to seek out and punish terrorists without sacrificing our own precious liberties in the process. But in order to do this, the institutions and processes that are at issue in the fight against terrorism must have the trust and support of the citizenry.

On July 28, 1997 the Subcommittee held a hearing to examine the circumstances surrounding the interrogation of Mr. Richard Jewell, in connection with an investigation into the bombing of an Atlanta park during the Olympics of 1996. The Subcommittee found that a number of procedural irregularities raised concerns about the conduct of that investigation. The hearing also underscored a troubling climate of distrust of law enforcement officials that has emerged among some Americans, which, if not amelio-

rated, over time may have a corrosive effect on American society.

We need a society in which individual responsibility and honor, among government personnel and throughout the private sector, are taken seriously. In particular, the FBI and other government agencies entrusted with responsibility for domestic and national security must be above reproach. It only takes one or two instances of Constitutional abuse to damage public confidence in the government, or in government security programs. If government officials, from the President on down, are not held accountable to standards of personal and professional integrity, then government will lose the respect and confidence of the public, to the benefit of terrorists and others who do not wish our country well.

Subcommittee Initiatives

The Subcommittee's preparatory investigation led to several initiatives, such as production of a report included in the Subcommittee's hearing record of February 24. This report documents the limited resources available to identify and remove foreign terrorists from the U.S., while underscoring the need for the INS to take a more active role in counterterrorism strategy. The Subcommittee's urging also resulted in the appointment of a counterterrorism coordinator within the INS, as well as funding for fifteen additional INS agents to be posted at the currently existing seventeen Joint Terrorism Task Forces around the country.

The Subcommittee also examined a 1996 Congressional law[21] requiring the INS to develop a program to track foreign students entry and exit, attendance at school, and sources of funding, to ensure that the program was fully implemented. While the INS agreed in 1996 that the American public needs to know that "its government is guarding against the danger…[of] instances where terrorists and criminal aliens have been linked to student visas,"[22] the Subcommittee found that the national development and deployment of a Foreign Student Tracking Program had been cut significantly just prior to the hearing. Public airing of the issue resulted in a commitment to fully restore funding for the program, as well as a stated policy commitment to the program.

CHEMICAL & BIOLOGICAL WEAPONS THREATS TO THE U.S.

Issues & Objectives

The Subcommittee held a series of hearings and briefings in Spring, 1998 on chemical and biological weapons (CBW) threats to the United States. Hearings were held jointly with the Senate Select Committee on Intelligence, in recognition of the fact that national efforts against CBW require the highest possible degree of integration at the federal level. In addition, our joint hearings recognized that a full understanding by the U.S. intelligence community of the nature of the CBW threat to the U.S. is an essential foundation upon which national strategies and policies must be built.

We also sought to explore how the capabilities of our national security agencies, and in particular the Armed Forces, should be brought to bear in a domestic CBW crisis. As noted earlier, CBW terrorists are not our only concern. Foreign state adversaries may also resort to use of WMD. And because the Department of Defense (DoD) is charged with defending the country against external attack, and because of

the enormous chemical and biological weapons expertise resident in the military, we also wanted to consider the appropriate roles for the military and law enforcement in our national effort against CBW use. Within this broad context, the Subcommittee had a number of specific objectives.

- Assess the adequacy of U.S. policies and capabilities to prevent, deter and respond to CBW against the U.S. homeland. Does the U.S. have a national system for responding to such incidents? Are capabilities appropriately sized in light of assessed threats posed by states and non-state actors?

- Highlight the importance of improving intelligence collection and analysis of CBW threats to the U.S.

- Better understand the long-term medical consequences of exposure to chemical and biological weapons attack. This will, in turn, help Congress reach more informed judgments about needed enhancements to our public health infrastructure and national policies on the stockpiling, distribution, and use of anti-dotes and vaccines.

- Examine whether expanded legal authorities for the prosecution of CBW-related activities were desirable. The suspected anthrax incident in Las Vegas in February lent some urgency to our task.

Observations & Findings

Classified briefings from the Intelligence Community painted a sobering picture of growing proliferation networks, aggressive national CBW programs, and increasing levels of violence and lethality associated with terrorism. There is a national consensus on the growing likelihood of a CBW incident in the United States in the next ten years, but disagreement about whether a biological or chemical threat is more likely, whether a terrorist group or nation-state is more likely to use such a weapon, and whether the home-grown threat is of greater concern than the foreign threat.

Part of the uncertainty stems from the fact that too few collection and analytic resources are devoted to examining the CBW threat to the United States. Too much of the U.S. analytic effort remains focused on traditional "bean-counting," a relic of the Cold War arms control days. The Deputy Secretary of Defense recently conceded that "when it comes to chemical and biological weapons threats, we don't have an integrated intelligence assessment today, to be honest."[23] We know little about the intentions and employment doctrine of our foreign adversaries. And while the Director of Central Intelligence has warned of growing terrorist interest in CBW, we know precious little more. U.S. intelligence missed entirely the emergence of the Aum Shinrikyo cult in Japan, despite the very public anti-American rhetoric of its leader and—in hindsight—clear indications and warning of the group's intent to conduct a chemical attack.[24]

The hearings also uncovered that there are no formal processes or infrastructure to facilitate the sharing and analysis of CBW-related information among federal agencies. This situation leads to an inevitable outcome. As one witness testified, "Individually, these organizations collect data that, when viewed independently, may not provide knowledge about plans for an activity or campaign… However, correlation of diverse data sources would likely enhance our capability to identify key indicators

and provide warning.[25]"

Moving beyond the question of intelligence, the Subcommittee found that three years after President Clinton issued his counter-terrorism directive in June 1995—following the Tokyo subway attack on Oklahoma City bombing—the U.S. is still inadequately prepared to respond to a chemical or biological weapon incident. The recent release of yet another Presidential Directive (PDD-62), which principally addresses coordination for WMD contingencies, and appointment of a National Coordinator for counter-terrorism, underscore our continuing lack of preparedness.

U.S. national strategies and polices still demonstrate confusion and disagreement over basic roles and responsibilities for domestic preparedness for CBW attack. While the FBI has been placed in charge of "crisis management" of a CBW incident, expectations about the role and contributions of the Department of Defense are less well understood or articulated. DoD has been slow to embrace "homeland defense" as a core mission of the military. DoD's efforts to date to train first responders and beef-up National Guard and Reserve capabilities—which are by themselves critically important—do not appear to reflect a strategic vision of the military's role in protecting America against new threats.

U.S capabilities would be overwhelmed by a large-scale chem-bio attack.

Protocols that do exist that delineate the roles of government agencies in a CBW incident have never been exercised in a realistic manner. It is uncertain—in the absence of rigorous tests and exercises to validate established concepts of operation—whether we actually have an effective national response systems for a CBW attack against the U.S.

It also appears that U.S. capabilities would likely be overwhelmed by a large-scale chemical or biological attack or multiple incidents. The number of specialized military chem-bio teams can be counted on one hand. And they have to get to the site of the attack quickly—a truly daunting challenge without adequate advance warning. We have seen no systematic effort to develop agreed planning scenarios to guide development of contingency plans and to help identify equipment requirements.

Shortfalls in the biological weapons area are especially disturbing. Unlike the effects of chemical weapons, it may take days or weeks for us to even become aware whether a biological weapon has been used. The number of casualties from a biological weapons attack will more closely resemble a nuclear attack than a chemical attack. However, our public health infrastructure and medical communities lack resources needed to quickly detect biological weapons attack and treat victims of such attacks. Local first responders—to include FBI agents in the field—also lack equipment needed to detect, identify and monitor the presence of biological agents at the site of an attack.

Finally, witnesses testified that the existing legal regime designed to make illicit acquisition of biological weapons agents more difficult has not been fully implemented.[26] The Attorney General further recommended passage of a new law that would ban outright possession of

certain biological agents which, curiously, is not against the law today.

Subcommittee Initiatives

The Subcommittee has launched several initiatives, ranging from prevention and deterrence to the response aspects of the CBW problem.

First, Chairman Kyl asked the Intelligence Community (IC) to produce the first-ever unified intelligence assessment of the foreign CBW threat to the United States, encompassing state as well as non-state actors. He asked the IC to give special attention to adversary employment doctrine, in order better to understand how to prevent and deter CBW use. The IC tasked and produced a very insightful analysis, which hopefully will lead to future intelligence efforts to develop a validated CBW threat against which defense and preparedness programs can be measured.

Second, Chairman Kyl has been urging DoD to declare "homeland defense" a formal mission of the military, and to assign the mission to one of the Commanders-in-Chief with responsibilities for U.S. territory. Assigning the "homeland defense" mission to a senior commander means driving resource and planning decisions in the Pentagon. It is also the first step for developing a coherent view of DoD's role in defending the U.S. against CBW threats. A recent speech by Deputy Secretary of Defense John Hamre, in which he announced the homeland defense mission would be developed and assigned to a designated command in the next several months, is welcome news.[27]

Third, the Subcommittee has been pressing the Administration—with some success—to commit more funding for equipping our state and local first responders and medical communities. Congress approved in October 1998 substantial increase—measured in several hundred million dollars—for programs aimed at equipping and training firemen, police, and EMS, and for improvements to our public health infrastructure. Long overdue funding for the select biological agent transfer program was also included.

Fourth, Subcommittee staff have been working with other committees to improve coordination within the Congress and intensify Congressional oversight of our CBW preparedness. In addition to the joint effort with the Intelligence Committee, the Subcommittee worked with the Armed Services Subcommittee on Strategic Forces on oversight of the Nunn-Lugar domestic preparedness training program. Subcommittee staff also assisted the Appropriations Subcommittee on Labor and HHS in putting together a hearing on deficiencies in our public health infrastructure for dealing with CBW incidents.

Subcommittee staff have begun drafting legislation that would outlaw the possession of biological agents in certain circumstances. Currently, there are more legal impediments in this country to purchasing a handgun than acquiring deadly viruses and bacteria. Any person can legally possess these biological agents, until the government is able to demonstrate in court that the individual possesses the substance with the intent to use the biological agent as a weapon.[28]

We need to give law enforcement the authority to arrest individuals known to possess biological agents, well before they get to the point of making viruses and bacteria into weapons and threatening to use them. At the same time, the law must allow legitimate medical, re-

search, pharmaceutical use of such agents to continue. We have, therefore, been exploring an expanded registration regime that would build on existing regulations for biological agent transfer, and ensure that law enforcement authorities can quickly identify those persons engaged in legitimate biological-related activities. The objective is to bring the law on biological weapons in sync with U.S. statutes on chemical weapons required as part of the Chemical Weapons Convention.

Finally, there is a continuing need for Congress to monitor and seek to influence the development of national strategy, policies, and capabilities for combating CBW threats against the United States. In particular, this should include oversight of Department of Justice activities in this area, and the implementation of a recently concluded Memorandum of Understanding between the Justice and Defense Departments, assigning lead responsibility for WMD counter-terrorism preparedness to the Justice Department.

CRITICAL INFRASTRUCTURE PROTECTION

Issues and Objectives

The United States is the most computerized and interconnected society in the world. We have enormous military clout, and can project our national power anywhere in the world—within hours. We have a national intelligence system, designed in the wake of Pearl Harbor, created specifically to seek out indications and provide warnings that will prevent surprise attacks from occurring ever again. And we have a real-time, high-tech and global-dominating economy capable of providing all of the awesome technology and innovation that both support the comforts and conveniences of daily life and fuel our military and intelligence power.

But our economy, our intelligence systems, our military—and our very existence—are supported by a set of interdependent critical infrastructures.

Today, information systems control key aspects of our economy and society, including the infrastructures upon which our way of life and even our survival depend. The electric power grid. The public switched telecommunications network. The air traffic control system. The banking system. Rail transport. Oil and gas distribution networks. Information technologies are expanding personal and commercial freedom because of the growth in choices they bring. But the phenomenon of a national information infrastructure also presents a highly lucrative target, as more and more of the transactions vital to our national life become a part of this intricate network.

With the benefits of technological advances come a new set of vulnerabilities that can be exploited by individuals and terrorist groups as well as foreign nations. Today an enemy doesn't need to travel thousands of miles and confront superior forces in an attempt to attack the U.S. The networked and inter-related nature of our critical infrastructures means our enemies needn't risk attacking our strong military if they can much more easily attack our soft digital underbelly. Compromise of these systems -- which are principally owned and controlled by the private sector -- also brings risks to personal values of individual privacy and liberty, private property, and freedom of choice.

The merger of computers with tele-

communications has created a huge testbed for experimentation with exploitation of networked information systems: the Internet. The full range of avenues for manipulation enabled by this information web are unknown, but they include the possibilities for compromise or damage to any information system that is a part of it or is accessible through it. And because all information systems must have imbedded controls and operating systems, the possibilities for manipulation of a system once penetrated would be virtually limitless. The Internet may be a playground for creative young minds, but it also affords the opportunity for willful, hostile actors, perhaps standing behind the experimenters, to watch and learn.

In light of these concerns, in the FY 1996 Defense Authorization Act, pursuant to an amendment offered by Senator Kyl, the Congress directed the President to report on 1) an architecture for performing indications and warning of a strategic information attack on the U.S., and 2) the future of the National Communications System, (constituted by President Kennedy in the wake of the Cuban Missile Crisis to ensure enduring communications), in a era of information threats. Unfortunately, those reports were never filed.

The threat of information warfare attacks on the U.S is real and growing.

In the FY 1997 Defense Authorization Act, the Congress directed the President to develop and report on a strategy to protect the nation against information attack. At a minimum, an effective national strategy would assign responsibilities to departments and agencies, direct an architecture for indications and warning of possible attacks, and establish a decision making process integrating key government and industry actors. It would coordinate existing activities (such as the security disciplines, industrial base policy, disaster preparedness) to maximize their effectiveness, and to identify the key deltas of additional work and investment that are needed for maximum payoff. And it would ensure that infrastructure protection concerns are factored in to related national policy decisions, such as regulatory reform and encryption legislation.

In lieu of providing that report, the President signed Executive Order 13010, which created the President's Commission on Critical Infrastructure Protection. And the Congress was told that the Commission's work would provide the answers the law directed.

In a series of hearings and briefings, the Subcommittee set out to better understand the vulnerabilities of our critical infrastructures, and what the Clinton Administration is doing to protect the nation against this new category of threat.

Observations and Findings

In a joint intelligence briefing with the Senate Select Committee on Intelligence, we learned that foreign capabilities to mount information warfare attacks against the United States are real, and growing. And in a hearing held in November of 1997, General Tom Marsh, Chairman of the President's Commission on Critical Infrastructure Protection[29], painted an alarming picture of significant vulnerabilities and the ease with which our computer dependent society can be disrupted by determined adversaries.

A classified briefing on a DoD exercise named ELIGIBLE RECEIVER reinforced the point. In the summer of 1997, Joint Chiefs of Staff conducted the exercise to find out how easy it would be for an enemy to attack U.S. critical infrastructures and military computers. During ELIGIBLE RECEIVER we learned how a small team of two dozen people using readily available computer hacking tools could attack the military's critical infrastructures, and within four days, cripple our ability to respond to a simulated crisis in the Pacific Theater. The details of the ELIGIBLE RECEIVER exercise were first presented publicly in a May, 1998 briefing by the National Security Agency to the Subcommittee.

As it happened, ELIGIBLE RECEIVER became the precursor to a real world event. In the midst of our buildup to possible new hostilities in Iraq, unclassified DOD information systems came under attack during "Solar Sunrise" discussed earlier in this report. In a briefing from Defense officials, the Subcommittee learned that, for a week, the United States government was uncertain if Iraq or someone else was attacking over military computer networks. In fact, the attacks were serious enough that the President was personally briefed that the country might be under information attack.

The episode demonstrated that it is very difficult to identify, attribute and respond to cyber-attacks, and to assess whether an information attack is a crime or an act of war. Moreover, it demonstrated that we still have little understanding of whether, how and under what circumstances foreign adversaries might resort to information attacks against the United States.

It is clear that the lack of understanding and critical thinking about infrastructure vulnerabilities at the highest levels of government has meant that the U.S. has failed to develop effective strategy or policies for protecting critical infrastructures. Despite extensive work, the Marsh Commission did not attempt to address the question of national strategy. Former Senator Sam Nunn and former Deputy Attorney General Jamie Gorelick served as co-chairs of an advisory board, established to assist the President in evaluating and implementing the recommendations of the Marsh Commission report. In their March, 1998 testimony before the Subcommittee, they emphasized the need for effective national policy and strategy to meet these pressing concerns.

In May, 1998, the President signed a new Presidential Decision Directive—PDD-63—that lays a foundation for infrastructure policy development and appoints a National Coordinator for Security, Infrastructure Protection and Counter-terrorism to direct PDD-63 activities. Following on the heels of the release of that document, the newly named National Coordinator briefed the Subcommittee on the policies set forth by the new PDD, which has four main features. The PDD: (1) declares as a national goal the ability to protect infrastructures from intentional acts; (2) emphasizes the importance of public-private partnership, and directs each sector to produce a plan; (3) establishes a structure for coordination; and (4) directs NSC principals to submit a schedule to implement a national plan integrating the sector plans.

While recognizing the importance of PDD-63 to advancing national policy, the Subcommittee found that the PDD leaves a number of critical issues unaddressed:

- First, the PDD **does not address the information warfare threat**. It focuses a

great deal on criminal hackers and terrorists, but not at all on the emerging information warfare threats posed by foreign nations. From the standpoint of national strategy, there is a big difference between protecting against individual hackers and protecting the nation against a systemic attack.

- Second, the PDD **does not identify the elements of a defense** against information warfare attack, nor does it assign responsibility for such defenses. Indeed, the Defense Department is given very few duties at all.

- Third, the PDD **does not establish an indications and warning architecture** that would discern preparations for an information attack; nor does it set up a system that would detect if and when national systems were under attack.

- Fourth, the PDD **does not set up a process to identify what is critical**. Without such a process, national planners will have no basis upon which to make decisions on committing scarce resources.

- Finally, the PDD **defers virtually all of the elements** necessary to developing a national strategy for infrastructure protection to the drafting of the national plan. It remains to be seen whether the Clinton Administration's 180 day interagency effort will bring us any closer to having a strategy for infrastructure protection than the efforts of the past several years by the Marsh Commission and the drafters of PDD-63.

Clearly, development of sound national strategy and policy for critical infrastructure protection is a work in progress. And Congress will be looking for ways to help, whether in response to legislative requests from the Administration, or through its own initiatives. No one contends it will be easy. At the same time, while no nation is as vulnerable to information warfare as the U.S. because of our significant reliance on the information infrastructure, no nation is better poised to incorporate both offensive and defensive measures into its national security policy, because of our superior technology. It should be possible to develop strategy and policies that will ensure the security of American citizens from this new twenty-first century threat.

Subcommittee Initiatives

The "Solar Sunrise" incident has shown the need for legislation to make it easier to investigate cyber-attacks. During that investigation, court orders were needed in jurisdictions throughout the country in order to track the attackers. The Congress may want to consider legislation to streamline the process of obtaining court orders in multiple jurisdictions. Chairman Kyl has asked the Department of Justice to assess the need for new legislation and to provide the Subcommittee with its recommendations.

A second area of Subcommittee activity relates to the FBI's National Infrastructure Protection Center, which was established at the direction of the Attorney on February 26, 1998. The Subcommittee has been conducting oversight of this important asset as its policies, procedures and operations develop, with the objective of ensuring that the assets that the NIPC represents be put to best use, and integrated into a coherent national strategy and set of programs for information assurance.

Chairman Kyl has been promised the two reports, directed by law in the 1996 DOD Authorization Bill, which were supposed to have been supplied first, by the work of the Marsh Commission, and second, in the course of developing PDD-63 but which, in fact, remain outstanding.[30]

Finally, the Subcommittee will continue to monitor the implementation of PDD-63. As a first step, the PDD calls for the development of a national plan 180 days from signature, or roughly December 1998. Chairman Kyl has asked Administration witnesses to return to brief that plan when it is ready.

YEAR 2000 (Y2K) PROBLEM

Issues & Objectives

One of the most immediate threats to the Nation's critical infrastructures is the Year 2000 Problem (Y2K). The Y2K problem arises because many older computer systems and embedded chips record dates using only the last two digits of the year (a convention adopted to save memory). If left uncorrected, such systems could treat the year 2000 as the year 1900, generating errors or system crashes. These problems are exacerbated by broader interoperability concerns, asY2K compliant systems may interconnect with noncompliant ones. National remediation efforts, to identify date-dependent code and chips, diagnose problems, devise and implement fixes, test their efficacy, and investigate problems that may have been overlooked, have been very uneven. Many government agencies are behind schedule, which means they are likely to miss the inflexible Y2K deadline of January 1, 2000.[31] Industry estimates on remediation efforts within the United States vary widely; and it is even more difficult to assess prospective disruptions in other countries. The simultaneity characteristic of the Year 2000 -- all of these problems, large and small, converging at the same time -- introduces yet another level of concern.

In short, there will certainly be some disruptions in our lives come January 1, 2000. But it is almost impossible to predict at this time how serious these disruptions will be. At one end of the spectrum of possibilities, there may be nothing more than a collective period of inconvenience, as problems emerge and are corrected. But at the other, large scale problems with such major systems as Air Traffic Control, or the amalgamation of a great number of hardships and system failures, raise the possibility of more serious consequences for the economy, public safety and national security. We simply do not have enough good information to be able to judge how serious the problem might be.

The Subcommittee began looking at the Year 2000 Problem in late 1997, with at least three aims in mind: 1) developing a baseline understanding of the severity of the Y2K problem for individuals and for the nation as a whole; 2) raising awareness of Y2K as a national security and emergency preparedness issue; and 3) promoting comprehensive Congressional oversight of government efforts to address Y2K, especially as they impact critical infrastructure systems. We were also concerned about the possibility that efforts to fix the immediate Y2K problem may create opportunities for adversaries to gain access to and perhaps tamper with our critical computer systems. And we have considered the implications that potential Y2K litigation could have on remediation efforts.

Observations and Findings

Subcommittee investigations found that U.S. industry representatives have been frustrated with the lack of early leadership by the Executive Branch on the Y2K problem. Despite an early intense focus on other national information infrastructure issues during the first Clinton Administration, it wasn't until February 1998 that the President formed the Council on Y2K Conversion. Unfortunately, the Council may lack the appropriate staff and budget to tackle the immense task it was assigned.

Part of the job delegated to the newly formed President's Council has been to help government agencies prioritize their activities in an effort to get on track. To date, government agencies have been concentrating on remediation efforts to meet the Year 2000 deadline. But little to no attention has been paid to contingency plans to deal with Y2K related emergencies. When Chairman Kyl wrote to the newly appointed Director of the President's Year 2000 Commission to ask about emergency preparedness planning, the Director replied that FEMA was the designated agency lead. Unfortunately, the Director of FEMA reported that his agency does not have an ongoing effort focused on Y2K. In October of 1998, FEMA began to examine how the Federal Response Plan might be updated to meet Y2K generated emergencies.

The Clinton Administration was late to recognize the severity of the Y2K problem.

Private deregulated industries lack adequate industry-wide capabilities to assure that their respective infrastructures effectively transition into the 21st century. And yet, the telecommunications and electric power industries only began limited Y2K contingency planning in the Fall of 1998 and they are ahead of the rest despite expectations of looming Y2K difficulties.

Despite ongoing corrective measures, there are no guarantees that there won't be serious widespread disruptions. The probability of widespread outages may be low, but the number of code corrections and the increased potential for new software errors in the telecommunications networks are statistically compelling. If not addressed in a timely manner, the failure of embedded systems could have an equally negative impact on the electric power industry. Similar stories could be told for other infrastructure sectors.

There is a tremendous amount of frantic work going on to fix Year 2000 computer and embedded chip problems by January 1, 2000. But companies have been reluctant to provide information on their remediation efforts for fear they may be sued if what they say proves misleading or incomplete. In view of these concerns, the Subcommittee jointly with the Year 2000 Committee sponsored a series of industry briefings to gain an appreciation of their need for legislative relief.

The Subcommittee also found that both private industries' and the government's Y2K program management has failed to seriously consider the security risks associated with Y2K fixes. The subcontracting of code corrections to foreign firms and unknown sub-contractors has increased the United States' potential sus-

ceptibility to cyber attacks and information warfare attack by our adversaries.

Finally, Y2K is the first simultaneous challenge to the nation's infrastructure. How the nation handles the effects of Y2K may well be a test of our readiness to deal with the effects of an information warfare attack.

Fixing Y2K deficiencies is not a technology problem; it is a management problem. And for government, it is a leadership challenge to enhance public awareness, to ensure the readiness of emergency plans and programs to carry us through Y2K failures, and to anticipate and be prepared for the foreign policy and national security implications of Y2K disruptions.

Subcommittee Initiatives

In April of 1998, the Senate established a special committee to review the efforts of private industry and raise awareness about the seriousness of the Y2K problem. Subsequently, the Subcommittee has been supporting the work of the Special Committee on the Year 2000 Technology Problem, which is chaired by Senator Robert Bennett and includes Senator Kyl as a member. The Subcommittee has shared its expertise on infrastructure protection and information security, as well as transferred staff and resources to the Committee.

This Subcommittee continued to assist the Senate Special Committee on the Year 2000 Technology Problem in holding its first hearings on energy and telecommunications in Summer of 1998 to examine how the industry was dealing with Y2K vulnerabilities, contingency planning and information sharing.

The principal joint accomplishment to date has been the enactment of the Year 2000 Information Disclosure Act. The Act, (Pub. L. No. 105-271), enacted by Congress at the close of the Second Session, was the result of intensive government-industry work under the sponsorship of Chairman Kyl as Chairman of the Subcommittee and the Judiciary Committee representative to the Special Committee on the Year 2000. The principal purpose of the act is to ensure that concerns over liability do not have a chilling effect on sharing Y2K information essential to remediation efforts. It should not be confused with more sweeping proposals to excuse potential defendants from responsibility for their own remediation; it merely limits liability from claims arising from the good faith disclosure or exchange of information in attempts to fix Y2K problems.

The Subcommittee has been successful in stimulating other actions as well. For example, Chairman Kyl successfully pressed the FCC to re-charter the Network Reliability and Interoperability Council (NRIC) to examine Y2K. The Subcommittee has also been encouraging FEMA to develop Y2K-related emergency response plans, with mixed results. FEMA officials wrote to Senator Kyl and explained that the agency had no assessments of the electric power industry or telecommunications and were not developing any contingency planning. As a member of the President's Y2K Conversion Council, FEMA has the lead on contingency planning. FEMA officials met in July of 1998 and decided that there was no need to work on contingency plans until January of 1999, when the agency anticipates there maybe some sort of assessment on which to base its planning. FEMA has begun exploring how the existing Federal Response Plan could be employed to meet a Y2K-related emergency either at a state or national level.

Jointly with the Chairman of the Antitrust Subcommittee of Senate Judiciary, Chairman Kyl wrote to the Attorney General to request expedited consideration of any business letters seeking antitrust review of proposed Y2K information sharing. We have also requested the General Accounting Office (GAO) to survey and report on other legal issues associated with Y2K.

ENCRYPTION POLICY

Issues & Objectives

Perhaps no other issue addressed by the Subcommittee so clearly brings to the fore competing national security, public safety and privacy concerns than encryption policy.

There are two separate issues embedded in the encryption policy debate. The first focuses on a domestic matter: how do we maintain individual privacy of communication, while also maintaining law enforcement's ability to read encrypted communications when authorized by the court under constitutional authority?

The second issue has an international dimension: how do we prevent foreign countries with policies inimical to the United States, terrorist groups, and organized crime from obtaining encryption technologies that would undermine our intelligence collection efforts?

The Subcommittee held one hearing devoted especially to encryption policy; but encryption issues have arisen in nearly every Subcommittee hearing in the 105th Congress. In these hearings and related activities, the Subcommittee has sought to:

- Complement full Judiciary Committee hearings on encryption, by investigating the use of encryption by private citizens, business and government on the one hand, and by criminals, terrorists, and foreign adversaries on the other.
- Establish for the public record the views of interested parties to the encryption debate. This includes the Intelligence Community, law enforcement authorities, so-called "cyber-libertarians," the U.S. information technology industry, and business users of encryption.
- Lay the foundation for evaluating various legislative approaches for encryption policy that have been introduced, and perhaps assess the need for other approaches.
- Promote cooperation between government and industry on possible solutions.

Observations and Findings

Subcommittee hearings highlighted how encryption technology is vital for protecting personal and commercial data. People need to be able to operate information systems with ease, and with confidence that their privacy is secured. The government needs to have secure systems, to protect sensitive information and national security communications. And our nation's critical infrastructures need to be protected, in light of growing "information warfare" threats from hackers, terrorists and foreign governments.

However, unbreakable code in the hands of criminals adds a terrible tool for unlawful acts. If the U.S. does nothing to properly control unbreakable code, Americans increasingly will be victims of unsolvable crimes. Today, organized crime and drug cartels are sophisticated users of computers, and increasingly are turning to encryption to hide their unlawful activities. For example, the Subcommittee learned that an international terrorist, who was plotting to blow up 11 U.S. airliners, recorded his terrorist plans on his laptop computer files -- which were encrypted. A multi-state gambling enterprise used encryption to hide its records of the daily take on bets, payoffs, and accounts due. A major international drug lord recently used encryption to frustrate a court-approved wiretap. And the numbers of criminals using encryption are doubling each year.

U.S encryption policy must not be a zero sum game.

In the course of our hearings into encryption policy, we heard from law enforcement agencies across the country. They are in unanimous agreement that the widespread use of encryption ultimately will devastate our ability to fight crime and prevent terrorism, unless we have built in public safety features into encryption products or architectures.

The Subcommittee's work de-bunked the myth that giving law enforcement the ability to gain access to encrypted communications or computer files provides the U.S. government *carte blanche* to violate an individual's right to privacy. It is clear that a system to permit law enforcement access *only* upon a court's authorization would maintain today's stringent constitutional safeguards. Contrary to popular opinion, the U.S. government does not listen in on the communications of Americans. Wiretaps are strictly controlled and scrutinized by the Courts, as would be authorizations for access to coded communications.

In the international arena, the Subcommittee learned that foreign adversaries may acquire U.S.-made encryption technologies, due simply to the success and global market dominance of the U.S. software industry. This, however, poses a significant challenge to our intelligence community, which relies heavily on signals intelligence to detect terrorist preparations, proliferation networks, and other politico-military developments. High-tech encryption tools, in the wrong hands, could defeat our intelligence gathering capabilities.

It will clearly be a struggle to keep foreign sources of encryption from falling into these hands. But equally clear, the United States has a national security interest in carefully managing and controlling exports of high-tech encryption technologies. The Clinton Administration's recent decision to lift export controls over many categories of encryption products was distinctly unhelpful to efforts to achieve an overall balanced policy. We also need more industry leaders who understand that the strength of America's defenses are vital to our freedoms as well as to their bottom line.

As Chairman Kyl said in an address to the Heritage Foundation, "such important policy decisions must not be cast as a zero-sum game. I am convinced that we can -- and we must -- develop policies that support each of the several vital goals we have at stake, as individuals, as a community, and as a nation."

Subcommittee Initiatives

Chairman Kyl and Subcommittee Ranking Member Senator Dianne Feinstein have been working to bring together senior law enforcement officials, intelligence community representative and industry CEOs and CIOs to help broker a solution acceptable to all parties. Chairman Kyl has offered a framework to industry to counter the "genie is out of the bottle" approach to the encryption issue.

The "genie premise" is that encryption software is free and widely available (PGP being the most frequently cited example), rendering moot any attempt to impose controls over its transfer, manufacture or use. Yet at the same time, manufacturers and sellers of products with encryption features argue that they are losing market share to foreign competition because of export controls. Which raises the question: if users can simply download encryption software for free, why is there still a market for American products with encryption features?

The answer must be that the demand for American products is based on something more than encryption features alone. If that is true, it implies the possibility of addressing the needs of law enforcement without jeopardizing market share. In that regard, Chairman Kyl offered a model of the domestic market for information security solutions. The proponents of domestic controls may have done a disservice in focusing on a one-size fits all technical solution such as "key recovery." Such a focus limits the search for acceptable solutions to the cryptography—without due regard to the reality that cryptography is just one piece of the information security puzzle. Chairman Kyl's framework suggests that discrete applications and user groups must be addressed individually, providing an opportunity to identify promising technical solutions for accessibility where and when it is most useful.

The Subcommittee has also produced two reports on national encryption policy issues. One describes in considerable detail the principal issues of the encryption policy debate and provides an assessment of some of the policy and other solutions that have been proposed. The second report critiques a study by the National Research Council, examining proposals to develop a key management recovery infrastructure.[32] Both reports have been distributed to Congressional Committees examining encryption issues, and to other interested parties.

SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION HEARINGS HELD DURING THE 105TH CONGRESS

Date	Topic
March 19, 1997	"Internet Crimes Affecting Consumers"
July 28, 1997	"The Internet Gambling Prohibition Act of 1997"
July 28, 1997	"Interview of Richard Jewell in connection with the July 27, 1996, bombing at Centennial Olympic Park in Atlanta"
Sept. 3, 1997	"The Encryption Debate: Criminals, Terrorists, and the Security Needs of Business and Industry"
Nov. 5, 1997	"The Nation at Risk: The Report of the President's Commission on Critical Infrastructure Protection"
Feb. 24, 1998	"Foreign Terrorists in America: Five Years After the World Trade Center Bombing"
March 4, 1998	"Biological Weapons: The Threat Posed by Terrorists" with the Select Committee on Intelligence.
March 17, 1998	"Critical Infrastructure Protection: Toward a New Policy Directive"
April 6, 1998	"Meth: Our New Deadly Neighbor" field hearing in Phoenix, AZ
April 16, 1998	"Law Enforcement Needs in Indian Country" field hearing
April 22, 1998	"Chemical and Biological Weapons Threats to America: Are We Prepared" with the Select Committee on Intelligence.
May 20, 1998	"S. 512: Identity Theft"
June 10, 1998	"Critical Infrastructure Protection: 'Eligible Receiver' and the new PDD"
Sept. 3, 1998	"U.S. Counterterrorism Policy" (chaired by full committee)
Oct. 8, 1998	"National Security Considerations in Asylum Applications: A Case Study of 6 Iraqis"

Please refer to the Subcommittee website (www.senate.gov/~judiciary) for additional information.

CITATIONS

[1] COMMISSION TO ASSESS THE BALLISTIC MISSILE THREAT TO THE UNITED STATES, EXECUTIVE SUMMARY PURSUANT TO PUBLIC LAW 201 104TH CONGRESS (JULY 15, 1998).

[2] SUBCOMMITTEE ON INTERNATIONAL SECURITY, PROLIFERATION, AND FEDERAL SERVICES, COMMITTEE ON GOVERNMENTAL AFFAIRS, A MAJORITY REPORT, THE PROLIFERATION PRIMER (JAN. 98).

[3] BRIAN JENKINS, THE POTENTIAL FOR NUCLEAR TERRORISM 8 (1977).

[4] See JAMES K. CAMPBELL, WEAPONS OF MASS DESTRUCTION TERRORISM (1997), for a thorough discussion of the phenomenon of "post-modern" terrorism.

[5] See Threats to U.S. National Security: Hearing Before the Senate Select Comm. on Intelligence, 105th Cong. (Jan. 28, 1998).

[6] The Identity Theft and Assumption Deterrence Act, S. Rep. No. 105-274, 105th Cong. (1998).

[7] Oversight of the Department of Justice: Hearing Before the Senate Judiciary Comm, 105th Cong. (July 15, 1998).

[8] Threats to U.S. National Security: Hearing Before the Senate Select Comm. On Intelligence, 105th Cong. (Jan. 28, 1998) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation).

[9] See REPORT OF THE NATIONAL DEFENSE PANEL, TRANSFORMING DEFENSE, NATIONAL SECURITY IN THE 21ST CENTURY, (DEC. 1997) which highlights the need for increased attention to "homeland defense."

[10] GENERAL ACCOUNTING OFFICE, COMBATING TERRORISM: SPENDING ON GOVERNMENT-WIDE PROGRAMS REQUIRES BETTER MANAGEMENT AND COORDINATION, GAO/NSIAD-98-39 (DEC. 1997).

[11] Terrorism War Spawns Silence, USA TODAY, Sept. 23, 1998, at 1.

[12] Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, 108 Stat. 1796 (codified in scattered sections of 18 U.S.C.), 18 U.S.C. 2332a Use of weapons of mass destruction (1994).

[13] U.S. Counter-Terrorism Strategy: Hearing Before the Senate Judiciary Comm, 105th Cong. (Sept. 3, 1998) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation).

[14] Foreign Terrorism in the U.S.: Five Years After the World Trade Center: Hearing Before the Senate Judiciary Subcomm. on Technology, Terrorism, and Government Information, 105th Cong. (Feb. 24, 1998) (statement of Dale L. Watson, Section Chief for International and Naturalization Service).

[15] See generally Watson, supra note 14; PBS Documentary, Jihad in America, 1995, SAE Productions; U.S. Counter-terrorism Policy: Hearing before the Senate Judiciary Committee, 105th Congress (September 3, 1998) (Statement of Louis Freeh, Director, FBI).

[16] DOROTHY E. DENNING AND WILLIAM E. BAUGH, JR., ENCRYPTION AND EVOLVING TECHNOLOGIES: TOOLS OF ORGANIZED CRIME AND TERRORISM WGOC MONOGRAPH SERIES (1997).

[17] HILLARY MANN, OPEN ADMISSIONS: US POLICY TOWARD STUDENTS FROM TERRORISM-SUPPORTING COUNTRIES IN THE MIDDLE EAST, RESEARCH MEMORANDUM, NO. 34, 1 THE WASHINGTON INSTITUTE (SEPT. 1997).

[18] Watson, supra note 14.

[19] Foreign Terrorism in the U.S.: Five Years After the World Trade Center: Hearing Before the Senate Judiciary Subcomm. on Technology, Terrorism, and Government Information, 105th Cong. (Feb. 24, 1998) (statement of Steven Emerson, The Investigative Project).

[20] Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, 110 Stat. 1248 (1996).

[21] Program to Collect Information Regarding Foreign Students and Other Exchange Program Participants 8 U.S.C. § 1372 (1996).

[22] THE TASK FORCE ON FOREIGN STUDENT CONTROLS, U.S. INS, PRINCIPLE PAGE, FINAL REPORT ON CONTROLS GOVERNING FOREIGN STUDENTS: AND SCHOOLS THAT ADMIT THEM, FINAL REPORT, (DEC. 22, 1995).

[23] John J. Hamre, Deputy Secretary of Defense, Remarks at Defense Special Weapons Agency Annual Conference on Controlling Arms (June 11, 1998).

[24] See William Broad, How Japan Germ Terror Alerted World, N.Y.Times, May 26, 1998 at A1.

[25] Chemical and Biological Weapons Threats to America: Hearing Before the Senate Judiciary Sub-comm. on Technology, Terrorism, and Government Information, 105th Cong. (Apr. 22, 1998) (statement of Donald C. Latham, Member of the Defense Science Board).

[26] Antiterrorism and Effective Death Penalty Act of 1996 Pub. L. No. 104-132, 110 Stat. 1284, §511 (e) Regulation of Transfers of Listed Biological Agents (1996). See also Additional Requirements for Facilities Transforming or Receiving Select Agents, 42 C.F.R. pt. 72.6 (1996).

[27] Hamre, supra note 23.

[28] Biological Weapons Anti-Terrorism Act of 1989, Pub. L. No. 101-298, 104 Stat. 201 (1990).

[29] THE PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION, REPORT ON CRITICAL FOUNDATIONS, PROTECTING AMERICA'S INFRASTRUCTURES (OCT. 1997).

[30] Letter from Sandy Berger to Jon Kyl (Feb. 9, 1998).

[31] U.S. OMB, PROGRESS ON YEAR 2000 CONVERSION, 6TH QUARTERLY REPORT (AUG. 15, 1998).

[32] STAFF OF SENATE COMMITTEE ON THE JUDICIARY, SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION, 105th CONG., 1st SESS., REPORT ANALYSIS ON ENCRYPTION 'RISKS' REPORT, (OCT. 1, 1997)