The Terrorism Threat and U.S. Government Response: Operational and Organizational Factors

Edited by

James M. Smith

and

William C. Thomas

INSS Book Series

March 2001

Published by

USAF Institute for National Security Studies

US Air Force Academy, Colorado

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
00Mar2001	N/A	-

Title and Subtitle The Terrorism Threat and U.S. Government Response: Operational and Organizational Factors	**Contract Number**
	Grant Number
	Program Element Number
Author(s) James M. Smith, William C. Thomas	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) USAF Institute for National Security HQ USAFA/DFES,2354 Fairchild Drive, USAF Academy, CO 80840 Studies, US Air Force Academy, CA	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes ISBN:0-9710900-0-9	
Abstract see report	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** SAR
Number of Pages 212	

The USAF Institute for National Security Studies

The dual mission of the USAF Institute for National Security Studies is *to promote national security research for the Department of Defense within the military academic community and to support the Air Force national security education program.* INSS coordinates and focuses outside thinking in various disciplines and across services to develop new ideas for USAF and DOD policy making. Located within the staff of the Dean of the Faculty at the USAF Academy in Colorado Springs, INSS is an independent research center supported by various DOD organizations. In addition to the USAF Academy Dean, the primary INSS sponsor is the National Security Policy Division, Nuclear and Counterproliferation Directorate, Headquarters US Air Force (AF/XONP). The Institute helps to develop research topics, select researchers, administer sponsored research, and host conferences and workshops that facilitate the dissemination of information to a wide range of private and government organizations. Its research centers on arms control, proliferation, regional security, environmental security, information operations, Air Force policy, and space policy.

You can reach INSS at 719-333-2717, or write to the USAF Institute for National Security Studies, HQ USAFA/DFES, 2354 Fairchild Drive, Suite 5L27, USAF Academy CO 80840.

March 2001

ISBN: 0-9710900-0-9

The Terrorism Threat and U.S. Government Response: Operational and Organizational Factors

Contents

Foreword: Twenty-First Century Terrorism

Bruce Hoffman

It is impossible to talk about 21st Century terrorism without first discussing some of the changes we see occurring in terrorism today. Here I think there are five key points that we have to think about regarding the stereotypical terrorists in the past compared to terrorists today.

- First, terrorists today are not part of defined organizational entities with visible and discernible command control apparatuses. Rather, what we see are more amorphous, less distinctive organizations.
- These organizations are not organized as hierarchical, pyramid-shaped structures, identified by their leader or commander-in-chief at the top. They are much flatter organizations, along the lines of networks or organizations that function much more competitively. You can see the difference today as we try to get our arms around Al-Qaeda, the organization—or maybe the movement—associated with bin Laden. Compare it with more stereotypical terrorist groups of the past. We knew who the leaders of the Red Army Faction were—Andreas Baader and Ulrike Meinhof. In fact, we generally referred to the group as the *Baader-Meinhof* Organization after its leaders. Similarly, few people called the *Fatah Revolutionary Council* by that name; instead, we called it the *Abu-Nidal* Organization. These groups were distinct entities with leaders.
- Also, we knew what they wanted. We may not have agreed with them. We may have found their aims and objectives heinous, objectionable, intolerable, but at the same time, at least we could understand what they were about. We knew what motivated them, what their aims were, how they dovetailed their actions to suit their agendas, and we had a sense of what they wanted and who they were.
- Also, what we see today is groups that have been changed. As the stove-piped command-control apparatus or structures have eroded, groups feel that in their independence they are more able to carry out ambitious types of operations. Essentially you see a greater willingness by groups to inflict massive indiscriminate casualties. You have to pause here and think for a moment, go back to the bombing of the World Trade Center in 1993. Now, putting aside whether it was possible to actually topple the North Tower onto the South Tower and kill 60,000 people, consider the goal. Just pause to compare that to the previous decade, to heinous acts of international terrorism—committed by the sorts of guys we thought were the really bad terrorists, public enemies number one, such as Abu-Nidal, Baader, Meinhof, and others. Very rarely, if at all, do we have evidence of these groups contemplating World Trade Center types of very grand, very ambitious terrorist events. They planned incidences of hijacking, planted bombs on planes, but still those types of things would kill at most in the low hundreds, and more likely, only a handful of deaths. They weren't contemplating incidences of violence that were expected to kill tens of thousands. So that is an important difference too.
- Finally—and I think this is a fundamental point— groups today claim credit less frequently than they did in the past, for a variety of reasons. For some groups, terrorism is less of a means to an end than an end itself, serving God or the cathartic self-satisfaction of striking a blow against the hated enemy, for example. Violence is less tailored and as the violence has become more indiscriminate, the terrorists themselves have become more reluctant to claim credit for events. Compare this to the 1970s and 80s. Terrorists routinely were proud when they carried out an operation. In fact, they told us that they did so. They issued communiqués. They not only told us what they did, but often in turgid, overwrought, agonizing, complex prose, explaining exactly why they did it. Think back a few months ago to the assassination of a labor leader in Italy by a group reviving or resuscitating the Red Brigade (a group assuming the Red Brigade's mantle). The *modus operandi* was the same—a selected and directed discriminate act of violence committed against one individual, then a claim of credit saying that they did it, followed by a 28-page diatribe or treatise explaining exactly

why the organization carried it out. Now compare that with some of the most significant and spectacular terrorist acts of the past decade, such as PanAm 103, the bombing of the Jewish Community Center in Buenos Aires in 1994, the attack on the Tokyo subway in 1995, the bombing of the Alfred P. Murrah office building in Oklahoma City in 1995. None of those incidents have had credible claims attached to them. No group or individual has come forth to claim responsibility. Although in some of the cases we know who is responsible, there have been no claims made, not in the sense that was common practice in earlier eras of terrorism. So that is one set of big changes.

The second set is that these changes are affecting the operations, organizational dimensions, and even the targets of terrorism, as well. Terrorist groups in the past were, for want of a better word, numerically constrained. Let's talk about organizations that were notable. The Red Army Faction, throughout its twenty years of existence, never varied from having more than roughly 25 to 35 hard-core members. The West German police would sweep up one generation by displaying "Wanted" posters with about twenty faces, and a few years later you'd see another twenty faces. The faces changed, but the numbers never got larger. The Red Brigade, at its high point, was slightly larger, with 75 persons. But to get to larger terrorist groups, you have to look at the IRA, with estimates suggesting that membership was about 400 hundred— that is members who were trigger-pullers, bomb throwers, and active terrorists. Or you can look to the Fatah Revolutionary Council, which was estimated to have in excess of 500 members in the 1980s. And, we saw that as terrorist groups with stereotypical structures grew too large, there were lots of problems. How many books have appeared in the recent past by ex-IRA leaders, telling of traitors who started to forsake terrorism and people who couldn't be trusted. The Red Brigade has similar stories. While the Fatah Revolutionary Council, Abu-Nidal's organization, was the biggest of its era, there were two major fratricidal, internecine blood-lettings. As the group got larger, the disputes got bigger and essentially the group turned inward on one another other. That is what undermined the organization and made it less of a threat. Compare that to today, when it is very difficult, if not impossible, to get a bearing on how many people are members of Al-Qaeda, maybe 4000? 5,000? Is it less? Is it more? What we are talking about is a different type of process, a different type of terrorist, and different type of group.

Another difference is that in the past, operations were directed against a comparatively narrow target set. Left-wing terrorists would target government officials, capitals of industry, bankers—people who they blamed for the wrongs of the system. The nationalist terrorists would target government officials, representatives of the state, policemen, or members of rival communities. But the violence was still largely constrained and fairly narrowly focused.

And then the last change. In the past, terrorists operated out of a set of defined sanctuaries or safe-havens and engaged in activities within a somewhat limited area of operations. For example, Middle Eastern terrorists would largely travel from the Middle East and carry out international terrorists acts predominately in Europe, very rarely in Latin America, for example. We knew where the terrorists were based, we knew how they were trained, what their capabilities were, essentially what their aims were—we could more-or-less reach out and touch them. Compare that to today and what is happening as the terrorist sanctuaries are destroyed or disappearing. Of course, the collapse of the Soviet Union was the first step, but now, with countries like Libya moderating their policies and other countries, such as Afghanistan, with an uneasy form of government, decreasing their safe-havens—even the Taliban has engaged in some discussions with the U.S. with regard to bin Laden—terrorist sanctuaries are disappearing.

All of these changes and the decline in safe-havens does not mean that terrorism is going to go away anytime soon. It does mean it will change. What we see is that in the past, the terrorist threat was at least palpable. We knew what it was, where it was coming from, who was doing it, and what they wanted. And, needless to say, we never had to worry about the prospect of terrorist use of chemical or biological weapons. What they were doing was essentially of limited consequences and effects. You could anticipate them, and their violence was kept within bounds that were acceptable.

I would argue that the changes that we see will not only continue but grow. Terrorists are like sharks in

water; if they stop, they do not succeed. Terrorists always have to stay one step ahead of what their enemies are doing and one step ahead of the counterterrorism technology curve. If they do not stay ahead, they are not going to succeed. And if they do not succeed they will not achieve their objectives. As I said, diminishing sanctuaries does not mean that terrorism is going away. Rather, I would argue that if the terrorists don't have a safe place to hide out in any more, they are going to burrow themselves deeper into worldwide networks. We already see this to an extent occurring throughout the world, in bin Laden's organization, for example. One of the persons under indictment in New York is a U.S. citizen, a resident of Texas. Another bin Laden follower is a resident of West Virginia; another was a member of the U.S. Army. And it is not only bin Laden's organization. Groups like the PKK and the Liberation Tigers of Tamil Eelam are spreading throughout the world. As they lose their traditional sanctuaries, they are turning to transnational communities where they are burrowing themselves and using the community as almost a remote base of operations, rather than having a set base in one part of the world, as was the case in the past. Associated with this, these groups are relying increasingly not just on the professional hardcore terrorists but a much broader network of amateur terrorists, activists, lackeys, helpers, sympathizers, and supporters.

With the lack of bases and lack of patrons, these groups are turning increasingly to crime and towards greater involvement with formal criminal links—not only as a means to raise money to sustain operations but also as a means to increase patronage and increase their hold over transnational communities. In other words, it is like the old style bosses in the U.S. at the turn of century. When immigrants came off the boat, they were met by a political machine that gave them jobs and in return got their votes. The same sort of process is occurring in these transnational communities. These organizations are giving individuals work, in both the legal and illegal sectors, and they are winning their allegiance and winning their support. These groups are consciously reversing the pattern of immigrants who came to a country and sought the melting pot, sought to be absorbed, to become more American than Americans. These organizations, as a means both to prey upon and keep their control over the community and to enhance their patronage, are actively working to erect barriers to prevent people from integrating into society. We see how the more adept groups of this sort are able to generate an income stream, estimated to be between $1 million and $3 million per month. So, bin Laden is not the only sugar daddy, not the only revolutionary philanthropist out there. Many of these organizations, the PKK, the Tamil Tigers, and others have incomes estimated in this range from both illegal and "legal" activities.

I think in terms of the changes we will see, the impact of diminishing sanctuaries, greater involvement in crime, and high-income streams will be very profound. But when we look at the types of weapons and tactics terrorists will use, we have to be more careful. Terrorists, as radical as they may be politically, are just as conservative operationally. They want to succeed; they have to succeed. For that reason, they rarely deviate from established patterns and therefore stay within a fairly narrow tactical repertoire. They use what they have high confidence in, things they know will work, with only minor deviations. Larger and more powerful car and truck bombs have been about the only innovation in recent terrorist acts.

I think the next step up from car bombs, as we harden embassies and other likely terrorist targets and make it more difficult for terrorists to reach out and strike at the targets they traditionally hit by car/truck bombs, they will need to turn to alternative weapons. They are not going to lay down their arms and give up, so they will find other weapons and tactics and means to reach their targets. And here is an obvious class of weapon choices: ultralights, UAVs, all types of distance and stand-off weapons, surface-to-air missiles, rocket-propelled grenades fired from a distance, remote control mortars, and Man-Portable Air Defense Systems (MANPADS). Rather than saying that these are tactics or weapons that terrorists will use, I believe terrorists are experimenting with these types of weapons today and perfecting them for use.

Then there is the whole issue of chemical, biological, and radioactive terrorism. Why the interest now? Given the whole past patterns of terrorist activity and their mindsets, I think it is likely that we will see some act involving these types of unconventional weapons within the next five years. But there are two important caveats. One, it is not going to be the type of destruction of entire cities and mass havoc we anticipate. Rather, I think it will have more in common with the 1995 attack on Tokyo's subway—an unsuccessful, even discrete

and limited attack that, nevertheless, had profound and far reaching psychological repercussions.

Would terrorists resort to the indiscrete use of weapon of mass destruction (biological) when a far more limited discrete use of a chemical weapon, which is easier to fabricate and release, can achieve the same end? I have no doubt that terrorists would want to cross to weapons of mass destruction (especially biological and radiological) and investigate this new form of violence. But I think we have to look back to the past to see that even if terrorists have motivation to use this type of weapon, there are formidable technological barriers that, at least for now and perhaps in the near future, will constrain them from doing so. Look at Aum Shrinkyo. Aum was not a stereotypical terrorist organization. It was a national industry with membership estimated at up to 50,000. It was not one of the organizations operating on a shoestring budget; Aum assets were estimated to be as high as $1 billion. We are not talking about terrorists who sat in back rooms of tenements and basements, making pipe bombs. These people were fitted out with state-of-the-art war tools, the best tool-and-die machines that could be purchased. These weren't people with just a modicum of experience, a high school education that they brought to bear in making bombs with all kinds of improvised explosives. Instead, they were deliberately recruited, the cream of the Japanese intelligensia, the cream of the Japanese scientific and engineering community, the best people they could find. So, you had a group with enormous resources, and with all those resources the group embarked on an attempt to use biological weapons. And it failed miserably. Not only was Aum reduced to using sarin, a chemical weapon, but look at how they used it. Can you imagine a less sophisticated attack than putting sarin in plastic trash bags and wrapping it in newspapers? This is not to say that our concern about terrorists use of these weapons is misplaced or unfounded. It is only to say that terrorist ability to utilize or operationalize them is still difficult. For that reason, when we see terrorist use of these weapons, they will most likely use the simplest ones—which are chemical weapons—and the devastation will probably be on a much more limited scale than predicted today.

The changes that we see, though, in terms of weapons and tactics, will extend beyond group imperatives and beyond even the outright use of violence to different tactics, such as non-violent tactics and the increasing use of information to thwart counterterrorist techniques. There has been a tremendous amount of focus on destruction of systems, on paralyzing cities, shutting down air traffic control, and so on. But the point is terrorists are success freaks. They need intelligence; they are intelligence freaks, as well. If they can get into a system and mine that system to get information to facilitate their conventional paths, that is exactly what they are going to do. The pattern of terrorism in the past bears this out. The IRA, for example, was able to get onto a main computer. Instead of shutting the system down, they used it to get information on home addresses of policeman, politicians, and prison guards. In short, they extracted information that they could use for conventional operations. Other terrorists might get this information and shop it and sell it to other people who might find it useful to buy as a commodity. It is also instructive to note that two years ago, when the IRA wanted to black out London, wanted to shut down the entire city, they didn't recruit hackers, they didn't resort to trying to penetrate the system electronically. They got together some good old fertilizer for the public libraries, the plants, the switching stations and transformers around London, and set about making bombs. They intended to drive around that night and blow them up systematically. So, it is not to say that information age warfare is not a threat. But, we have to think that the terrorists will use it first to get information, not necessarily to destroy it—and, of course, as we see now, to spread the word. You just have to go on the Net to see that. My students used to give me a list of 40 or 50 sites that virtually every terrorist in search of national liberation would use. The Net to them is useful. They want to exploit it; they want to keep it up and running because that is how they are getting the message across. That is one thing.

The second issue, tied to the transnational communities, is the increasing emergence of above-ground support groups who engage in intensive lobbying and political pressure as a means of legitimization, to enhance the stature of these groups, as a means of PR to try to convince countries that the groups are not terrorist organizations. They also use it as a means to harass their enemies or any government that takes action against them. They use legal means to strike back. We see this happening now in Washington, where the group *Mujihadeen* and the Liberation Tigers of Tamil Eelam are suing the United States government in the District Court to be taken off the list of thirty organizations designated as terrorist by the Secretary of State in October

1997 that are prohibited from fund raising in the United States.

Finally, we'll see greater networking and help provided to other terrorists and criminal groups. Increasingly, we are seeing weapons used by terrorists, in say, South Asia turning up in Lebanon, in turn Israel, also in Turkey. These groups are sharing their weapons, their expertise, and they are also attempting to leverage off the transnational lines of communication of other communities or other groups.

So, when one sees this picture, we come to the conclusion that it is a different type of terrorism. Military force and economic sanctions—two weapons and two means traditionally relied upon—are going to be of fairly limited use against these amorphous, stateless, transnational groups. I think this is already borne out by the bombings of the U.S. Embassies in Tanzania and Kenya, which I think underscore how terrorism is very much a highly dynamic phenomenon, constantly changing and evolving in order to obviate or overcome the security measures and physical barriers placed in their path. So terrorists who want to attack an embassy are not necessarily going to be deterred by a large setback, such as buildings far from the street. Rather with larger and more exponentially powerful bombs they have and will be able to overcome that setback and still take down buildings and commit their acts. Or, as I said earlier, if we prevent the use of car/truck bombs, the terrorist will find other means to carry out these missions, as borne out in East Africa.

Similarly, the retaliatory U.S. cruise missile attacks demonstrated the difficulty and complexities in countering terrorism, in responding to terrorism. The results showed that when force is used, sometimes the repercussions cannot be anticipated but can prove to be counterproductive. By this, I'm talking about the lionization of bin Laden that followed the attacks and the shift away from the victims and the targets of bin Laden's attacks to the target or victims of our retaliatory strikes. And what this new dynamic or this new calculus suggests is the need for innovative full-capacity responses that do not follow just one path but meld together different strands into a coherent strategy. This process begins with the realization that terrorism is not a phenomenon amenable strictly to military solutions alone.

Military force has a part to play, but it can not be seen as the be all and end all. In this sense, we need to understand better what force can and cannot achieve. To do this, we do not have to go back to 1998; we can go back thirteen years ago to another case where military force was used in response to terrorism. I am not making a judgement about whether military force should or should not be used, but I am trying to assess the effects of it. The 1986 air strike on Libyan forces was widely touted and believed to be an archetype of success of using flying forces against terrorists. I would argue, however, that this is one example where we may have felt good and indeed it may have sent a powerful message, but in point of fact it had little if any discernable effect on the terrorists or their patrons. Libyan terrorism afterward not only continued, but escalated. According to statistics that we keep at RAND, in the year following the 1986 air strike, Libya was identified as responsible for at least fifteen acts of state-sponsored terrorism, many of which were directed against the U.S. and against Britain as punishment for having allowed U.S. jet fighters to take off from British bases. Not only that, but Qaddafi actually escalated his support for terrorism. Libya went out and got some hired guns, the Japanese Red Army faction, who he paid to carry out attacks on behalf of Libya in retaliation for the U.S. air strikes. It also shows how much terrorism has changed today from then. When the Japanese Red Army (JRA) engaged in these attacks, they did not say the JRA did it, they said the AAIB (Anti-Imperialist International Brigades) carried out the attack. This was a sort of shorthand at the time, so we would have a pretty good idea who was behind JRA in the operating capacity. Not only did Qaddafi go out and get hired guns, but he also escalated Libya’s attacks. In 1987, he attacked U.S. and British diplomatic facilities in Spain and Indonesia. In 1988, Qaddafi upped the ante. He sent a Japanese Red Army terrorist, Yu Kikumura, to the U.S to carry out an attack that was supposed to coincide with the second anniversary of the U.S. bombing. Five years before the World Trade Center bombing, Kikumura’s orders were precisely to go to the financial center of New York. When he was arrested on the New Jersey Turnpike, officials found in the trunk of his car several hollowed-out fire extinguishers that contained not only black powder but roofing nails, crude antipersonnel devices. That same day that the attack was scheduled to go off, a car bomb exploded outside a USO club in Naples, Italy, killing seven persons. So Qaddafi did not stop. Not only that, as punishment to Britain, he began to ship an estimated 140 tons of arms to

the IRA. Finally, in terms of having deterrent effects on other groups, the evidence is also marginal. During the six months before the U.S. retaliatory strike, there were 41 terrorist attacks on U.S. targets; in the six months afterwards, there were 54. Thus, the actual cause and effect was reversed even on other terrorists groups; the deterrent value was not evident, against Libya or other terrorist groups.

Then there is another problem—inflicting collateral casualties. During the U.S. air strikes, despite our best efforts to avoid civilian casualties, none-the-less and tragically, 36 Libyan civilians were killed and 96 others were wounded. Terrorism is predominantly psychological warfare. What we do by inflicting collateral casualties is to automatically hand over to our enemies the fodder to vilify or attack us, just as we did recently. We become the problem, not so much the terrorists. Also, from a moral standpoint, innocent civilians are innocent civilians, whether they are Americans or Libyans. If we are going to retaliate, if we are going to maintain the moral high ground against terrorists, we have to be careful and ensure we do not inflict collateral casualties. All of this is to say, not that we should not use military force, it is to say that by itself it cannot be the only solution.

That does not mean we have been able to come up with many other better solutions, because other non-military responses have had equally mixed results—economic sanctions, for example. Certainly Iraq is a case in point, where the effect of sanctions has not been what we hoped. Arguably, they have had little effect on Iran after more than 20 years. This is a major issue of debate between the U.S. and its European allies. Europeans say that their positive and constructive engagement in critical dialogue is more likely to win Iranians over than the U.S. hard-line and sanctions. I am not sure about that, but U.S. economic sanctions have not lived up to their expectations. Even the recent developments in Libya are not clear-cut evidence of the value of sanctions, but may be more of a reflection of Qaddafi's weakness. He is not the main player in the Middle East. Moreover, Libya is a fairly isolated, weak country itself, and not a major player or renegade in Middle Eastern politics. Sanctions might work, but they are not an immediate solution. And then, in my book, I cite a 1997 State Department analysis where the intelligence community itself was dismissive of the effects of economic sanctions. Not one of the countries listed on the U.S. State Department's list of state sponsors has ever reneged or declared publicly that they will no longer engage in terrorism.

Given this state of affairs, what does one do? How do you respond to terrorism? The first step is to realize and accept the limitations of military force against terrorism in strategic terms. Military force certainly does have a place but probably more at a tactical rather than strategic level. Sometimes military force is the only and perhaps the best way to communicate a specific tactical end, e.g., disrupt a plot, sabotage a pending attack, damage logistical support networks, and others—it certainly has a place there. But as a strategic tool, having an overall effect on the problem, the phenomenon, its effects are less clear. We see that military force's real utility is in containing control of the pattern, not solving it. I think we have to conclude that there is no one ultimate solution to terrorism. There can certainly be improvements in human intelligence, international cooperation, and strengthened responses to make it more difficult for the terrorists to operate, but that by itself is not going to stop them. To do so, what we need is to use military forces as part of a broader framework, a comprehensive plan, an overall approach that harnesses force and uses it alongside other practical non-lethal approaches. History repeatedly shows that individual and sporadic application of force by nations has borne very little fruit. It has to be part of a pattern or plan to have any effect. And here, formulating a response strategy obviously cries out for fresh thinking, innovative approaches to this phenomenon, especially a phenomenon that is changing.

Part of our response to terrorism, and I do not mean this in a negative way, is that as a nation we derive a certain cathartic satisfaction from getting back, striking back at our enemies. That is part of it too, but to really come to grips with this model perhaps we have to break that cycle. In this respect I think the challenge is to avoid the fate of the apocryphal German generals of WWI. When the story is told, the apocryphal generals planned to fight the last war, and were not victorious generals but generals locked into defeat. The German general staff was supremely confident that they had the world's most capable military force, with sophisticated armaments and a sophisticated technological plan. Of course, we see what happened. They failed to anticipate the changes in warfare that resulted in a very different form of conflict. In conclusion, I would say terrorism is a dynamic phenomenon and one that requires a similarly innovative, dynamic response—one that is just as

dynamic and innovative as the terrorists'.

What are those approaches? These are my thoughts, this is not the result of a RAND research project or serious research. I am trying to think—we know what has not been successful, but what might work; what sign posts are there for the future that we might leverage off of, that would be food for thought that would push us in different and perhaps more productive directions? The first would be to explore alternatives emphasizing the nonviolent approach. Certainly this circuit is a whole psychological operation inherent to special operations forces and inherent to our military. But in this respect it may be useful not to just study the open literature because if you follow the open literature the main response to terrorism is cruise missiles which is perhaps the most low-risk, but is of questionable efficacy. You have to go back to our response to the East African bombing to understand what I am talking about. When you talk about it, it was viewed by many Muslims as a blow by Mohammed. We have to counter the popular alienation and polarization that fuels terrorism.

How do you do that in practical terms? We had an opportunity and we missed it precisely because we focused on the use of force and did not think about the psychological connection. Only 12 of the 267 persons killed in the embassy bombings were in fact Americans. Indeed, amongst the Tanzanian and Kenyan casualties, there were many Muslims. And, in fact, at the time moderate opinion in the Arab world, particularly on the Iranian peninsula, was appalled; they were horrified by the fact that innocents were killed and also that Muslims were involved in it. And then what happens? Newspaper accounts push people more in the direction of condemning bin Laden and terrorism. Then what happens? The cruise missile attacks come along and in an instant negate those sentiments. That is not to say we should not have fired the cruise missiles, but it was a lost opportunity to influence opinion against terrorists and terrorism. We were oblivious to the nuances and insensitive to the response. Moderate opinion in the Arab world was not necessarily against the cruise missile attacks *in toto*. In fact, they thought the attacks against Afghanistan were justified; there were terrorist bases there, terrorist training camps. But with the attack on the Sudan, not withstanding the controversy that has since surfaced about whether it was VX or not, but even at the time, the controversy of taking that strong of an action against another nation, took the focus away from the U.S., Kenyan, and the Tanzanian victims and put it on Sudan as a victim and contributed to the lionization of bin Laden. The point here is that sometimes more can be gained by not using force than by using it. The bottom line is that to plan these operations we have to pay greater attention to the psychological connection.

So where does this leave us in terms of trying to deal with terrorism? First, we have to accept that terrorism is not a problem that is completely solvable, nor can it be completely eradicated. And this is why I think it is mistaken to call or analogize terrorism to a war. This raises unrealistic expectations in the American public. But also calling what is actually a tactic a war inflates the terrorist's power, inflates the coercive abilities of our enemy. It also creates a different sense. A war is something that has a definable beginning and widely has definable ends. It begins with a conquest and a vanquishment, which is seen as the end. It is then followed by a truce, an armistice, and negotiations to settle the problem. That is not what terrorism is about. It is a far more multifaceted, idiosyncratic, worldwide phenomenon.

The difficulty in countering the problem of terrorism does not mean that we give up but that we need to have much more realistic expectations and we marshal our enormous energies and our attention when and where they are most effective, if not to solve, at least to ameliorate the problem and reduce it. Here I would argue, we are missing the point, we are increasingly focusing on terrorism too much as an organizational phenomenon, as an organizational dynamic, and what we are forgetting is that terrorism is a phenomenon that draws individuals to it, that often results in individual choices in becoming terrorists. One unexplored area related to terrorism, one thing that is ignored, is the personal choice aspect and personal inducements. When one studies the past quarter century of terrorism countermeasures used throughout the world, one example constantly comes onto the screen, and that is the Italian government's use of the repentance program against the Red Brigade. That was used as a wedge to woo people away from terrorism. But it is mistaken in the popular mythology that this was a way to rehabilitate terrorists, to integrate them back into society. It was nothing of the sort. It occurred at a time when the Italian authorities were so frustrated by the lack of intelligence they had on the group that they turned to this

means as a way to uproot the group, to gain information, to gain intelligence that they could use to bore in at the leadership of that organization and then systematically dismantle it. And it worked. Indeed, in talking to Italian government officials in intelligence they offered another example. When the Mafia was bombing art galleries, they used the same approach: money, personal inducements, to get information that they could use against criminals and that proved effective.

I want to give another example. It is an example of how thinking differently can pay greater dividends than plowing the same field that we have been stuck in for a long time. In May 1998, I had the opportunity to go to Israel in the Gaza Strip and to talk to people there who ten years ago were on the terrorists' side who are now senior officials in the Palestinian authority. I fell into a conversation with someone who had been a senior leader in the Fatah, and we were talking about the general problem of HAMAS. He was talking about his frustrations, which were no different from those discussed here in Washington. And he stopped and said to me, putting this idea in my head about thinking "outside-the-box" and thinking along different, even outlandish lines. Since much of what were doing is not having a big effect, maybe some other ideas can make a difference. He said that the Palestinian Liberation Organization (PLO) had a problem in the 1970's. "We had an organization called the Black September organization. This was the most elite terrorist group we had. They were suicidal, not in the sense of religious terrorists who surrender their lives to ascend to heaven, but in the sense that we could send them anywhere to do anything and they were prepared to lay down their lives to do it." And of course the success of Black September was manifold. The assassination of the Jordanian Prime Minister, the 1972 Munich Olympic massacre where eleven Israeli athletes were killed, the seizure of the Saudi Embassy at Khartoum where the American ambassador and chargé were killed, were big events. Then there came a time when Black September was no longer needed. The Palestinian Liberation Organization had gained the world's attention. Arafat was invited to address the United Nations General Assembly and Palestine was granted observer status in the General Assembly. Terrorism became an embarrassment, so Arafat instructed his senior aide to turn off Black September. The senior aide tried to decide what to do with these guys, these zealous fanatical terrorists. The PLO spent months thinking of all different ways to stand down Black September and then they came up with a very simple idea. They had the idea of marrying them off and getting them families to keep them away from violence. They went around to refugee camps and places where the PLO had offices in the Middle East and told attractive woman in their twenties that they had a mission of the highest importance to the nation, and invited them to Beirut to be introduced to young men of Black September. In short, they created a mixer. Then they told the members of the Black September "If you get married, we will give you $3,000 and an apartment with a gas stove, refrigerator, a color TV, and a job with the PLO; and if you have a child within a year, we will give you an additional $5,000." The senior aide worried that the PLO would laugh at this idea, but it worked. Without exception, all the guys found wives, settled down, had children and were periodically tested. The PLO would give them legitimate passports and offer to send them on legitimate PLO missions, to their offices in Geneva and Paris. Without exception, not one of them wanted to travel abroad for fear of being arrested and losing all that they had. I am not telling you that we should institute the policy in the U.S. of having mixers and introducing terrorists to women, but what I am saying is that this is a different approach on the individual level that has also worked in other countries. I attribute the success of Northern Ireland, not so much to Gerry Adams's moderation or Martin McGuinness's moderation or other things, but for the past 15 years the Northern Ireland office has, on an individual basis, taken some of the hardest core terrorists in prison and let them out on parole, let them go back to their families and see their parents getting old and let them see the political situation, the economic situation, the social situation and see that that Northern Ireland is changing for the better. And the black and white polarization that they felt when they became terrorists, when they went in, has changed and is not as bad. And almost without exception, that program worked to wean individuals away from terrorism. So rather than concentrating, as we have been, on the organizational dimension and one has to say not getting very far; it makes more sense to use force alongside psychological operations, alongside ways we can reach out at the terrorists and get them away from violence, that may prove more effective than what we do now. I do not know if that will be the case, but I know it can not be any less effective. The question is, could policy makers and the public be sold on it?

Chapter One

Terrorism Threat and Response: A Policy Perspective

James M. Smith and William C. Thomas

Introduction

Observations of the terrorism of most interest to the United States can be organized into two distinct periods of inquiry. The first begins with the advent of the modern era of international political terrorism that began to directly affect the United States roughly from 1970. This terrorism was characterized by its political motivation and agenda, its conservative approach to weapons, tactics, and casualties, and its clear lines of authority and structure—even including in many cases state sponsorship and sponsor-imposed constraints on the range of available action. This is what we refer to here as "traditional" terrorism.

The second period of terrorism of direct interest to the United States is that of the "new" terrorism that became evident in the last decade of the 20th century. After a decline in terrorism directed at the United States following the concerted anti- and counter-terrorism efforts of the late 1980s and into the 1990s, the U.S. witnessed a rapid succession of devastating terrorist attacks. From the 1993 bombing of the World Trade Center in New York City, through the 1995 bombing of the Murrah Federal Building in Oklahoma City, to the 1998 bombings of two United States Embassies in Africa, the US government and academic community witnessed a new wave of interest and action. And standing behind this renewed attention stood the "poster child" of this "new" terrorism—Aum Shinrikyo and its Sarin chemical gas attack in the Tokyo subway system in 1995. The renewal of terrorism directed against U.S. targets, the advent of terror attacks on the U.S. homeland, and the demonstrated prospect of the terrorist employment of weapons of mass destruction all coincided to usher in a new wave of examination of the expanding terrorist threat and of the broadened requirement for U.S. government response. It is those subjects—the changing threat and expanded response—that are addressed in this book.

Purpose

The terrorism threat of interest in this volume is specifically that directed at U.S. citizens, property, and interests both at home and abroad. American citizens abroad have long been primary victims of international terrorism. Added to that continuing trend is the advent of both transnational and homegrown terrorism within the continental United States. Those two factors are not likely to change any time soon. As Bruce Hoffman puts it, "Terrorists have targeted the United States more often that any other country. . . . The reasons why the United States is so appealing a target to terrorists suggest no immediate reversal of this attraction."

Thus, it is both necessary and timely to undertake a comprehensive examination of the changing terrorist threat and of appropriate response actions from a U.S. government policy perspective. This book presents some pointed observations and recommendations as inputs to that examination. It asks what has really changed and what stays the same in terms of the terrorist threat. It examines resultant changes and threads of continuity for appropriate response mechanisms and capabilities. It presents recommendations to prevent, deter, preempt, defend against, mitigate, and respond to the new threat. And it examines the status and adequacy of response policy and organization to meet that threat. Perhaps most significantly, it undertakes all of those tasks specifically from a practitioner’s perspective, lending added salience to its message.

Overview

In reviewing his efforts in research and writing on terrorism, Brian Jenkins recently observed "Over a quarter

century of research, yet terrorism persists. It is because terrorism is not a problem that awaits a solution. But rather . . . it is a changing threat." While there remains much legitimate debate over the extent, imminence, and nature of the "new" dimension of the threat, terrorism has clearly changed since the 1970s and 1980s. While the number of incidents may be dropping, the lethality of attacks against Americans has risen sharply. Those attacks today include targets in the United States as well as overseas, and the possibility of an attack involving weapons of mass destruction has become very real. Like any other social phenomenon, terrorism evolves over time as the society of which it is a part continues to change. Much of that perceived change, as depicted in the media, is based on anecdotes, worst case scenarios, or simple, unreasoned fear of the unknown. Rational analysis of the modern terrorist threat reveals not only how the nature of terrorism is changing, but also how the U.S. can organize to deter it and, if necessary, mitigate the effects of an incident.

This book is a collection of current research from academia, the U.S. government, and the private sector. The authors' experiences and approaches to the issue vary, but they share a deep understanding of the concepts underpinning terrorism. They provide an analytical approach that promotes an awareness of the terrorist's perspective, and then develop a strategic structure for combating it. Their recommendations regarding operational and organizational measures provide policymakers with several options for addressing modern threats.

Those threats are different in some fundamental ways today than they were twenty years ago. The first section analyzes the changes that have taken place and forecasts the most likely concerns in the near future. There is consensus among the authors that the strategic environment has changed, resulting in groups that are more difficult to detect and motivations that increase the possibility of mass casualties. The use of weapons of mass destruction (WMD), including nuclear, biological, and chemical weapons, appears somewhat more possible, in light of not only changing objectives but also the availability of weapon components. A relatively new terrorist tool, cyberterrorism, increases the risk of mass disruption of essential services. Though many of the concerns voiced in the mass media appear to be based solely on conjecture and anecdotal evidence, the authors agree that after careful analysis, the threats posed by these new weapons are still very serious.

Meeting these threats may require not only new tactics, but also an entirely new conceptual framework. For decades the American paradigm has been to address terrorism as a criminal problem, but a number of authors suggest that the time has come to treat it as a political issue. Preempting threats from both international and domestic sources may require means that go beyond the traditional legal system. The distinction between military missions and law enforcement tends to blur in some cases, and the result may be increased cooperation between civilian and military agencies in countering, combating, and responding to the threat.

The goals of consequence management efforts should be twofold, as explained in the final section. Obviously, the need to effectively marshal resources following an incident should lead to policies and technologies that can save the most lives and assist in finding those responsible. A second goal of effective consequence management, though, should be to deter an attack by lowering its potential impact, thus reducing the political return to the terrorist. The message that comes through the final two sections is an economic one: raise the cost to the terrorist through preemption, and reduce the gain through effective mitigation of the effects.

In the Foreword, Bruce Hoffman makes the point that the terrorist today is not the stereotypical terrorist of the past. The changes are dramatic, and if the United States does not adjust its response accordingly, it faces grave dangers in the not-too-distant future. Whether the response takes the form of increased law enforcement activity, the use of economic sanctions or incentives, or increased military involvement in counterterrorism, the fact remains that the U.S. must adapt to the threats posed by twenty-first century terrorism.

The Twenty-First Century Terrorist Threat

Much as the Cold War seemed to provide some sense of stability in the military arena, the terrorism of the past decades consisted of known enemies whose motivations were generally understood. But just as the world's

political structure has changed, so too has the terrorism that is a part of that structure. Many of the political objectives that limited a terrorist's use of force have given way to new motivations that seem to capitalize on casualties. Horrific weapons of destruction, often foregone in the past, may be just the tool required by modern terrorists. An understanding of this "new" terrorism is essential before measures can be employed to combat it.

Stephen Sloan begins by identifying key indicators that demonstrate how terrorism is evolving in "The Changing Nature of Terrorism." He proposes four areas of change that deserve consistent study: the context and environment of terrorism; changing motivations; technological transformations; and, adaptations in the organizational doctrine of terrorist groups. All of these issues are addressed further by the other contributors to this book. They do indeed turn out to be key points that require analysis.

One item of concern, however, is that policymakers tend to focus on short-run considerations rather than long-term threats or goals. An emphasis on immediate threats and recent incidents may blind policymakers to slowly evolving trends, such as long-term societal changes that are not evident in a short-term analysis. In addition, rapid technological transformations may leave analysts in a reactive mode, not affording them the opportunity to look toward the future. Effective deterrence and preemption of terrorist attacks will require a shift to a long-run analytical approach.

In "The Terrorist Threat to U.S. National Security," James Smith and William Thomas present a broad survey of contemporary terrorism that highlights evolving threats. The authors first outline a model of the essential components of terrorism, including the strategic, operational, and tactical factors, and the linkages between the three. Using the Aum Shinrikyo cult as a case study, they examine terrorist motivations, organizational structures, and the selection of victims and targets, as well as the degree of lethality.

Through a review of relevant literature and an analysis of trend indicators, Smith and Thomas identify four key objectives of terrorist groups. They go on to discuss evolving organizational structures and the means of attack that help terrorists attain these goals. By studying how terrorists are motivated, and their preferred means of attack, the authors provide guidance to policymakers who develop the U.S. response.

David Kay suggests in "The NBC Threat" that one of the most difficult tasks facing any analyst is to assess the validity of a threat that is still emerging. In this chapter, he addresses the evolving concerns regarding WMD terrorism. The stakes are high in this arena; failing to act early enough can lead to widespread consequences, while focusing too much on the threat can waste resources that might be better spent on addressing more likely forms of terrorism. Kay observes the attention being given to relatively recent events involving nuclear, biological, or chemical threats, and suggests that analysts should keep a balanced view when examining them. Though examples from the past do have value, a simple extrapolation from a few incidents may lead to incorrect conclusions.

Instead of merely projecting past trends into the future, Kay challenges analysts to identify key indicators of the broad changes that may lead to new forms of terrorist attacks. He identifies terrorist motivations, American vulnerabilities, and the ability to use various types of weapons as critical indicators that may signal a change in the threat. His study of these indicators, rather than merely trend analysis, leads him to conclude that the threat of nuclear, biological, and chemical terrorism is in fact one that should be taken seriously. He then proceeds to identify the policy implications of this critical analysis.

Another issue that must be taken seriously is cyberterrorism. In "The Cyberterrorism Threat," Gregory Rattray suggests that, as with WMD, the fear of computer-based terrorism is often based more on anecdotal evidence and lack of understanding than on a rigorous analysis of the threat. But much as in the case of WMD, the author's study of terrorist motivations, capabilities, and limitations, leads him to conclude that the threat is serious and growing. He suggests definitions and outlines the scope of activities that might be included in this field.

Rattray identifies two areas of particular concern. First, terrorist capabilities in this field are growing. Rapid technological advancements have created an environment in which a terrorist can conceivably attack and cause widespread disruption with limited danger of American retaliation. Second, America is vulnerable to a disruption of its information systems. While reliance upon the information infrastructure has grown, the problems of limited redundancy and uncoordinated response efforts have grown as well. He concludes with a series of policy recommendations designed to improve system protection and make cyberterrorism more dangerous for its practitioners, in the hopes of removing it as an attractive option.

Preemption and Deterrence of Twenty-First Century Terrorism

We can use the analysis from the preceding discussion to explore methods of preventing terrorist acts. Two strategic means are available. First, preemptive measures are designed to understand our own vulnerabilities, learn of efforts to take advantage of those vulnerabilities, and interdict those efforts. Going hand in hand with this are policies to deter attacks by raising the stakes for the terrorist, whether through threats of retaliation or by reducing our vulnerabilities and making success much harder.

David Tucker begins by examining America’s approach to the previously identified threats in "Combating International Terrorism." His thesis is that the current paradigm, that terrorism be addressed as a criminal act rather than a political one, is inappropriate. The perspective of terrorists is that their acts are political in nature. In order to effectively understand and prevent their activities, authorities should consider adopting the same point of view.

Tucker reviews the new form of terrorism that must be addressed. Modern terrorism has a distinctive structure that makes more use of networks than of independent cells. Advances in communications have facilitated the employment of networks to enhance efficiency and security. There has also been an increase in "amateur terrorism" perpetrated not by established organizations, but by ad-hoc groups that come together to plan and carry out a single mission before disbanding. These terrorists are very difficult to identify and track. Finally, the lethality of terrorist acts has increased as terrorist motivations have changed and more deadly means have been employed. Dr Tucker suggests that the U.S. response must address these new aspects of terrorism. The American interagency structure consists of formal and informal networks; perhaps a more structured hierarchy would be more appropriate. The US should also employ the proper tools to meet the current style of terrorism. Economic sanctions and threats of force may be more useful in response to state-sponsored terrorism, but economic incentives and increased intelligence efforts may prove more suitable for the growing non-state threat.

James Wirtz argues in "Antiterrorism via Counterproliferation" that this particular tool can be effective well beyond the problem of state use of WMD against military forces, and can bolster US counterterrorism efforts. He begins with an explanation of counterproliferation and demonstrate its applicability to different threats. Though designed to deter and protect against the use of WMD by states against military forces, he writes that it can be very effective in countering the use of WMD by terrorist actors.

Wirtz goes on to suggest four propositions. First, although counterproliferation is designed to counter military threats from states, it provides much in the way of deterrence and defense against both state-sponsored and non-state terrorism. This results from the fact that in addition to an element of punishment, an effective counterproliferation strategy emphasizes denial of gains by providing means of mitigating the effects of a WMD attack. His second proposition is that, as the U.S. becomes better at protecting its forces on the battlefield, adversaries are likely to focus more on asymmetric methods, such as terrorism. Third, if the U.S. is therefore more likely to face WMD attacks by non-state groups, then it must be prepared for such an attack. Consequence management preparations then become effective means of countering terrorism. Finally, while there are synergies between counterproliferation and counterterrorism, there are also tradeoffs, especially in terms of budgets and resources.

Another means of countering terrorism is through effective intelligence collection and analysis. Peter Probst reports in "Antiterrorism via Intelligence" that the U.S. intelligence community is searching for new means of combating terrorism. He discusses some of the vulnerabilities that have recently come to light as the U.S. military engages in a wider variety of missions. As American forces become involve in lower-intensity operations, new threats arise in the form of increased employment of third country nationals, and the potential for attacks against bases far removed from the conflict area.

Probst highlights a number of shortfalls that demonstrate the U.S. intelligence community has not responded to the needs of modern terrorism. He suggests that American intelligence analysts need to try to understand terrorists better, to be more aware of their perspective in order to more readily perceive their strategies and tactics. Special attention must be given to the emerging problem of the lone terrorist, such as the Unabomber, who is much more difficult to identify and track than is an organization. Ideally, the offensive and defensive aspects of combating terrorism would be blended together under the auspices of a single organization.

Although not included as a chapter in this book, in a presentation at the conference preceding this volume, "Antiterrorism via Physical Measures," General Wayne Downing and Ambassador Allen Holmes emphasized the point that we must understand the terrorist's perspective. While Tucker frames his expression of this point in the context of deterring terrorists at the strategic level, Downing and Holmes focused instead on the operational and tactical levels. By seeing what the terrorist sees, they argued, we will be in a better position to prevent a particular attack or, if prevention fails, to protect the potential victims and reduce the success of an incident.

Downing and Holmes suggested that, just as terrorists can adopt new weapons and new structures, so too can the United States. They also recommended that viewing a situation from the standpoint of a terrorist, rather than as a victim or a responder, can lead to a better understanding of the threats and vulnerabilities. For instance, they suggested reviewing the "essential elements of information" about a particular target in order to find and address the same weaknesses that terrorist are searching for. They offered a strategy of deterrence, denial, detection and protection, and recommended methods for achieving each. Finally, they concluded with a series of policy recommendations that included, among others, a reexamination of the balance between the safety of deployed military forces and the accomplishment of the mission. Their analysis and recommendations add a significant dimension to the operational lessons presented for government action in this book.

Responding to and Organizing for Twenty-First Century Terrorism

Should an attack occur, its ultimate impact will depend on the response by government agencies. A point that becomes clear through these chapters is that the response structure, though outlined on paper, relies in many cases on informal relationships to overcome the problems of overlapping authority and communication between agencies. Though new capabilities and organizational doctrine are being developed, the need exists for a comprehensive review of the means of mitigating the effects of an attack. Deterrence will also be enhanced as it becomes clear that a terrorist incident is unlikely to have the desired impact.

William Thomas, in "The Military's Response to WMD Terrorism," explores the requirements for DoD support to civil authorities in the aftermath of a domestic WMD event. Those requirements, for training civilian first responders and providing rapid support after an incident, are also tightly constrained in law, which Thomas states is probably overly restrictive for today's environment. He also explores the expectations that civilian responders hold for military support, with both federal and state officials including DoD assets in their contingency plans. He also overviews the current state of ongoing development of military capabilities that might be brought to the response effort, finding a long and growing list of military units and efforts tailoring their missions, equipment, and training to ensure the capability to support domestic WMD response.

Thomas provides an evaluation of the effectiveness of the military response to date in fulfilling the tasking of executive and congressional directives and existing response plans. In general, he finds that a good start has

been made, but that much remains to be done to provide the level of integrated response that a major WMD attack would demand. Finally, he reminds us throughout that the objective of the military response to domestic WMD terrorism is deterrence—mitigation of the consequences of the attack so as to render WMD attack a less attractive option for terrorists seeking to reach their action goals. That must remain a visible goal across all efforts.

In a related presentation on "Consequence Management" at the INSS terrorism conference preceding this book effort, Rick Roman of the Centers for Disease Control and Prevention, the CDC, addressed the initial detection of and response to a domestic chemical or biological (CBW) attack. He defined consequence management in this case as being a three-part plan designed to protect public health, restore essential services, and provide emergency services. The public health system will play a major role in determining the scope of a response to a CBW incident. There is already a set of agents for which the public health system monitors in order to identify an attack and sound the alarm. In the event of a CBW attack, the public health system has four primary goals. First is the detection of an attack, followed closely by a diagnosis of its nature. It then becomes necessary to evaluate the scope of the exposure and identify and implement the appropriate control measures.

According to Roman, one of the major difficulties in addressing CBW terrorism is differentiating between a naturally occurring illness and a terrorism attack. Indeed, one of the most vexing problems in combating CBW terrorism is recognizing that an attack has occurred. The CDC has established a set of indicators that they use as part of a nationwide health surveillance system. Working closely with a network of state and local public health agencies, they hope to identify an attack early enough to be able to initiate a response before the exposure becomes widespread. Rapid identification, he pointed out, is essential if an effective response is to be mustered.

In another conference presentation not specifically included in this book but covering earlier efforts in the evolution of military response capabilities, "Military Support for Civil Response to Attacks Using Weapons of Mass Destruction," Colonel Jay Steinmetz agreed with a number of our authors when he suggested that the U.S. may need to reconsider the view that terrorism is a crime rather than a political act. As has been proposed earlier, events in the 1990s demonstrated that the modern forms of terrorism may result in the criminal paradigm leading to a less effective response. He went on to review the integrated civil-military structure that has evolved over time, and finds many problems of overlapping authority and unclear chains of command. These problems will need to be addressed, he pointed out, if the system for combating terrorism is to be an effective deterrent to terrorists. He suggested that the DoD is unique in its ability to mobilize manpower and resources quickly, but its role has yet to be fully developed.

There are a number of piecemeal solutions that will contribute to the effort, though they will not by themselves lead to a fully integrated structure. Key among these, he pointed out, is the creation of the Rapid Assessment and Initial Detection (RAID) teams. Steinmetz analyzed the role and capabilities of these units, which are already being deployed. The RAID concept integrates the National Guard into the counterterrorism structure, bringing with it national coverage, a rapid initial response capability, dedicated communications bandwidth, and significant resources for reachback purposes. He cautioned, though, that this is merely a first step toward synergizing the hundreds of disparate efforts spread throughout the Federal, state, and local levels of government.

"International Incident Response," written by the staff of the Operations Directorate of the State Department’s Office of the Coordinator for Counterterrorism, takes us beyond the domestic realm and addresses the problems arising when terrorists strike Americans overseas. Though the U.S. developed emergency support teams for domestic and international incidents over a decade ago, the response to a foreign incident is still muddled by controversy. Incidents such as the bombings of two U.S. embassies in Africa demonstrate the need to resolve these issues, lest they hinder the efforts to protect Americans overseas.

One of the major problems that has dogged the American response is the uneven application of the "no concessions" policy, under which the U.S. states it will not negotiate with terrorists, but which was not always

followed during the 1980s. Another concern stems from the question of when it is appropriate to send American resources abroad in response to a terrorist attack. Depending on the incident and the environment, it may be preferable to defer to the host nation's response structure while the U.S. merely provides support. In other, non-permissive environments, a more direct response by the U.S. may be required. Of course, the U.S. has to decide whether to send unique counterterrorism resources overseas at all, as that may leave us more vulnerable to a domestic attack. Finally, in order to provide an overseas response capability, appropriate resources need to be procured. There are currently many questions regarding the nature of the equipment that is required and the source of the funding. Until these issues are resolved, response teams must operate with equipment that is rapidly becoming outdated. In addition to replacing aging equipment, of course, the U.S. must prepare for new forms of attacks as well.

Finally, Douglas Menarchik deviates from some of the other authors as he suggests in "Organizing to Combat Twenty-First Century Terrorism" that leadership is more important than organizational structure in determining the effectiveness of the country's response to terrorism. He identifies five issues that have consistently been debated over the past thirty years: the threat and nature of terrorism; terrorist priorities; the criminal nature of terrorist acts; efficacy of a legal, rather than a military, response; and the question of whether terrorism is a symptom of underlying causes or separate from those causes. As the answers to these questions change from administration to administration, they shape the American response to terrorism.

Menarchik reviews the terrorism policies and perspectives of senior leaders throughout the last five administrations. He identifies both the changes in policies and the recurring themes. By noting the trends, he forecasts future threats and suggests possible responses. Above all, he recommends a low-key approach that maintains terrorism as a priority for each administration. Rather than creating a new bureaucracy, such as a "terrorism czar," he suggests instead doing a better of job of integrating current efforts.

The Road Ahead

Changing threats to American national security demand new methods of addressing them. Whether these include new organizations or merely a restructuring of existing capabilities, it is imperative that the U.S. recognize the changing nature of the terrorist threat. An effective response is one that can deter and preempt an attack, either through raising the threat to the terrorist or reducing the potential impact. Jay Davis writes in the Epilogue that the U.S. has realized there is no "silver bullet" approach to combating terrorism. Instead, it is pursuing a number of options which, when combined effectively, can significantly reduce the threat to Americans at home and abroad. The key to countering terrorism effectively, he writes, is to learn from past successes and failures, recognize the need for change, and ensure the executive and legislative branches share a common vision for the future.

This collection of experience, wisdom, and recommendations, then, addresses the enduring and changing threat, policies and approaches to prevent the realization of that threat, and both operational methods to mitigate the effects of a realized threat and organizational schemes to better coordinate and direct U.S. government actions to counter terrorism. A word of caveat before we present the collected wisdom. The chapters that follow are uneven in content and scope, inconsistent in approach, and incomplete in addressing the full range of the topic at hand. There are several reasons for this outcome. First, we limited the authors to either current or recent past employees of the U.S. government, or to those whose contractor or consultant activities keep them closely linked to that government, in order to ensure a policy focus and practical applicability to the book. Second, we asked them to keep their contributions unclassified and releasable. Finally, we asked first for conference presentations on their activities of focus, but then for follow-on chapters for consideration for this book. As a result, the chapters are very uneven in length. Some are much more broadly cast than others to add to the educational value of the collection, while others are more tightly constrained due to their subject matter and the sensitivity of much of the material in that particular area. The work is incomplete largely because some of the conference papers could not be crafted as chapters, or their presenters were too involved in policy implementation to reflect in writing on past policy inputs and activities. Some of the presenters have been

"riding a moving train" as their particular areas of policy have been in dynamic development and continue to be unsettled. Thus, we present what we believe is a valuable contribution to the study of the terrorism threat and U.S. Government response, but we make no claim as to providing the complete and final word in this arena.

Chapter Two

The Terrorist Threat in Strategic Context

James M. Smith and William C. Thomas

Introduction

This chapter presents a broad survey of the terrorism threat to United States citizens, property, and interests to capture the state of that threat early after the beginning of the millennium. Much has been written elsewhere on various aspects of and changes in terrorist motivations, tactics, weapons, and organizational schemes, and this chapter does not attempt to add volume to that literature. What it does is consolidate and systematize numerous lessons, particularly those drawn within the policy-oriented literature, into an overarching strategic context to allow for pointed analysis of the terrorist threat to United States national security.

The snapshot presented here is taken with a wide lens, establishing the threat within its strategic context. That context is key. Viewing the many pieces and parts of contemporary terrorism is valuable, and for such a complex phenomenon, much of the necessary detail can only be developed through specific and narrow development. But a full understanding of the threat requires that those detailed parts be viewed within a coherent whole—only then can the true nature and extent of the threat be seen. Further, the strategic context must be at the heart of any response strategy. You must comprehend the terrorist's strategy to counter it with yours.

This survey, then, proceeds by first establishing terrorism within its strategic context to allow comprehensive analysis. The essential components of terrorism are identified and developed in detail, and they are then related within a dynamic flow diagram suggested as a model framework for terrorism description and analysis. That framework can be applied to today's terrorists and their preferred targets to illustrate the range and variety of terrorist threats affecting US citizens, territory, and interests now and into the 21st century. Finally, that strategic context and the perspective it provides are applied to suggest the broad outline of appropriate response strategies to enhance US national security.

Strategic Context

It is beyond the scope of this chapter to seek to establish a universally accepted definition of terrorism. Indeed, the difficulties in trying to define the phenomena even within the Executive Branch of the United States government are legendary. However, discussions of what terrorism entails are useful in identifying essential elements to incorporate into examining the nature and extent of the threat. Broadly stated, the "terrorism" of interest here is calculated violence applied toward coercive intimidation or provocation. The "calculated violence" component points to a focus on the instrumental act—the bomb or the gun, the shooter, the victim, the violence. The "coercive intimidation or provocation" points to the ultimate objective—the creation of fear as leverage toward changing some aspect of government or society. Bruce Hoffman reminds us that the two central differentiating factors of the terrorist are his dedication to a political cause (thus marking him as distinct from a common criminal) and his instrumental reliance on violence (that differentiates him from other political extremists). The central point is that terrorism cannot effectively be viewed as one or the other; it is not simply the act, nor is it simply the objective. Both perspectives are essential to fully understand, analyze, and respond to terrorism, and both are highlighted in our conceptualization of terrorism.

Our focus in this chapter is specifically on political terrorism—a strategy of violence within a broader political context. This deemphasizes the violent act of the single criminal or deranged individual acting toward personal ends, and it marginalizes the occasional use of indiscriminate violence as a tactic within a wider revolutionary campaign. We choose to focus on political terrorism not because it is the only source of threat, but because it is the most complex manifestation of terrorism, thus incorporating all of the components that we

want to identify and develop in overviewing the full range of threat. The terrorism of focus here forms the strategy, the central manifestation of the political violence, and the vehicle designed to reach the political end. This terrorism is the "systematic political terrorism" that the world has seen in changing forms since the 1970s. Systematic terrorism aims toward a strategic end, and it both can and must be viewed as the political strategy that it is. In a classic statement, David Fromkin presents a comprehensive characterization of the strategy of terrorism.

> All too little understood, the uniqueness of the strategy lies in this: that it achieves its goal not through its acts but through the response to its acts. In any other such strategy, the violence is the beginning and its consequences are the end of it. For terrorism, however, the consequences of the violence are themselves merely a first step and form a stepping stone toward objectives that are more remote. Whereas military and revolutionary actions aim at a physical result, terrorist actions aim at a psychological result.
>
> But even that psychological result is not the final goal. Terrorism is violence used in order to create fear; but it is aimed at creating fear in order that the fear, in turn, will lead somebody else—not the terrorist—to embark on some quite different program of action that will accomplish whatever it is that the terrorist really desires.

From this and other conceptual approaches to terrorism, we have drawn together what we see as the essential components of terrorism. Developing these components and then adding their dynamic relationships allows us to build a template that can be applied toward a fuller understanding of today's terrorists and their brands of terrorism.

Operational Factors

Operational factors define the group and place it into the world of political violence. "Causes may be broadly conceptualized as any one of an array of observable economic, political, social, and/or psychological factors." Causes are those long-term (social inequities, political disenfranchisement, economic depressions) or short-term (ethnicity, relative deprivation, government repression) conditions that underlie the resort to a strategy of terror. There traditionally have been at least three broad categories: redress of grievance, overthrow and replacement of the existing government/system, and liberation from "foreign" masters. Today one might add destruction of the existing order to that list at minimum as an intermediate cause. Whatever the specific set of factors behind the strategy, the cause serves as the driving force for recruitment, support, and planning—all of which are sub-elements of structure.

Figure 2-1: Essential Components of Terrorism

Operational Factors **Group Type/Cause** **Group Structure**
Tactical Factors **Act** **Actor** **Weapon** **Victim(s)**
Strategic Factors **Target of Terror** **Objective of Terror**
Linkage Factors **Operational to Tactical** **Causal Link/Action** **Tactical to Strategic** **Instrumental Link/Fear**

Broadly defined, structure includes a range of subordinate elements essential to carrying out the strategy such as planning, surveillance (intelligence), transportation, papers and identification, arms, money (finance), publicity and propaganda, and command and control as functions of organization. Or "organization provides the formalized structure utilized for the planning, coordination, and application of extranormal forms of political violence." It includes the terrorist political and "military" infrastructures that form the organizational strengths and weaknesses of the strategic and tactical sides of the movement. Taken as a whole, structure is a critical part of the strategy, and it has traditionally provided a central focus for defeating that strategy.

Group Types/Causes. A comprehensive analysis of the twenty-first century terrorists and their terrorism must begin with a meaningful grouping of contemporary practitioners. Several insightful observers of terrorism offer their groupings for our evaluation. Bruce Hoffman retains a classical left-right political focus, drawing distinctions between the "old" left and right and their late 1990s mutations. He also gives special attention to ethno-separatist nationalist practitioners of terrorism as the primary actors through the 1980s, and he adds terrorism based on religious imperatives as another categorization deserving of separate attention, particularly in the 1990s. In developing those four categories, he also discusses the issues of state sponsorship, the advent of terrorism "for hire," and the growing trend toward employing amateur terrorists only tangentially attached to the larger group. Hoffman's detailed development of these categories explains historical changes in terrorist goals, motivations, and tactics. We incorporate his insights into a slightly broader framework tailored to the threat to US national security.

Ian Lesser develops a more comprehensive listing, his based on functional and geographic-based terrorist threats to US interests at home and abroad. He projects ethnic separatist and frustrated nationalist threats to the US arising particularly from within successor states to the former Soviet Union. He also sees the increased violence from religious motivated groups as continuing into the foreseeable future. Further, while the ideological groups of the past have waned, Lesser raises the possibility of a re-emergent and invigorated left or a resurgent right engendering new violence. Significantly, Lesser highlights the dangers of terror tactics within an ongoing small-scale contingency or as a carryover by the losing factions from an earlier conflict. He also brings attention to the rising prominence of the violence associated with international crime. Finally, he cites the problem of extreme alienation giving rise to terror attacks. This broader listing, particularly as it is tailored to the threat to US interests, is adapted with input from Hoffman for our use here.

We develop seven categories of groups, regardless of the location of their operations, as representing the broad range of the terrorist threat to US citizens, territory, and interests. Our first four categories—classical and new left, ethno-separatist/nationalist, religious extremist, and classical and new right—combine elements of Hoffman's central groupings as also reinforced by Lesser. These are the primary group types and causes behind the strategic, political terrorism of most interest to the United States today. The last three are applications of terrorism within another type of strategy—not specifically political—but they threaten US interests, and their strategies are open to a US strategic response.

- ***Classical and new left.*** Ideological terrorism based on leftist causes was a mainstay of the 1970s and 1980s. RAND data showed that eight of the 11 active international terrorist groups in 1968 were left-wing ideological groups. This number rose to 22 of the 64 groups active in 1980, and it remained at 22 of the 42 active groups in 1992. Significant for these groups, the political cause overshadowed all other factors—they sought to replace the corrupt old order with one of their choosing. Toward that end, classical leftist groups have always tailored their action to appeal to a popular constituency, with their violence thus constrained, choosing symbolic targets and specific armed propaganda operations for mass effects designed to remake the state. The "victory of liberal democracy" that ended the Cold War may have decreased the appeal of such groups, at least temporarily, and the demise of states that supported this form of terrorism has reduced their available resources. The transition, though, to new norms and forms of political and economic order is proving slow and painful, and this might well prepare the ground for a renewal of terrorism from the left, now from a combination of the traditional and an emergent "new" left. This new left, perhaps more international—designed to create an international civil society no longer tied to the state—and less hierarchical in form, will likely still be constrained by an overarching desire to achieve legitimacy.

- ***Ethno-nationalist/separatist.*** Modern irredentist terrorism rose out of the aftermath of World War II and reached its zenith in the Palestinian groups active in the 1980s. For example, 37 of the 64 international groups active in 1980 were classified as "nationalist/separatist." That figure had declined to 13 of 42 active groups in 1992. However, this brand of terrorism continues as a significant factor in the US threat calculus. These terrorists combine a political objective with ethnic and often religious components, but the political side reigns supreme. They choose symbolic targets to influence both local and international audiences, seeking to embarrass, discredit, and coerce the local government while also gaining their group publicity and support. Gaining and maintaining legitimacy is critical to attaining their goals, so their violence is measured to maintain a socially "tolerable" level and avoid alienation. It is argued that they are most violent early in their existence as they employ violence for hoped for catalytic effects toward a widened conflict and late in a failing cause out of frustration and for revenge. The US may become an attractive revenge target if we have supported the government these groups oppose.

- ***Religious extremist.*** Terrorism based around religious imperatives is both the oldest and the newest form of terrorism. The modern reincarnation of this historical form arose in the wake of the success of the Iranian Revolution of 1979-1980. RAND recorded no primarily religious terrorist groups in 1968 and only two of 64 in 1980. However, 11 of 42 groups fit this description by 1992, and by 1995 that number was 26 of 56 groups. Significantly, the rise of religious-based terrorism has signaled a shift from violence measured to fit a political agenda to increased lethality associated with a total, holy war. Violence for these groups is legitimized as a sacramental act, even a divine duty, with the believers forming their own—and the only—constituency of interest. The victims and the target are inconsequential outsiders, as are the general mass observers. The constraints placed on the violence of the left and the separatist are gone. Finally, while leftist and separatist terrorism uses violence as a means to affect change in the existing political order, religious extremist terrorism sees violence as a cleansing tool to remove an existing order deemed unfit to rule—or to exist. Data show that while the overall number of incidents has declined as religious-based terrorism has become prominent, the number of fatalities associated with terrorist acts has risen. For example, in 1995 every act with eight or more fatalities was perpetrated by a

religious-based actor.

- ***Classical and new right***. While terrorism from the right is not new either, today a new offshoot has emerged out of the religious imperative described above. It is difficult to determine if today the religious imperative is more important than the political cause, but this category is broken out to add focus to the domestic US manifestation of terror based in extreme right-wing politics, racism, and a "transparent veneer of religious precepts." Interestingly, the European variety of right-wing terror matches American political and racist leanings without the religious undertone. In either case, this category of terrorists today employs the most indiscriminate violence, often seeming irrational to general observers. It is, however, not completely indiscriminate or irrational, but is aimed at deliberate intimidation of governments, ethnic and racial groups, and foreign citizens living in the terrorists' homeland. Finally, and significantly for those seeking to thwart such groups and their acts, these groups are both widely dispersed in non-hierarchical but like-minded cells and internationally linked together for information sharing. The Southern Poverty Law Center identified 435 active "Patriot" groups in the US in 1998, as well as 248 "Patriot" Web sites. While not all of these groups advocate violence or racism, they provide a fertile breeding ground for the beliefs that may lead to future terrorist activity.

- ***Byproduct of regional conflict (SSC/MTW, past or present)***. The post-Cold War regionalization of conflict has created increased opportunities for states and state-sponsored actors to seek asymmetrical means to attack stronger foes, particularly the United States. While the state strategy here is to defeat the stronger foe or cause it to withdraw its support and presence from a more traditional unconventional or conventional regional conflict, or to retaliate for past involvement in such a conflict, terrorism may be selected as an operational means toward that end. Peter Probst wrote in 1992 that

  > One result of the spectacular coalition victory in the Persian Gulf war is that nations opposed to the United States and its coalition partners are significantly less likely to resort again to conventional warfare as a means to advance their foreign policy goals. Rather, there will likely be an increased reliance on indirect forms of aggression, such as terrorism, subversion, insurgency and other forms of low-intensity conflict.

State involvement, either direct or through the use of sponsored surrogates, is an enduring factor in such cases. Again, the terrorism here is within a larger conflict strategy, but the terror and its possible consequences must still pose a significant threat to the United States.

- ***Crime, drugs, and privitization of terror***. Similarly, the late 1990s surge in international criminal violence, whether revolving around the drug trade or the wide-ranging enterprises of the underground economy of transitioning eastern Europe, has begun to spill over into the political arena. If the "narco-terrorism" experience is representative, this violence could spawn terrorism directed at United States victims and targets. The "strategy" behind the violence in these cases is the illegal activity and its economic dimension, but the effects must be considered in US policy and strategy.

- ***Anarchy and rage*.** Finally, as another dimension to the threat to US citizens, property, and interests, we today see instances of "agenda-less" terror—violence perpetrated by independent actors lashing out due to frustration and rage. They see some aspect of the political, social, and/or economic system as responsible for an unacceptable plight, and they reach an as yet not fully understood point where violent destruction is their chosen resort. It will be difficult to anticipate the next Unabomer, or a future abortion clinic attack by a lone actor. As this terror has no strategy behind it, it can only be blocked and its effects mitigated by the macro US strategic response—but it must be considered.

Group Structures. The traditional terrorist structure was a hierarchy of small cells, often with only a single link between them—one individual who knew the cell's contact point. This structure lent itself to strong central control, discipline, and a degree of security for the larger group, if not for each individual cell. That organization

scheme, however, is today being replaced with much flatter, much more decentralized networks, sometimes with a single central node, but often with multiple points of interconnectivity so that the group is not dependent on the fate of any one cell. This networked interconnectivity combined with modern telecommunications complicates detectability, allows stand-alone individuals and cells only loosely connected to (and not directed by) more visible groups, and facilitates communication and cooperation between like-minded groups across international borders. It allows small, remote non-state actors to play roles formerly available only to much larger, state-like structures.

This contributes to and reflects what Bruce Hoffman cites as the growing "amateurization" of terrorism—ad hoc amalgamations of like-minded individuals and dispersed, small groups sharing a common cause and mutually reinforcing action without central control. These cells may be indirectly influenced, remotely controlled at best, serving as willing servants, "cut outs," or even dupes for some larger cause. Or they may be simply acting on their cause which is in concert with other groups and their causes—a loose fringe engendered by other terrorist groups or even by more mainstream, legitimate groups espousing a fervent cause. In any case, such groups face fewer constraints than did their centrally connected predecessors, and they complicate detection and countering strategies because they have a much lighter "footprint," using varied tactics and weapons in unpatterned acts of violence.

Tactical Factors

Tactical factors focus on the direct elements involved in a given act of terrorism: the terrorist, the weapon, the victim, and the act itself. Terrorist actors are difficult to categorize. While different groups attract or seek to recruit specific segments of society, "All that can be said with any degree of confidence is that terror was (and is) a pursuit of young people, and that in most other respects the differences between terrorists are more pronounced than the features they may have in common." Today, with the "amateurization" noted above and with criminal elements also employing terror tactics for their ends, categorization is further complicated. Terrorist victims also defy easy categorization. Other than the fact that Americans have traditionally predominated as victims of international terrorism, and that among Americans diplomats, businessmen, and members of the military services have been most at risk, victims have represented a wide range of people and things: men, women, and children; young and old; famous and ordinary; planes, trains, ships, cars, and buildings.

But terrorist weapons and tactics do fit into somewhat predictable patterns, and their use can also be grouped around related acts. They change as terrorists adapt to their successes and failures, but those changes tend to occur over time in identifiable trends, not overnight. Bombs have been the favored mode of attack, ranking highest in terrorist tactics from 1968 through 1994. For example, in 1992 they accounted for almost half of all incidents (46%), and that percentage was stable (between 40 and 50%) since 1968. For that same period, second place went to attacks on installations (by weapons, arson, and sabotage other than bombing) at 22% since 1968. Hijackings were a distant third (12%), with assassinations (6%), and kidnapping (1%) rounding out the top five. Bombings require few people, can be carried out with relatively crude devices, allow the bomber a fair chance to escape prior to detonation, and today can incorporate new and sophisticated explosives, timers, and fuses. These trends may now be changing slightly, however. Bombing began to decline in popularity in the 1990s, falling to 34% of all incidents by 1994 (still the most favored tactic) and to second place at 24% in 1995. Armed attack may be replacing it at the top of the tactical chain, representing its stable 24% of all incidents in 1994, but rising to first place at 44% in 1995. These trends warrant closer scrutiny and analysis to see if they indeed represent a reversal of favored tactics or only a temporary aberration in the larger pattern. By 1995 kidnappings and assassinations remained far distant third and fourth (14% each), and hijackings had largely dropped from the US radar screen.

Trends in terrorist tactics generally remained unchanged from the 1960s into the 1990s. This led to terrorists being characterized as tactically conservative, despite their radical politics, with an imperative to assure success, even if moderate, over risking tactical innovation. Three significant aspects of the tactical threat are changing

today, however, and warrant specific attention. First, and as a basis for the other two trends, is an increasing technical sophistication and operational competence in the late 1990s. Today's terrorists continue to learn from other practitioners of terrorism and adapt new weapons and tactics just as their predecessors did in the past. This is seen by analysts as more a factor of human exploitation of available technologies than as a technologically driven trend. However, coupling new and lethal technologies with more technologically capable terrorists under conditions of less constrained violence creates a volatile danger. This leads to a second changing threat factor that is the increased potentiality for terrorist use of the specific technologies of nuclear, radiological, chemical, and biological weapons. Without the political constraints of the old left and traditional irredentist causes, the likelihood of terrorists attempting attacks employing such weapons of mass destruction increases. While the reduction in states supporting terrorism limits the resources available for covert nuclear programs, chemical and biological weapons are relatively cheaper, and could provide the appropriate level of terror. Third, others note movement away from destructive technologies toward tactics of mass disruption, with modern terrorists exploiting information technologies for both tactical offense and defense operations, and for support of their organizations. This has even been tabbed "netwar," and it represents yet another added dimension to the threat. Both mass destruction and mass disruption threats are developed in much greater detail in subsequent chapters of this book.

Thus, the tactical environment and its elements, while not exactly straight forward, are at least well known and studied, and are important in both responding to an individual act and designing a general response policy. Both investigation and prevention rely heavily on specifics of the tactical environment. Certain groups may prefer particular victims, a particular style of device or type of explosive or weapon, follow a predictable *modus operandi*, or even fit a specific personnel profile. Such characteristics are key to solving a specific criminal incident or seeking to block an identifiable category of attack. With the advent of flatter, non-hierarchical organizations and even loosely linked or unlinked actors, in some cases no such "footprint" may be readily identifiable or predictable. In all cases, however, the larger, strategic environment is central to a broader attempt to understand and defeat the terrorist. "[Terrorism's] success seems to be due in large part to a miscomprehension of the strategy by its opponents. They have neglected the more important of the two levels on which terrorism operates."

Strategic Factors

More important, and at the heart of the strategic context we seek to develop, are the strategic factors of target and objective—the real object and rationale of the group and its acts—the "more important of the two levels." Terrorism is designed to evoke a response from the ultimate target of the act, the government or society. The intention may be that the government change its external policy, changing its support to or from a nation or government. Or it may be to discredit the government, graphically demonstrating that it cannot control its territory or protect its citizens, that it cannot govern. It might be to drive a wedge between the government and its people. Or it could be simply to publicize and recruit to a cause. In all of these cases, and more, the act and its victim(s) will be directly or indirectly but symbolically linked to the target, and fear is intended to transfer the effect from the act to the behavior of that target.

Further, terrorism is intended to cause its target to react in a specific way. This is the end goal, the overall objective of the strategy. Government or society must change, and the strategy points directly as a continuum from its root cause toward affecting that change. Government or social reaction—whether over-reaction, under-reaction, or pointed reaction—is the goal at the output end of the process, and the strategy succeeds or fails only as a function of the direction and degree of the reaction it achieves. Those targets, reactions, and the objectives they seek can be categorized in a variety of ways, with a selected sampling developed below.

Targets of Terror. The brief discussion here addresses both direct and indirect targets and victims of terrorism undertaken to impact United States national security. The scope of this discussion is not exhaustive, but is simply representative of the wide range of potential targets and victims. There are four general (macro) categories that encompass the central focus of that range of threat and are considered a comprehensive listing

for the purposes of this chapter. First, the United States government continues to represent a primary target of terrorism. As noted earlier, Americans have traditionally predominated as victims of international terrorism, and among Americans, diplomats, businessmen, and members of the military services have been most at risk. This has recently changed slightly, with the 1995 RAND data placing Americans in second place for favored victims that year. It remains to be seen whether this represents a long-term decreasing trend. In fact, given the post-Cold War US global leadership role, United States government presence and policy may become even more prominent targets of international terrorism attacks both abroad and at home. Second, US business has been and will continue to be a popular target of terrorism. As the globalization of the world economy continues, US business presence and influence will become increasingly visible and vulnerable. Third, the United States public is also an attractive target of terrorism. The leading roles of the US government and of US business combine with the centrality of Hollywood and Madison Avenue in global commercial media to highlight the US citizenry and public opinion as primary targets of terrorism. Finally, international systemic institutions and stability are of central importance to United States interests, and thus present attractive terror targets.

Within each of these categories, there could be both direct and indirect targets and victims of terrorism. This underscores again the prevalence of symbolic links from cause to motive to victim to target and objective—this symbolic tie is a key (along with the terrorists' objectives) to understanding both the act and the strategy behind terrorism. As such, this symbolic linkage is a central element in terrorism threat analysis and response planning. Finally, note that there is today a cascading of multiple possible victims, particularly directly linked victims in each of the four general target categories. The wide scope and prevalence of United States presence, power, and visibility throughout the entire world guarantees this abundance of potential victims and, to terrorists, lucrative targets. This demonstrates the extent of symbolic linkages that are possible while also pointing out how much this can complicate terrorism analysis and planning to combat terrorism today.

Objectives of Terror. John Arquilla, David Ronfeldt, and Michele Zanini develop terrorist paradigms that imply instrumental objectives. For example, in developing their Coercive-Diplomacy Paradigm, they state "From its earliest days, terrorism has often sought to persuade others, by means of symbolic violence, either to do something, stop doing something, or undo what has been done." This is a listing of instrumental objectives. Similarly, their War Paradigm implies a goal of inflicting damage within a "war," an asymmetrical strategic battle of the weak against a much stronger foe. Finally, New-World Paradigm terrorism seeks destruction toward societal disruption, leading to the replacement of the current order with one the terrorist prefers. These three paradigms form a useful typology, but it requires a good deal of interpretation to flesh out key factors and consequences of terrorism from this categorization alone.

Bruce Hoffman suggests five sequential objectives of terrorism: attention, acknowledgement, recognition, authority, and governance. According to this typology, terrorism first seeks publicity for its cause (attention), then it seeks to legitimate that cause in the eyes of the target public (acknowledgement), and it follows that legitimization by seeking the status of representation for its chosen constituency (recognition). Hoffman notes that while terrorist groups have on occasion reached those three stages, few have attained the final two. These are the award of a seat at the political table in an official capacity (authority), and control of the target political apparatus (governance). According to our categorization, the reactions and objectives sought by political, strategic terrorism are more pointed to Hoffman's first three stages and more broadly will generally fall under one of the following: Recognition, Intimidation, Coercion, or Provocation. We see these objectives as sometimes singular and sometimes simultaneous, and not necessarily sequential. Each is detailed below.

- ***Recognition.*** Recognition is important for all terrorist groups. They seek to publicize and legitimize their cause, and a terrorist incident guarantees immediate news coverage. A terrorist incident will draw attention to a particular issue and perhaps galvanize the general public to support the organization's cause. Incident timing and the specific victim/nature of the act is often tailored to "get the message across." For the terrorist, the media is a critical tool for getting his message out—a violent act guarantees media coverage. Media is business, and news organs will give their attention to stories that attract viewers or readers. As one observer commented, "nothing is so newsworthy as violence." There is also a concern

that if they do not give coverage to incidents, terrorism will escalate in violence until the media finally gives in. Ultimately, even the threat of violence can lead to publicity for the terrorist cause.

Terrorists also require funds and recruits, guns and materials, logistics and support. Often they seek recognition directly in support of building and sustaining their infrastructure. Robbing banks or armories, seeking publicity for recruitment as well as to further their political cause, terrorists often undertake fairly "normal" criminal acts to secure this essential support. This can be a point of vulnerability for the group, and criminal patterns should be monitored to track terrorist cycles of infrastructure building.

- ***Intimidation***. When organizations find they lack public support, they may turn to terrorist activities as a means to frighten society to act in a specific way. This is the "terror" in terrorism. The target in this case is the population as a whole, with their fear and anxiety designed to force the government or the economic system to make the changes proposed by the terrorists. Terrorists might choose as victims only those segments of the population that are linked to their cause. For instance, left-wing groups might initiate a bombing or assassination campaign against financial or industrial leaders, and "ecoterrorists" often focus their attacks on developers and the timber industry.

- ***Coercion***. A group may try to coerce the government into taking certain actions in an attempt to bring about societal changes. Terrorist incidents with coercion as the objective are quickly followed by specific demands and threats of further violence. Kidnappings and hijackings are popular tactics here because they provide the terrorists with bargaining chips and hold the possibility of being resolved without permanent injury to the victims. Such activities are often conducted in response to government actions—"revenge" by a terrorist group is primarily a means of encouraging the government not to repeat an action.

Civilian casualties are an important consideration of coercion. Terrorists realize that their demands may be lost in the confusion that would follow an incident like the destruction of Pan Am Flight 103 or the bombing of the World Trade Center. They must consider that civilian causalities may anger the public and lead to demands for government retaliation. Public officials would be less likely to negotiate with a group that committed such an act. The power, then, lies more in the threat of violence than in violence itself. For this reason, events such as kidnappings and hijackings, small-scale actions such as assassinations, and acts of violence which appear random but which cause few, if any injuries, are more likely to be perpetrated by groups that see coercion of the government as their goal.

In the face of today’s terrorism—particularly that associated with religious extremism and tactical terrorism from larger-scale conflicts, terrorism as a spill-over from international criminal activities, and the terrorism of anarchy and rage—*retribution* may be added as an adjunct operational reality to the strategic objectives of intimidation and coercion listed above. Since violence is essentially a tool for achieving a goal, and since retribution in and of itself does not advance a cause, we specifically do not suggest it as a strategic objective of terrorist violence, but rather as a related factor for violence that is designed to achieve either *coercion* or *intimidation*. In all cases, governments need to recognize the objective(s) behind the action because the entire cause-to-objective chain might then be evident, allowing the response to focus directly at the terrorist strategy. Governments need to understand the interactive linkages from the ultimate objective of the specific group and its cause to motive for the act and generator of instrumental fear pointed at the act’s target.

- ***Provocation***. Another means of increasing support for a cause is to decrease support for the government. Terrorists may commit acts designed to provoke the government into a response that will be resented by members of the public. Warrantless searches, roadblocks, repressive measures against civilians—all of these can reduce the trust people have in their government, leading to acceptance of the terrorist perspective as the more attractive alternative. Provocation can best be accomplished by attacking the government directly and inflicting significant damage/casualties on it. The hope is that there will be some within government who will seek revenge against the terrorists, and their response may have an impact on innocent, law-abiding civilians. As Fromkin wrote "Brutality is an induced governmental response . . .

that has enabled terrorist strategies to succeed in many situations. . . ."

Linkage Factors

Most significant are the linkage factors. As Bruce Hoffman puts it, "All terrorists seek targets that are rewarding from their point of view, and employ tactics that are consonant with their overriding political aims." It is these linkages that add the dynamics to terrorism, linking political cause to destructive action and further linking that destruction to its broader target and intended effect. The key linkage to the tactical environment, the linchpin that activates the strategy into an act of terrorism, is cause to action. It is here that an individual or group chooses to carry out specific acts of violence in support of the strategy. This linkage translates cause into action, and it applies the organization at the tactical level, indicating the short-term level of popular support, recruitment, and operational capabilities. Just as causes are varied and organizations range from simple to complex, action motivation is difficult to generalize. "Any explanation that attempts to account for all its [terrorism's] many manifestations is bound to be either exceedingly vague or altogether wrong." Context is the answer here, and it is the principal contribution of the strategic perspective. The broad context, the strategic environment, holds the answers to most questions about who, how, and why terrorism exists and operates at a given place and time.

The linchpin on the output side of the act is fear—the psychological effect and the critical dynamic of the terror. It too must be analyzed within the strategic context of terrorism. Strategic terrorism is, at base, an extreme form of psychological warfare, and the broader fear engendered by the act lends its ultimate credibility. The means are justified by the ends, and the end is that the target reacts due to fear. Adding in these linkages adds dynamic interactions across all of the essential components, and it is this dynamic presentation of terrorism at the millennium that we now examine.

Terrorism Dynamics

These essential components can be viewed in their dynamic interactions as depicted at Figure 2-2. The value of examining the components as they interact is that it underscores the analytical value of examining terrorism not simply as a tactic or an isolated incident but as a strategic threat within a strategic context. That full context enables the analyst to fit known details—of the group and its cause, a specific threatened target, an individual act—against other critical components to provide understanding, warning, response planning, and policy options. It highlights and relates both knowns and unknowns, allowing both forward and back mapping across the components to broaden understanding and, perhaps most importantly, to indicate the right questions to ask to fill in the critical blanks toward full understanding and effective response.

Figure 2-2: Terrorism Dynamics

Strategic Environment

A	***Tactical Environment***	
c	*Weapon*	
t		
Cause > Structure > i >	*Actor* *Victim*	F
o		e
n	*Act/Threat*	>a>Target>Objectives
		r

While terrorism is anything but linear in any of its complex dimensions, the essential components are related in linear fashion here for ease of explanation. Moving from left to right across the components as depicted here, one begins with the operational factors of group type/cause and structure. The different types of groups, whose causes were developed in some detail earlier in the chapter, adopt their own organizational characteristics. These operational factors, cause and structure, mark each type of group as somewhat unique, and they provide the will and capability components behind any given act. This combination of will and capability, then, provides the link that enables the terrorist action. Within the tactical environment, the component actor and weapon proceed directly from the operational factors—the group's recruitment, training, weapons preferences, experience, availability, etc. And the chosen act and victim are symbolically linked back to cause, as well as being dependent on the capabilities of the terrorist actor and the available or chosen weapon. Further, the entirety of the tactical components—actor, act, weapon, and victim—are specifically designed to generate fear that will instrumentally affect a strategic target or targets toward the furtherance of a strategic objective. That fear adds the element of intent to the picture, and the all-encompassing linkages are clear—from cause all the way through to objective and back again.

This representation of the interactive essential components allows general terrorism analysis and understanding, it provides a systematic structure to analyzing acts after they occur, and it facilitates analysis before-the-fact as an element of policy planning. However, again, the broader strategic context is needed to relate the individual components and bits of information into a coherent whole. Whether from the left or right, at home or abroad, it allows the analyst to understand the terrorist's strategy so that it can be countered with an effective strategic response.

Figure 2-3: Strategic Responses to the Terrorist Threat

Strategic Environment

A c t Cause > Structure > i > o n	***Tactical Environment*** *Weapon* *Actor* *Victim* *Act/Threat*	F e >a >Target > Objectives r

Tactical Response

Strategic Response Strategic Response Strategic Response

The same essential components along with their dynamic interactions indicate points of attack for an effective response strategy. These components and the dynamics between them not only define the terrorist group, its critical characteristics, and its operational, tactical, and strategic dimensions. They also point to its relative strengths and weaknesses, indicating potential response strategies to effectively counter key strengths and to capitalize on weaknesses. The terrorist can be blunted, his damage prevented or limited, by tactical response policy elements. And he can be preempted or deterred—even defeated—by strategic countermeasures that target and attack his operational and strategic nodes. The strategic context, then, with its essential elements

developed and related within an overarching strategic perspective, is at the center of both terrorism threat and response. It provides the template for a comprehensive threat assessment, and it provides the framework for systematic response policy planning.

Terrorism in Its Strategic Context: One Example

This chapter has presented the argument for such a strategic approach to terrorism—specifically for viewing contemporary terrorism within its strategic context so that all of its key elements are examined, related, and considered in formulating an effectively designed and targeted strategic response. That context, while largely developed from lessons learned in viewing "traditional" terrorism, remains applicable in slightly broadened or altered application to the "new" terrorism of the early 21st century. Now, in this final section of the chapter, we briefly discuss one case within that context to highlight the necessity and utility of this approach in analyzing the contemporary terrorism threat and planning policy in response.

The case briefly summarized here is that of Aum Shinrikyo, the group that undertook a Sarin gas attack on the Tokyo subway system in March 1995. It is selected as representative of elements of the "new" terrorism and is developed within the strategic context presented here.

Operational Factors

A central defining characteristic of the "new" terrorism is the appearance of religious extremism as a primary causal factor behind terrorist activity. In fact, some would argue that religious motivations have supplanted political causes as the *raison d'être* of modern terrorism. We see, however, a combination of religious and political threads intertwining at the heart of Aum.

Aum Shinrikyo represents the range of "new religions," hybrids of traditional elements of Buddhism and either other traditional religions or unique mixes of religious or philosophical tenets, that are fairly common in modern Japan. Aum took on an apocalyptic dimension centered on the belief that an eventual conflict would destroy the current organizing structures in Japan and elsewhere, leaving a political and social void to be filled by chaos until an intellectual and organizational force could assert itself to create a new societal order. Aum, then, on surface blended hybrid Buddhist tenets upon a foundation of apocalyptic vision. However, in anticipation of the need to step into the post-apocalyptic void, Aum maintained a very political core. The inner cadre of Aum leadership was organized into a "shadow government," with a structure directly mirroring Japan's executive department and functions. Individual Aum leaders were assigned positions to prepare to assume those duties in the new order. Aum also ran, albeit unsuccessfully, a slate of candidates for seats in the Japanese Diet.

So Aum blended the "new" religious motivation to action with the political core that has characterized "traditional" terrorism. Their preparedness to assume governmental function blended with absolute opposition to the existing government to inspire preparation for violent action to accelerate or augment the coming apocalypse and to protect the group until that day arrived. Aum developed hierarchical "operational" organs, a highly sophisticated infrastructure, and extensive support mechanisms. Using the broader religious periphery for first-level recruitment and basic funding, Aum developed business enterprises and internally selected technical expertise to support its action program. These eventually included both conventional and chemical/biological weapons labs derived from legitimate cover enterprises, and the Aum weapons program was ultimately as well financed and technically supported as many smaller government programs.

Tactical Factors

While Aum in the early 1990s was a broad-based and large, horizontal religious movement, it contained a very vertically stratified and tightly disciplined action cadre at its political center. The several violent actions carried out by the Aum cadre look much like traditional terrorism—the same individuals involved in planning and executing the acts, this group acting in close concert with an equally small and disciplined direct support

cadre, all under the direct control of the central leadership of the group.

Aum's initial employments of chemical weapons were a mix of experimental and operational action. They chose an initial victim based on direct operational significance, but they experimented with field application of their chemical weapons—in the end unsuccessfully when their effort to create a gaseous form of Sarin in the field resulted in their dispersal van catching fire. However, Aum continued with its reliance on chemical attack as their primary form of action, probably to both exploit their economic and technical capabilities in this arena and to further their end goal of creating broader effects from their action that would hasten the ultimate global conflict to usher in their rise to power. Toward this end, Aum was certainly willing to accept mass casualties, but their continuing problems with dispersal and application present a significant lesson caveat to be added to discussions of the "new" terrorism and weapons of mass destruction. Aum, in spite of its level of funding, expertise, and technical facilities and support was not able to master the employment of this class of weapons. Effective employment of WMD is not simple, nor can it be assumed to be inevitable. Perhaps more primitive application methods are best suited to such groups, at least in the near term.

Strategic Factors

In terms of victims and targets, Aum progressed from direct attacks on victims-as-targets to victims as symbolically linked to their actual target. For Aum's first (and ultimately failed) Sarin attack, the intended victim was the leader of a rival "new religion" and his followers and audience. The target of the fear to be generated by this attack was the followers of this rival group and any other citizens who represented potential recruitment targets of the messages advanced by the new religious sects—many of whom were conceivably in the audience and thus also intended victims of the attack. This connection of victims and targets is closer to pure criminality than to what we view as terrorism; however, this attack appears to have been as much about field testing the Sarin and its dispersal system as it was about the root cause of Aum. Intimidation to enhance future infrastructure development was the goal.

The second Sarin attack (also less than fully successful) was intended to kill three judges who were presiding at a trial involving Aum. The attack was planned to gas the judges, their courthouse, and an adjacent police station—again a victims-as-target attack against the direct, localized component of the justice system registering a threat to Aum. Poor planning caused the attack team to arrive after the judges had left the courthouse, and the subsequent shift to attack their apartment complex failed when the gas dispersed too widely to affect the specific apartments of interest. Direct intimidation for self-protection and enhancement was again the goal.

Finally, the Tokyo subway attack represents the ultimate application of terrorism for the purpose of intimidation toward self-preservation. Japanese national police under the Ministry of Justice had amassed sufficient evidence to mount a raid on the Aum compound and chemical weapons laboratory. The attack employed unsophisticated dispersal following the earlier failures—plastic bags of liquid Sarin punctured by the pointed ends of umbrellas. And even though the operation involved rush-hour attacks on five separate subway trains in the Tokyo system, those five particular trains were all due to arrive at Kasumigaseki station shortly before eight o'clock on a weekday morning. This station services the Ministry of Justice headquarters, and the timing would have meant that many of the passengers on those trains would have been Justice employees.

Linkage Factors

The linkages then are fairly clear. In terms of instrumental linkages from action to objectives via the generation of fear, the pattern is consistent during this early operational/growth phase of development of Aum as a terrorist group. Aum felt that its legally protected religious status under Japanese law was threatened, as well as its growing weapons program and its ultimate aim of fomenting apocalyptic violence. It used terrorist action to both directly and indirectly affect the sources of the threat. Eventually, the group planned to employ broader, mass-casualty attacks to precipitate the envisioned apocalypse and facilitate its rise to societal power.

The direct action link was the threat to growth prospects posed by a rival religious group, and more importantly the threat of legal and police action to their protected religious status, their weapons program, and to the freedom of their action cadre. These were, however, second-order action links. The initiation of the Aum weapons program came as a result of the Aum leadership's reaction to the overwhelming conventional military superiority demonstrated by the United States military in the Gulf War in 1991. They no longer believed that global Armageddon would result in the fall of existing governments—they now feared US hegemony, and they felt entirely impotent in the face of American power. Weapons of mass destruction, then, were not selected simply to cause massive casualties. They were chosen as a necessary capability in the face of overwhelming comparative weakness. The religious and apocalyptic rationale justified the level of potential casualties, but operational considerations drove the decision to develop and eventually to employ these weapons.

Thus the Aum Shinrikyo case presents a mix of "new" and "traditional" terrorism—new structures and tactics overlaid on familiar patterns from the 1970s. The strategic context and its essential components presented here continue to provide analytical keys to understanding, and we argue to unraveling, strategies of terrorism. The strategic framework presented here, then, appears to bridge from its traditional base into the new manifestations of terrorism that presents threats to United States citizens, interests, and property today. It warrants continued investigation and application to better validate its relevance to 21st century terrorism.

Implications for Strategy and Policy

"Terrorism wins only if you respond to it in the way that the terrorists want you to; . . . its fate is in your hands and not in theirs." Terrorists adapt and improve—they learn—and the US government must also learn, adapt, and improve to effectively combat and respond to terrorism today. The first step, we maintain, is to firmly establish terrorism within its strategic context, for only then can you fully appreciate the totality of the strategy of terrorism and formulate an effective strategic response.

The world—and specifically the United States government—has endured three decades of modern political terrorism, calculated violence applied toward coercive intimidation or provocation. Terrorist violence is applied for its psychological effects; to employ fear to ultimately force a government to react in some manner designed to further the terrorists' ends. Today's "new" political terrorism has found its way onto US soil, but the international experience can help defeat it before it finds deeper roots here. Experience stresses that terrorism be viewed as a process, one linking the terrorist cause and organization via motivation to the violent action, and linking that action via societal fear to its real target, the government, in order to achieve its desired political objective through government action or inaction. The process perspective based in the strategic context of terrorism also indicates the utility and necessity of a strategic response—one targeted not just at the bomber, bomb, and victim, but at the cause-to-victim-to-objective chain. A strategy of terrorism demands a strategic response, a strategy that must be proactive, comprehensive, and integrated to win.

> By itself, as has been said, terror can accomplish nothing in terms of political goals; it can only aim at obtaining a response that will achieve those goals for it.
>
> . . . The important point is that the choice is yours. That is the ultimate weakness of terrorism as a strategy. It means that, though terrorism cannot always be prevented, it can always be defeated. You can always refuse to do what they want you to do.

==

Chapter Three

The Changing Nature of Terrorism

Stephen Sloan

Introduction

As one who has systematically studied terrorism since the mid-seventies I am very sensitive to the dangers of seeking to forecast new trends in terrorists, organization, motivation, tactics, strategies, and capabilities. The very nature of terrorist organizational doctrine with its emphasis on clandestine activities makes it difficult to ascertain changes in the immediate and near future, much less engage in an over-the-horizon strategic assessment of the changing nature of terrorism. Both analytically and operationally one can contend that if there is "a fog of war," there most certainly is "a smog of terrorism," which makes it particularly difficult to look through a very opaque analytical crystal ball. The challenge of engaging in a longer-term assessment is further exacerbated by the understandable concern among policy makers and those involved in the operational arts to address the immediate threat, which often comes into focus after a particularly egregious and sensational act of terrorism. Terrorism analysis is therefore often essentially short term and reactive in nature as one crisis after another defines our understanding of terrorism through a narrow focus on the development of measures to deal with the current threat environment. Moreover, assessments often take on labels representing what may be "trendy," since they may be promoted by media coverage and temporarily be of concern to the public but not necessarily represent longer-term developments. Thus, for example today's emphasis on "Weapons of Mass Destruction," while certainly a most valid concern, is not new, but it is partially the result of the impact of the Aum Shinrikyo attacks that it is being given a level of policy and public attention that was often ignored despite the long-term concerns of scholars and practitioners in the counterterrorism community. Similarly, the bombings of the World Trade Center and the Murrah Federal Building energize policy makers to the reality of large-scale domestics acts despite the fact that these domestic threats were of very real concern to counterterrorism specialists as early as the late sixties and early seventies.

The problem of engaging in long-term forecasting is further complicated by two additional considerations. Firstly, the contexts or environments in which acts of terrorism mutate are often the result of slowly evolving social, economic, or political developments that are not amenable to current identification. The seizure of the hostages in Iran and the development of Islamic extremist groups who use terrorism as a weapon in the pursuit of their objectives were in many ways the outward culmination of a long-term, slowly emerging movement that was deeply embedded in history and that in part is a reaction to the crusades. Secondly, the rapid transformation of technology has also been difficult to predict. It took time for scholars to address the profound impact the mass media and particularly the "CNNDrome" would have on the development of modern terrorism. Who could have predicted the explosive growth of the Internet much less its increasingly profound influence on the strategies and capabilities of a new generation of terrorists? Nevertheless despite the dangers of engaging in predicting through "the smog of terrorism," the task is important if we are either constantly going to "fight the last war" (or incident) or be caught off guard by new developments on the techniques of terrorism that we have not identified. Will we be constantly caught in a reactive cycle of incident and response instead of catching up and moving beyond the rapidly changing learning curve of contemporary and future terrorists?

In seeking to engage in a future assessment it would be fruitless to attempt to identify an all-encompassing list of potential threats with a concomitant goal of developing an equally all-encompassing list of countermeasures. Change is not that orderly. Moreover this assessment will not seek a high level of specificity in discussing future challenges. Others can and will develop scenarios based on present and future strategic assessments and may also refine the means of dealing with them. Therefore the following broad-based assessment of the changing nature of terrorism is primarily intended to promote discussions of the future challenges—to look beyond and for a brief time stand apart from the daily contingency-driven threats that they must address. In so doing, perhaps one can more effectively anticipate new threats that in one form or another

==

will most assuredly threaten US national security. This chapter will therefore focus on the following areas of inquiry: (1) the environment and context that may help to identify and explain longer-term changes in the nature of terrorism. (2) the motivation that may in part stem from the changes in the environment and may transform the goals of the terrorists. (3) the impact of technological transformation on terrorist capabilities and (4) organizational doctrine that may change the long-term nature of terrorism in regard to the new demands such changes may place on those who are responsible for countering terrorism.

Before initiating the assessment it is important to note that the imperfect process of predicting is not intended to be ahistorical. There is a base line of knowledge that has identified various aspects of the characteristics and history of terrorism. While this essay recognizes that there is a degree of continuity in the goals of terrorism over the centuries since the days of the Zealots and Assassins that are important in engaging in strategic prediction, the focus of the following study will be on change, not continuity.

The Environment

On the international level the Cold War provided a degree of outward equilibrium and cohesiveness produced as a result of the balance of nuclear terror. The super-powers, having learned the dangers of direct confrontation in the Cuban missile crisis, utilized "the indirect approach" in the pursuit of their foreign policy objectives through the use of various forms of proxy war in support of client states or against unfriendly governments. Whether it was in El Salvador or Afghanistan, both Moscow and Washington sought to achieve their goals by seeking to manage conflicts without running the risk of full-scale conventional or nuclear war. While the dangers of confrontation were always possible, a degree of international order was achieved at great cost.

The imposition of outward order was particularly seen in the former Soviet Union where primordial loyalties in the form of ethnic identification, religious values, proto-national movements, or a combination of these and other loyalties were subject to the control of and often hidden under the domination of Moscow. These would surface with the call for self-determination with the breakdown of the Soviet Empire. This assertion of "primordial loyalties" of course was not solely related or limited to the fundamental transformation in the USSR and its satellites. Throughout the new states of the transitional area as well as the old industrialized states "primordial loyalties" competed with the veneer of a national identity, particularly in the former colonies, that often did not exist beyond the confines of the capitol. The "new world disorder" opened up a Pandora’s Box of new conflicts often based on deeply held old loyalties.

The assertion of these loyalties has led one authority to suggest that on the global level the competition between the super-powers has been replaced by a new paradigm of geopolitical conflict, the "clash of civilizations" where "…the great division among humankind and the dominating source of conflict will be cultural." But, it can be suggested that this paradigm is ultimately the result of the manifestation of two often-contradictory forces—modernization and tradition. What we may be now witnessing is the assertion of traditional beliefs in an expanding and increasingly interdependent social, economic, and political global environment. The very interdependence created by technology, as perhaps best personified by the impact of the medium of modern communication, has led to a reaction by forces of tradition who to varying degrees reject the construct of contemporary mass society that is often equated with what are perceived to be the highly secular values of the West. Whether this assertion, this quest for community takes place and is accommodated within a developed country—devolution associated in the Scots, Welsh, and the continued conflict in Northern Ireland, or whether it transcends a region—the full sweep of Islamic fundamentalism, one fact remains. We are not witnessing the "End of History" but the reassertion of traditional values in an expanding technological environment. As a result of this tectonic geopolitical shift, political violence in its many forms and particularly in regards to terrorism has become a central aspect of contemporary societal and political competition, replacing the rhetoric, strategies, visions, and tactics that were either used to motivate or explain terrorism as an aspect of super-power competition motivated or justified on the basis of competing ideologies.

==

In conjunction with the assertion of traditional loyalties is the increased breakdown of the nation-state as the major entity in international affairs. The state-centric model is now under assault as the superficial loyalty to idealized nation-states, particularly in the Third World, has been replaced either by transnational movements or subnational movements that are rejecting the legitimacy of the arbitrary constructs of states that were largely the result of the imposition of legalistic or physical boundaries of nation-states that ignored the more profound psycho-social boundaries that can bring people together or apart. With this breakdown of community, legitimacy, and order, we are now confronted with the reality that large areas of the world are for all intents and purposes ungovernable and are in effect part of the "...the world's 'gray area' where control has shifted from legitimate governments to new half-political, half criminal powers." The mythic body politic that defined and institutionalized terms of the relations among nations and the politics within states is now being transformed as new players now seek to alter the course of international politics.

These new players will certainly be influenced and will utilize what could be called "a revolution in terrorist affairs" fueled by the technological revolution that also characterizes contemporary international affairs. As we shall see, this revolution will at the minimum lead to the continued enhancement of the weapons that can be used by the terrorists—from fertilizer bombs to portable nuclear weapons. Such innovation will also have profound impact on the ways in which terrorists will spread their message of fear and intimidation—from pamphlets to the Internet. And perhaps most significantly, terrorists' technological innovation may also have a profound impact on the development of new organizational doctrine that will greatly enhance the ability of a new generation to increase their capabilities and yet at the same time make it easy to avoid detection.

The changing environment and the context in which terrorists will operate will therefore transform an enduring threat that at one hand uses the weapons and tactics as old as history with the most modern instrumentalities of violence today.

Motivation

While traditional motivation to resort to terrorism will continue and indeed be amplified because of the assertion of "primordial loyalties," the motivation may be analyzed as a function of frustration, relative deprivation, ethnic, racial, and religious strife, and other commonly ascribed causes of violence. Motivational factors may also change in response to the new conflict environment.

At the outset, the cosmopolitan ideology that was used to fuel wars of national liberation as well as campaigns of terrorism has largely lost its salience in contemporary political life. While Marxist-Leninist thought may almost have been assigned to "the dust bin of history," it did provide a world view and accompanying coherence in the form of doctrine, ideology, and strategy that was used to foment classic revolutionary "internal wars" and regional conflicts which employed terrorist acts and campaigns in the name of and for leftist ideologies. What will replace a blueprint—a strategy—for the use of violence and terrorism as an aspect of political protracted warfare that, however challenging, was understood and therefore capable of being countered through the appropriate policies, doctrines, and strategies?

In the first place just as we see the assertion of traditional loyalties, we will also witness the increased significance of such values in motivating those holding primordial loyalties to reassert themselves as we enter the new millennium. Rising religious fundamentalism will increasingly be employed to recruit terrorists and justify their acts by movements and organizations who reject the existing state system and its secular values. While there has been a focus on Islamic fundamentalism, it is vital to remember that all the major religions have their own zealots who in their rejection of the current order are not seeking to replace one political system with a theocracy or a system that most closely reflects their religious beliefs and practices. Both Middle Eastern and what can be called the American Ayatollahs share much in common. They seek a fundamental transformation in core values, and their applicability to the political, economic, and social system. It should also be noted, particularly in the case of various fundamentalist sects in Islam and Judaism, that there is no separation between church and state. Furthermore these extremists who may resort to terrorism view their objectives to be divinely

==

ordained and therefore will never be satisfied in seeking compromise "solutions." For they not only have a commitment to engage in what has traditionally been called a "protracted war," but a protracted Holy War, which is grounded in historical myth and reality and affirmed on the basis of achieving preordained goals over the long term. Armed with the strength of a commitment that transcends secular politics and indeed a temporal world, the new breed of terrorists as we shall see may not be concerned about public opinion in this life as they seek to achieve their goals. The suicide bomber by his or her act of destruction is engaged in a transcendental personal journey that places no limits and indeed justifies mass terrorism. This transformation will have serious implications on the ability of analysts to understand those who are motivated by the most fundamental beliefs since their beliefs will not necessarily be concerted to action on the basis of a rational choice or cost/benefit model of decision-making but will be driven by a commitment that ignores our attempts to primarily understand terrorism in the context of purposeful, rational violence to achieve a readily identified goal. Moreover the proliferation of sects with their inclusiveness, paranoia, charismatic leaders, and beliefs that cannot be understood in the context of traditional religious doctrine opens up yet another area of profound uncertainty and danger in terrorist innovation; uncertainty, because it will not be clear what these groups want, and danger, for they will have at their disposal and be willing to use weapons of mass destruction and may not be concerned with limiting their violence so as to not totally alienate public opinion in the quest for their goals.

The changing nature of terrorist motivation will further be complicated by the increased significance of new non-state actors who may use political rhetoric as a means of justifying their acts of carnage, when in reality they may be ultimately apolitical. These apolitical terrorists come from an ancient tradition or organized and unorganized crime going back to the syndicates of the past—the Cosa Nostra, the Triads, and now the Russian mafia. Their power has increased with the breakdown of the nation-state system. They have found a fertile ground for extortion and other criminal activities in the "gray area" and will increasingly use terrorism to achieve a degree of power and wealth. They have and will increasingly attempt to form alliances, work with or co-opt governments and, in so doing, achieve a level of legitimacy undreamed of by such groups in the past.

The motivation will also be changed by the emergence of "single issue" terrorists groups who will increasingly utilize modern technology and particularly the Internet to dramatize and coordinate acts of terrorism in the pursuit of their own often very idiosyncratic objectives. These groups will be very difficult to counter given their small size, their lack of a track record and coherent and well-known programs of action, and they will not fit within the past ideological spectrum of former terrorist groups that often explained particular terrorist goals during the Cold-War epoch.

What will also complicate terrorists' motivation will be the possible emergence of new groups that will practice and refine their own form of "terror from above." These groups will not necessarily be utilizing terrorism as an instrument of state repression. They may not be the right-wing death squad of the past but the amalgam of criminals, and apparecnicks who will use terrorism to maintain state repression and power. They represent the evolution of modern feudalism and fiefdoms that will not seek political legitimacy as a means of maintaining control. The "new lords" will combine the traditional means of engaging in regime repression with the technologies of control and intimidation that, as we shall see, are a manifestation of a "revolution in terrorist affairs."

The above analysis does not mean to imply that traditional motivations will not be significant in promoting future terrorists acts. But it is necessary to recognize that there are new actors, with changing values and goals that will be major forces in shaping the changing nature of terrorism.

Technology Transformation

It is perhaps the transformation in technology that will most significantly alter the nature of terrorism in the 21st Century. Just as the introduction of jet aircraft in the late 50's and early 60's transformed territorial terrorism into a form of non-territorial terrorism which used the medium of space to conduct operations and the introduction of satellite television enabled terrorists to almost instantaneously reach a global audience, so have

==

new developments increased their capabilities.

On the lower level of the technological spectrum, while classic bombs in the form of fertilizer and oil and their modern replacement, Semtex, will continue to be used, one can anticipate that a whole host of more compact and powerful explosive materials will be available to the terrorist. The compact nature of the material coupled with its changing composition will make such material even harder to detect even as a wide variety of new sensors have been developed to assist the traditional x-ray and magnetometer as illustrated by the employment of the thermal neuton activation technique to detect explosives. The constant battle between those who develop detection technology and those who develop counter techniques of masking explosive devices and other agents of destruction will in all probability intensify with the acceleration of technological innovation. The problems associated with detection and screening will further be complicated by the proliferation of relatively easy, small, hand- and shoulder-held weapons along with other portable devices. Furthermore one can anticipate a further miniaturization of terrorist weapons systems.

The unfortunate enhancement of terrorist destructive capabilities and concomitant tactical flexibility will further be enhanced by the continued development and availability of laser weapon systems that have already very effectively "painted" targets. Therefore a new generation of terrorists will have very marked improvement using new "stand-off weapons" with a far greater degree of accuracy than the "stand-off weapons" of the past. The challenges to those responsible for developing effective counterterrorism physical security means in general and those who must specifically address force protection requirements are very daunting. Furthermore, these new weapons capabilities will make it increasingly difficult to establish effective perimeters and fixed security zones against them. How can even the most innovative, technologically sophisticated physical security measures cover enough territory and be impenetrable to neutralize a new family of weapons including the increased use of electromagnetic pulses? Moreover one can also anticipate that the current development of a wide variety of non-lethal weapons will also enter the terrorist arsenal giving them another tool to engage in both psychological intimidation against the immediate victims and a larger target audience. Such weapons which ideally attempt to make the application of force in law enforcement and warfare "more humane" may be a potent "fear multiplier" in the hands of a dedicated and skillful terrorist.

In both the short and long terms, the impact of technology on terrorist weapons and capabilities is particularly significant in an increasingly more lethal terrorist threat environment. On one hand the existence of portable nuclear devices is of a current concern especially given problems of inventory and command and control in the former Soviet Union. In addition, the technology to develop such weapons can now more readily be disseminated along with information on two companion threats in regards to mass terrorism—chemical and biological weapons. In regards to these weapons a major problem for terrorists has been the danger that they can fall victim to the highly volatile material they handle and the problems associated with targeted or general dispersal of chemical and biological agents. Unfortunately one can readily anticipate the dispersal technique or the delivery systems will improve in conjunction with more effective safeguards in the illicit manufacturing of such weapons.

What has been particularly significant has been the logical extension of the profound impact of television and satellite communication through the rapidly developing and expanding use of the Internet and the revolutionary change that characterizes all aspects of computer technology. The terrorists now have at their disposal the medium to disseminate information and increasingly coordinate attacks against a wide range of targets from the relative safety of cyber space. In addition they will increasingly be able to conduct terrorism against the vulnerable technological infrastructure of industrial and post-industrial societies by targeting critical infrastructure, particularly in reference to computer facilities and networks. Through their actions, they will have the potential to directly and indirectly place large numbers of people in harm’s way by degrading an air traffic control network, public health care system, or other complex system that can profoundly threaten both personal and societal security.

The technological transformation, particularly through the Internet will also equip terrorists groups with a

==

new weapon of terrorism—virtual terrorism. Even if their threats may not be actualized through the use of the net, they magnify their threat. In effect they can create a climate of fear and intimidation that is a hallmark of terrorism by utilizing the Internet to not only spread their message of intimidation but also by create the perception that their threat has become a reality. The tragic case of TWA 800 illustrates the point. Pierre Salinger's contention that the aircraft was shot down by a missile was the product of a report from the Internet that was not validated. Yet, despite the conclusions of careful investigations, the missile theory still "has legs" grounded in the perception of an increasingly cynical public who utilizes conspiracy theories as a means of seeking to understand the complexities of modern political life. The Internet has been used to announce the Abu Nidal organization's Jihad and the intents of numerous other groups as well. If as Brian Jenkins noted, "terrorism is a form of theater aimed at the people watching," it is now a form of Internet communication where people can think they are actually experiencing an act of terrorism.

Beyond these future threats created by technology exist a whole host of new weapons, targets, and vulnerabilities that have yet to be identified. I will defer to the futurists. But one thing is quite clear—while terrorists have in many ways utilized traditional weapons of destruction and will continue to do so, they are not adverse to, and are indeed very innovative in, refining their capacity to engage in murder with frightening efficiency.

Organizational Doctrines and Capabilities

There is one area of change that may be at the nexus of the changes in the terrorist environment, motivation and technological transformation—terrorist organizational doctrine and attendant capability. The following discussion is not meant to imply that the core of understanding the dynamics of the changing nature of terrorism is predicated on organizational change by itself, but the impact of that change may none-the-less be very significant in charting the nature of terrorism in the 21st century.

Presently we are witnessing the emergence of a wide diversity of terrorists groups. While there will still be state sponsorship, sophisticated regional and transnational terrorist networks, we now also see a myriad of new groups who are held together based on commitments to a wide variety of sub-national loyalties, religious/cultists beliefs. In effect what we have seen and will increasingly see is the development of the "free floating terrorist group," a small cell-like organization that is not as in the past a combat compartmentalized entity that is part of a larger clandestine hierarchy. This type of stand-alone, mini-terrorist group may operate within an environment of racial, ethnic, and anti-government hatred, for example, but it does not have specific organizational ties to a larger organization nor is dependent on some level of support from a larger organization, a front group or a sector of the community. These "free floating" groups have already made their horrendous mark in the United States experience. Thus, while conspiracy debate will continue, the fact remains that a small terrorist "free-floating group" was able to perpetrate the worse domestic terrorist act with the bombing of the Murrah Federal Building in Oklahoma. In addition terrorists well-trained in survival techniques have and will continue to evade detection because of their skills and size. Eric Robert Rudolph, currently on the Federal Bureau of Investigation's 10 Most Wanted list after being linked to bombings at the 1996 Olympic Games and Atlanta area clinics, continues to evade authorities. These "bubba cells" should not be taken lightly. They serve to underscore that one does not need sophisticated organizational design or capabilities to engage in major acts of terrorism. Furthermore, given their small size and the fact that they are not dependent on a larger organization or community, they are difficult to identify, intercept, or penetrate than more sophisticated organizations with their own networks and track records. The term "small is beautiful" is unfortunately most salient in the changing terrorist organizational doctrine of various terrorist groups.

The potency of such organizations has long been realized. In J.K Zawodony's pioneering article "Infrastructures of Terrorist Organization" the author discusses what he calls the "centrifugal infrastructure" of terrorist groups. According to him, such structures have significant advantages over the traditional "ladder hierarchy" that characterizes most organizations and particularly governmental bodies' organizations in general and more specifically the security, police, and military forces responsible for countering terrorism. Such

==

advantages include direct and rapid communication and independence from society support. As governments seek to counter this organizational advantage two fundamental questions must be raised: (1) Can one use a ladder hierarchy to defeat a centrifugal hierarchy? (2) Can a government effectively develop centrifugal hierarchies while maintaining command and accountability over such organizations?

The strength of the centrifugal organization will in all likelihood be intensified because of technological advancement. In the past the centrifugal "free floating" nature of such organizations had an adverse effect on these groups to engage in coordinating campaigns of terrorism. But now that negative effect has been lessened via the Internet. For the Internet can provide a means for coordination among these mini-groups without sacrificing their independence and unity. The impact of the computer and particularly the medium of the Internet has led to the development of netwar.

> …the term netwar refers to an emerging mode of conflict (and crime) at societal levels, involving measures short of traditional war, in which the protagonists use network forms of organization and related doctrines, strategies and technologies attuned to the information age. These protagonists are likely to consist of small dispersed groups who communicate, coordinate, and conduct their campaigns in an internetted manner, without a precise central command. Thus, netwar differs from modes of conflict and crime in which the protagonists prefer hierarchical organization doctrine, and strategies, as in the past efforts to build, for example centralized movements along Leninist lines.

David Ronfeldt then provides excellent illustration about current organizational innovation and the future direction of terrorist organizational doctrines and strategies.

> Netwar is about the Middle East's Hamas more than the Palestine Liberation Organization (PLO), Mexico's Zapatistas more than Cuba's Fidelistas, and America's Christian Patriotic movement more than the Ku Klux Klan. It also is about Asian Triads more than the Sicilian Mafia, Chicago's "Gangsta Deciples" more than the Al Capone Gang.

The modification of the traditional terrorist's centrifugal organization through the use of the computer and the Internet fused with the growing significance of non-state or non-governmental actors will provide terrorists with a degree of flexibility coupled with an ability to coordinate attacks without loss of security. The modification may also force counterterrorism analysts to reorient their frame of reference beyond the model of traditional terrorist organizations which often combined a hierarchical organization in terms of leadership with the cellular nature of the combat cell. There will be an absence of a highly organized and identifiable terror network that in the past could be penetrated by technical intelligence or when state sponsorship did exist through penetration via the hostile intelligence service. Again it is worth noting that government counterterrorism organizations increasingly model themselves at the tactical level using the centrifugal model of their adversary without the loss of accountability and control that could lead, as in the past, to the development of "rogue elephants" whose absence of accountability may also lead to ignoring the policy directives of the political leadership.

Finally, the reorientation of counterterrorism organizations will require closer integration with non-state actors who are increasing their capability to act independently of government authority in the conduct of counter terrorist operations. Corporate and private counterterrorism services have increased in terms of numbers and, while their quality is uneven, there are "state of the art services." But would such services be willing to share proprietary information concerning threats that directly affect their organization, and on the other pole, would government at all levels be willing to share equally sensitive information with the private and corporate sector?

Conclusion: Placing the Threat in Context: Short- and Long-term Implications

The history of modern terrorism can be characterized by terrorist innovation manifested in threats and acts of violence followed by reaction on the part of governments at all levels. There is a major theme that emerges in

==

the so called "war against terrorism," that it is a "war" which is primarily defensive and a "war" where short-term tactical considerations are not integrated into or take precedence over the vital requirement to develop long-term counter terrorism policies, doctrines, and strategies. In the short term the focus shifts from one major group (or personality) to another—from Carlos to Bin Laden, and from low-level threat awareness to high-level concerns—usually after an incident as in the case of Aum Shinrikyo and the current concern about weapons of mass destruction. This is not to negate the danger of current threats, but the changing nature of terrorism will place a heavy responsibility on policy makers, analysts, and planners to look beyond the present threat environment and address the continuing impact of the dialectic of modern terrorism—the clash between traditional primordial loyalties versus an assertion of regional and universal demands, of low-tech weaponry versus high-tech weapon systems, and the power of the pen vis-a-vis the impact of the Internet, and the clash of accompanying motivation varying from deeply held religious beliefs to terrorism as a mercenary industry.

Unfortunately, given the focus on current threats, changes in the political climate, the recurrence of bureaucratic turf battles, and now more than ever the need for international cooperation to combat terrorism in an increasingly discordant and fragmented world "order," the future of the war on terrorism remains as bleak as the vaunted war against drugs. Admittedly, the causes for violence that lead to terrorism, as in the case the demand for drugs, are in part the result of more deeply embedded and very intractable societal problems that are difficult to resolve. But unless policy makers, planners, analysts, scholars, and most importantly the international community—however fragmented—attempt to see through the "smog of terrorism" and recognize the changes in the nature of terrorism, they will enter a new century which will be marked by acts and campaigns of terrorism that might lead not only to mass casualties but destroy an increasingly fragile interdependent social order.

Chapter Four

WMD Terrorism: Hype or Reality

David Kay

One of the most challenging tasks for any analyst or policymaker is to assess the validity of a threat that has not yet fully emerged. Such a determination is the foundation of deciding the level of resources that should be devoted to countering it and consequently not devoted to meeting validated and present needs. To act early may well head off a threat or, at least, lessen its consequences when it does finally emerge. When the threat potentially has the ability to inflict mass casualties on your own civilian population and perhaps alter the very shape of a free society then the requirements of leadership demand that such a threat be given serious thought. On the other hand, to act early may well waste resources on the worst case nightmares of the chronically paranoid and drain resources away from those that must contend with the day-to-day gnawing away of a hundred less dramatic, but already present, real emergencies.

We find ourselves today faced with just such a dilemma with regard to the potential use of weapons of mass destruction by terrorists. The description of the horrors that may await us as nuclear, chemical or biological weapons fall into the hands of terrorists have become the staple of Hollywood, pulp fiction and, now, serious analysts. The Deutch- Specter Commission Report ranks "Terrorist use of weapons of mass destruction against the United States or its allies" as first among "the most serious threats facing the United States. Thoughtful studies are being undertaken of how the country should prepare to respond to the challenge that such threats would represent, real budget decisions are being made, and new capabilities are starting to be deployed. On the other hand, the empirical evidence for believing that there is a threat of WMD terrorism seems to be as elusive as the challenge of preparing for it is daunting. Terrorist acts remain principally confined to specific countries and regions—Sri Lanka, Colombia, Algeria, the Middle East—and even in these areas the preferred weapon of choice remains an improvised high explosive device. While attacks on Americans have shown an increase in the last few years, terrorist incidents, in general, are less widespread than two decades ago.

Against this set of "facts", some have wondered whether WMD terrorism is not just the latest hype to come along as fertile imaginations are exercised in an environment lacking in real enemies or an American over reaction to a series of tragic, but isolated attacks. This group asks, "Where is the threat—Is it real?"

While analysis under conditions of extreme uncertainty is never easy, there are guideposts to which one should pay attention, although these guideposts are derived as much from our failures as our successes. First, among these is *suspect the trends*. Trend analysis and databases are valuable, but dangerous, tools in the hands of analysts. At best they are a guide to the past and can show us what the future will be like if it chooses to conform to the past. If, however, the problem is that "the future is no longer what it once was" then trend analysis and databases become the blinders that keep analysts from seeing discontinuities and transforming events. The IRA as a terrorist threat between 1940 and 1957 would have been judged a non-existent threat, a conclusion that a decade later would have been found woefully uninsightful. All too often, we in the analytical and policy communities ignore the most obvious limitation of databases and the trends they project. Databases only collect what we either can or choose to measure and ignore what we know we cannot or choose not to measure. For example, many look at the most widely available databases on terrorism and say they can find no evidence of a growing terrorist interest in using any of the weapons of mass destruction. Yet we should all know that these databases only collect terrorist attacks or attempted attacks that are reported in the public press. Terrorist actions that are thwarted outside of the glare of the press and that for reasons of continued operational necessity must remain unreported are not recorded. Other information that may be gained through national collection means of ongoing discussions and planning of terrorist groups and state supporters, if it exists, has to

be closely held. Public statistics have, at times, mislead even informed academic analysts to assert that the IRA and PLO could not be as skillful opponents as governments were asserting because these bombers were frequently blowing themselves up as they attempted to assemble and place their bombs. Little did outside analysts know at the time that governments were engaged in active measures to ensure that defective bomb-making material was entering into the terrorist inventory and that special techniques were deployed around vulnerable areas to disrupt devices before they could be planted. The statistics were wrong and consequently so were the conclusions of those who relied upon them as a guide for drawing conclusions.

If trend analysis can mislead, what other guideposts are out there to help the analyst or policymaker understand whether they may be facing a dynamic situation in which the wisdom of the past is best left to understanding the past, not guiding the future? While certainty is impossible and ambiguity will always remain—at least until the blinding event occurs that makes an only theoretical possibility real—there is one fundamental approach and nine guideposts that should be examined. The analytical posture must be one of constantly probing our world to see if there is an answer to the ritual question of *"why is tonight different from all other nights"?* In our zeal to describe and explain, we in the analytical community sometimes forget we have a more fundamental duty to test the world of our data for its surprise potential. In the world of terrorism and specifically the potential of WMD terrorism let me suggest nine guideposts that should be constantly assessed. These are:

1. Are the fundamental capabilities and/or access to new WMD-related capabilities of terrorists changing? Are they seeking to acquire new capabilities that would fundamentally alter their ability to threaten American interests?
2. Are the fundamental factors that motivate terrorists to take actions and that shape the types of actions they are willing to undertake changing?
3. Is the intent of terrorists with regard to what they hope to accomplish with attacks on American interests changing?
4. Are there significant United States vulnerabilities that open the possibility to terrorist attacks with WMD that, if successful, could provide a terrorist group a decisive advantage to accomplishing its objectives?
5. Are the consequences of a terrorist use of WMD likely to produce consequences that will deprive the United States of the ability or will to undertake actions to defend its interests or those of its allies or that will require actions that will alter American society in a significant manner?
6. Are the political, technical and military barriers to terrorist use of WMD falling?
7. A re their new potential terrorist groups or state supporters of terrorism emerging?
8. Are effective response capabilities to terrorist use of WMD so low that their absence could itself become an added inducement to the use of WMD by terrorist?
9. Has there been an increase in motivational models—either real or in popular culture—of terrorist use of WMD that might serve as a patterning or copy cat guide to further use of WMD by terrorists?

It would take a more extended study than there is time or space here to provide a detailed assessment of each of these guideposts against our knowledge of the evolving terrorist threat. On the other hand, even a quick scanning of these against easily available open source information is disquieting.

The end of the Cold War and the collapse of the Soviet Union have opened a floodgate of information, technology and skilled personnel all too familiar with WMD. New means of communications, particularly the Internet, have made possible long-distance, hard-to-detect collaboration and difficult to trace financial exchange mechanisms. New suppliers have arisen and non-proliferation regimes are becoming increasingly ineffective.

Beyond changing capabilities, the motivations for terrorism seem to be undergoing some fundamental changes. The classical understanding of terrorism involved the use or threat of use of violence in pursuit of political aims with most terrorists being motivated by either political or ethno-nationalist aims, and in either case, violence was carefully calibrated to advance a goal that almost always involved a rearrangement of

political power. To this mix more recently has been added quasi-religious and millenialist groupings with less clear aims and fewer constraints on their use of violence. Additionally, there appears in several regions to be a falling of constraints on violence and a rise of a culture of death where the affirmation is "I die I am." The despair on the streets of Algeria, Sri Lanka and in parts of the Middle East should warn us that old constraints on violence may not be an adequate guide to the future. And before we become too optimistic about the early signs of success in removing old reservoirs of terrorism in southern Africa and Ireland, events in the Balkans should remind us that we are also creating new reservoirs—or maybe better put, refilling very old ones.

Just as motivations are changing, so are the professionalism, technology and level of cooperation among terrorists. From pipebomb to car bomb to truck bomb all filled with more energetic explosive material the ladder is being climbed. While many of the devices and attack plans remain crude, where the terrorism continues over time the lesson is that the terrorists have become more sophisticated to counter improvements in the countermeasures of governments. In Ireland, Israel and wherever the narco-criminal gangs operate one can plot a steady upward curve of measure and countermeasure as the forces of society and terrorists struggle for dominance.

A hard lesson for those schooled in the formal military strategy and intelligence norms of the Cold War is that the prime importance of assessing and validating threat before developing requirements and subsequently capabilities is not applicable to terrorism. Terrorists go to vulnerabilities. Or put another way, vulnerabilities attract terrorists. Embassies in East Africa may seem a long way from the Middle East, just as Lockerbie, Scotland is a long way from Libya or Iran, but to a terrorist their attraction is that they are not inside the "moat" of highly valued assets that are carefully guarded. Civilian society in a democratic polity is the most vulnerable of all areas and the hardest to protect without changing the norms of society.

The largest generic vulnerability of the United States is that our complex federal system has left us with emergency responder forces that simply do not scale to even rudimentary WMD events. Police, fire and emergency medical services are locally derived and often staffed with a substantial number of volunteers. Local politics and budgets limit cooperation among many of these forces. Equipment and training requirements are derived from the daily burden of emergency events that such units face. When criminals acquire new weapons—military-style automatic weapons—or new tactical skills—encrypted communications and interception equipment—the local forces have faced major problems in responding. The economics of health care has led to a substantial reduction during the last decade of hospital beds in every metropolitan region of the United States. Mass casualties of either civilian populations or responder forces are not requirements that these forces generally have been scaled or trained to meet.

We are in a period when the overwhelming military might of the United States is becoming clear even to the slow learners among the world’s miscreants. Frontal assaults on interests that the US define as important invite a high level of conventional destruction and the opponents’ conventional counters are unable to inflict significant losses—even when "significant" may be defined as in the less than 100 category—on the United States and its allies. Two developments seem inevitable. The overwhelming dominance of the United States will foster greater resentment. Secondly, nations will seek courses of action that will allow them operational freedom from US conventional attack or, at least, the ability to inflict significant losses on the United States if it does attempt to frustrate their ambitions with military actions. Terrorism, and particularly, mass casualty terrorism, is a logical counter for such states. Chemical, biological and radiological terrorism offers tremendous difficulties of attribution—that is proving who really carried out an attack. Biological terrorism even has the added difficulty of determining or proving that one is really under attack and not simply seeing a natural disease outbreak.

Popular culture—movies, novels, video games and Internet chat rooms—are awash with chemical, biological and nuclear terrorism. The Secretary of Defense is threatening on Sunday television the population of the United States with a five-pound bag of sugar/anthrax in the hands of the Iraqis. We are vaccinating our military against anthrax and the Foreign Service is to follow. The Aum Shinrikyo, in this case a real terrorist group that

reads like bad fiction, loosens a Sarin nerve gas attack on the Tokyo subway. The President of the United States, in response to a popular novel, openly convenes an expert group of government and outside experts and then announces a $10 billion dollar program to respond to the threat of biological terrorism. Russian defectors tell us of the biological horror that the Soviets had planned to unleash on the West. The world having eliminated smallpox as a public health disease decides not to eliminate the last remaining cultures of the disease out of fear that someone may have cheated and we will need these stocks to cope with terrorists equipped with smallpox. Only a blind, deaf and dumb terrorist group could have survived the last five years and not been exposed at least to the possibility of the use of WMD while the more discerning terrorists would have found some tactically brilliant possibilities already laid out on the public record.

This all too quick look at the guideposts to analytical surprise suggests to this author that there is sound reason for believing that attempts at mass casualty terrorism deserve to be taken seriously. Terrorism in any form is extremely difficult to identify, track and counter. Data over the last several decades continue to show that approximately 90 percent of identified terrorist groups last less than one year and that only about 50 percent of those that make it beyond one year last a decade. Terrorism is to a large extent a "pop-up" target of loners and groups at the extremes of society. Short duration, isolated individuals and groups pose serious problems for intelligence and law enforcement. If they are embedded within US society there are significant legal and political hurdles to even monitoring their activities prior to criminal actions.

In this period where analytical warning can, I think, reasonably be given to policymakers that mass casualty terrorism looms as a real possibility, what are the priorities for government action? Let me get the obvious ones out of the way first, not because I believe they will really work, but because I think we would be extremely remiss if we did not attempt to gain some advantage from them. Actions that can deter and prevent terrorist use of WMD do need to be stepped up. Such actions include better intelligence—principally human intelligence—targeted against terrorists; better forensic and detection capabilities so that we can quickly and with high confidence understand from where a terrorist attack has originated and been supplied; and removing the obvious vulnerabilities such as those that leave US Embassies and American businesses abroad as easy targets and make US ports of entry and borders inviting welcoming points for WMD devices.

Second, and with far greater urgency than we have shown to date, we must begin to assemble and exercise the resources that will allow us to manage the consequences of attempts at mass casualty terrorism. If we cannot prevent—and I do not believe we will be able to—attempts by terrorists to use WMD then it is essential that we be able to respond to such attacks in a manner that lessens their impact, reassures our citizens that government can respond to such attacks effectively and without having to distort the fabric of a free society and take away from the terrorists any sense of accomplishment. Much more assistance must flow directly to helping local police, fire and medical responders better equip and scale their efforts to the challenges of mass casualty terrorism. They need more and better equipment and more realistic training that allows them opportunities to learn how to cooperate across jurisdictional boundaries and to maintain operational effectiveness even when their own ranks may be suffering from unprecedented casualties, for example, from the effects of biological attack. The Federal response force must overcome its own jurisdictional fragmentation and rivalries. Perhaps even more difficult, we must learn how to bring to bear the considerable resources of the US military in support of managing the consequences of mass casualty terrorism while at the same time respecting the Constitutional and political realities of a federal democracy. It is tempting to believe that the military’s obligation to defend the United States stops at the border—and actually should be pursued as close to the border of a foreign attacker as possible. And this is certainly one obligation and one that is not likely to disappear. On the other hand, if mass casualty terrorism on some scale that is quite possible does occur, it is likely that only the US military will have the organization, logistical capability and trained manpower necessary to reinforce the local responders. However, for this capability to become real and effective, this is a mission that must be accepted, resourced and exercised with local responders. This is not yet adequately the case.

Finally, we have significant gaps in equipment and technologies necessary to make a response to mass casualty terrorism manageable. These gaps include: chemical and biological detectors that actually work in real

field conditions in the hands of actual emergency responders; quick and accurate analytical techniques for the attribution of the source of attacks; decontamination techniques that meet the needs of actual environments where attack will occur; protection equipment that is affordable and that does not significantly reduce the operational effectiveness of those using it; protection gear for civilians under attack; protection technologies that can be incorporated into buildings and transportation nodes that reduce their vulnerability to attack; and much better medical therapeutics that provide protection against a wide range of biological agents and treatment for those who have been attacked.

Chapter Five

The Cyberterrorism Threat

Gregory J. Rattray

The last decade of the 20th Century has seen the rising concern over a new form of conflict, usually referred to as information warfare. As the US and other nations race forward into an information age, reliance on advanced information systems and infrastructures has grown significantly. Cyberspace has become a new realm for the exchange of digital information to conduct commerce, provide entertainment, pursue education, and a wide range of other activities. Information systems, in particular computer software and hardware, now serve as both weapons and targets of warfare.[1] The possibility of warfare in cyberspace presents opportunity but also involves significant new security risks. As the world's leading military power and the society most reliant on its information systems and infrastructures, the US may well face adversaries searching to find new weaknesses. These adversaries may include terrorists.

Similar to political assassination and car bombs, cyberterrorism could provide a new set of weapons for the weak to challenge the strong. Rapid technological developments based on the Internet and other information infrastructures through the end of the 20th Century create an attractive environment for groups who can not directly confront the US government, yet are willing to use death, destruction and disruption to achieve their objectives. Increasingly, cyberterrorists can achieve effects in the US from nearly anywhere on the globe. Terrorist groups can access global information infrastructures owned and operated by the governments and corporations they want to target. Digital attackers have a wide variety of means to cause disruption and/or destruction. Response in kind by the US government against sophisticated attackers is near impossible due to the difficulty of pinpointing activity in cyberspace and legal strictures on tracing attackers.

The possibility of cyberterrorism receives much attention. The Director of Central Intelligence, George Tenet, cautions about "a growing cyberthreat, the threat from so-called weapons of mass disruption."[2] Noted terrorism expert Walter Laquer observes "… why assassinate a politician or indiscriminately kill people when an attack on electronic switching will produce far more dramatic and long-lasting results."[3] A RAND study on terrorism produced for the US Air Force outlines the possibilities of "cybotage—acts of disruption and destruction against information infrastructures."[4] Yet, so far the US has suffered very little from cyberterrorism despite continuing conflicts with numerous adversaries, including those who employ terrorist means. Improved understanding of cyberterrorism must address why it has yet to fully emerge as a prevalent terrorist strategy. US policymakers need to understand constraints on its conduct as well as possibilities for its use.

What do we know? Evidence exists that cyberterrorism can occur. Government and commercial web sites are defaced almost daily. Computer systems suffer disruptions from intentional e-mail overloads and eruptions of viruses. Hackers of many stripes continue to prove capable of intruding on and exploiting a wide range of computer networks. These incidents can cause significant disruption and financial costs. However, cyberattacks have so far proved at most a nuisance for the US and its national security.

Looking to the future, we can expect cyberterrorism to become a more significant national security concern. Many assert that the US must expect a growth in the number of adversaries willing to use terrorist means.[5] The effectiveness of digital attack means will increase. So will US vulnerabilities to cyberterrorism. Terrorist organizations that wish to use these means can be expected to become smarter about both technological tools and effective targeting strategies. Limits to hitting back against cyberterrorism will remain a difficult problem.

Yet, cyberterrorists too will face significant challenges. When terrorists will develop requisite capabilities to conduct significant cyberattacks remains highly uncertain. The calculus of how cyberterrorism fits in with other

terrorist tools, including conventional weapons, weapons of mass disruption, and other techniques will determine the future significance of cyberterrorism. Cyberterrorism may well become a supplement to other terrorist means similar to how information warfare operations complement conventional military forces.

The US President, Congress and many others have clearly recognized concerns raised by cyberterrorism. The Federal government has initiated planning, assigning responsibility, and begun development of organizations to protect the US from cyberattack. However, these efforts are in early stages and must surmount considerable hurdles. The speculative hype combined with lack of real experience with this emerging phenomenon compounds the difficulty. A sound US policy to combat cyberterrorism and investment decisions must emerge from a balanced understanding of the potential threat and its limits.

Cyberterrorism—What Is It and Who Does It?

In general, terrorism proves a difficult topic to set boundaries around. One common approach to defining cyberterrorism is broad inclusiveness in addressing the actors, means and goals involved. My approach endeavors to delineate the threat in terms of factors relevant to evaluating US policy and organizational responses. Definitions and boundaries prove critical in establishing policy, defining organizational responsibilities and addressing resource allocation. So while arguably an artificial exercise, we will begin by answering two key questions—"What types of acts constitute cyberterrorism?" and "Who conducts cyberterrorism?"

This analysis of cyberterrorism centers on the activities of organized, non-state actors pursuing political or systematic objectives against the US[6] The activities of states conducting hostile activities in cyberspace against the US fall outside the realm of cyberterrorism into areas which can be labeled information warfare, espionage, or public diplomacy. However, we will consider the possibility that states may be associated with non-state actors in the furtherance of cyberterrorism. I also do not consider activities of individuals in the furtherance of personal objectives. However, because even individuals can

cause disruption and destruction in cyberspace, the possibility of cyberterrorists cooperating with individuals must be addressed. Also, while cyberespionage and cybercrime should not be lumped in with cyberterrorism, both types of activity could be used to support cyberterrorism.

Taking a stab at what acts constitute "cyberterrorism" involves addressing even fuzzier boundaries. From the traditional perspective, consideration of terrorism focuses on acts or threats of violence calculated to create an atmosphere of fear or alarm. For example, cyberattacks could cause train accidents with large death counts through tampering with digital signaling systems. Additionally, cyberspace presents myriad opportunities to commit acts that cause significant disruption to society without direct loss of life, injury, or harm to material objects. For example, digital attacks might cause stock market disruptions by denying service to computer and communications systems.[7] This analysis of cyberterrorism includes both acts that involve physical violence and those causing significant social disruption based on attacking information systems and infrastructures.

Additionally, cyberterrorists could conduct attacks with the goal of corrupting key information within a system that requires high confidence for its use. Corrupting information about blood types within a hospital data base or strike prices within the stock trade settlement systems would involve much more recovery time and effort than a simple denial of service attack on the same target. Such an attack would inflict direct economic costs from system downtime, checking and correcting data and settling disputes. Successful cyberterrorist attacks of this sort may also degrade user confidence in provision of services of fundamental importance to society.

Activities labeled as cyberterrorism must include recognition of both destructive and disruptive components. An open question is whether the potential for "mass disruption" created by reliance on information systems in the US will hold even greater appeal than attacks of "mass destruction" through the use of chemical, biological, and nuclear means.[8] Terrorists may prefer cyberattacks capable of causing widespread, observable impact but not

involving death and physical disruption rather than use of WMD or even conventional attacks in terms of limiting moral outrage and managing public opinion. Alternatively, "mass disruption" inflicted via cyberterrorism may prove too ephemeral to achieve desired effects. Governments and societies subject to cyber-based "mass disruption" may quickly learn to react and respond to such attacks, potentially even building up psychological resistance to such attacks.

Delineating the scope of activities that constitute cyberterrorism is difficult. The information age may well provide terrorist groups new ways to discredit governments and disrupt society to achieve their objectives. Therefore, cyberterrorism should be analyzed in light of the objectives sought.

Motives and Accountability

The nature of cyberterrorist campaigns, the means used, and the targets attacked will all depend on the motives of those groups considering the use of cyberterror means. Traditional analysis of terrorism has concentrated on groups with well-defined purposes for using violence as a means of political coercion.[9] Many terrorist groups such as the Weathermen within the US or the Red Brigade in Italy have engaged in efforts to overthrow or substantially change a political regime. Attacks are launched to undermine the legitimacy of the targeted government and garner support among a disaffected populace. Secessionist groups seeking the creation of new states or political autonomy for an ethnic/religious group also may use terrorist means to publicize their cause. Groups utilizing terrorist means to achieve such objectives include the Popular Front for the Liberation of Palestine and the Provisional IRA. A key feature of terrorism for political coercion is the willingness of groups to take credit for their attacks. The ability to inflict pain provides the principal source of leverage in negotiating with governments to achieve their objectives. Given the desire to secure the support of the general population and possibly to negotiate with governments, such groups may have self-imposed limits in terms of how vigorously and indiscriminately they choose to employ violence.

Taking a broader perspective on the issue of objectives, the use of terrorism by groups with millennial or anarchical objectives has become a

source of increasing concern.[10] Rather than pursuing a specific political agenda, such groups may use indiscriminate violence to create a general environment of fear and chaos prior to a general overthrow of Western political order or may even simply seek anarchy as a goal. The Aum Shinrikyo cult took no credit for the use of sarin gas by the in Tokyo subways. Laquer has highlighted the potential for such groups to view "superviolence" as an appropriate means to undermine the world political system in seeking their goals.[11]

A new thread in the analysis of terrorist motivations has received the label "war paradigm."[12] This paradigm holds that certain terrorist groups without the ability to confront opponents directly will take a strategic approach to conducting terrorist acts without making specific demands on the opponent. For example, Ramsey Yousef and others who executed the World Trade Center bombing had no known intent to acknowledge their role. The goal of such groups is to inflict damage and wear down opponents as part of an eventual victory in a long-term struggle. The focus of these analyses has been on groups motivated by Muslim fundamentalism, especially those associated with the Saudi jihadist Osama bin Laden. The attacks seen during the second half of 1990s on US military forces at Khobar Towers and embassies in Nairobi and Dar-es-Saalam may constitute such a campaign. Terrorists waging such campaigns may also see little constraint on inflicting damage or destruction against opponents.

Organization

Changes in the way terrorist groups organize will also impact their motives and perceptions of accountability. Traditional terrorist groups associated with the PLO and IRA relied heavily on tight central control over acts committed by the organization as part of an orchestrated pressure campaign against adversaries. However, the looser organizational structures of groups such as HAMAS, and Afgan Arabs may be enabled by the pursuit of less controlled, more destructive activities conducted by groups with anarchist or religious objectives. The "networked" organization of terrorist groups financially supported by Osama bin Laden has increasingly become the archetype for describing a new form of

terrorist organization with no clear center of control. John Arquilla and David Ronfeldt have strongly touted the strengths of such an organizational form for terrorists. Networked terrorist organizations could establish alliances of convenience with state sponsors, criminal organizations (especially those involved in the drug trade), and potentially with hacker groups.[13]

The utility for terrorist groups to employ the services of hackers as surrogates in the conduct of cyberterrorism has also received growing attention.[14] Hacker groups have demonstrated a willingness to sell their services to outsiders. In the most well known instance, hackers in Hannover, Germany during the late 1980s sold information they obtained through access to computer systems in Departments of Energy and Defense, defense contractors and NASA to the Soviet KGB.[15] These intruders first began to obtain access in 1986. After their initial discovery in 1988, the process of identification and apprehension of the Hannover hackers by the US and German intelligence and law enforcement agencies took over 18 months. During the Persian Gulf War, a group of Dutch hackers who had intruded into Department of Defense systems attempted to sell their services to the Iraqis but were apprehended by Dutch police.[16]

Most analyses of hackers as cybersurrogates for terrorism generally stress the ease and advantages of such activity.[17] It is presumed that terrorist groups will be able to easily contact hackers for hire while keeping their direct involvement hidden through the use of cut-outs and proxies. These hacker groups could then be employed to reconnoiter adversary information systems to identify targets and means of access. If hacker groups can be employed to actually commit acts of cyberterrorism, terrorist groups may improve their ability to avoid culpability or blame.

However, employing cybersurrogates would also involve important risks and disadvantages. Attempting to employ hackers to commit acts of significant disruption that may involve killing people would likely prove much more difficult than buying information for the purposes of intelligence gathering. Contacting and employing hackers would also involve major operational security risks for a terrorist group.[18] At a minimum, the intelligence

activities of hackers could be discovered and undermine planned operations. Terrorists without adequate leverage to control cybersurrogates run the risk of hackers being turned into double agents by hostile governments. The costs to a terrorist group of having an operation blown or providing adversaries information regarding their location or the identity of members would weigh heavily against use of such means. Both the German and Dutch hackers were eventually discovered, albeit after fairly long periods of activity and investigation.

The dearth of evidence means the calculus of terrorists considering use of cybersurrogates remains highly speculative at this point. One area for greater consideration is identifying which potential partners terrorist sponsors would consider more trustworthy. Some candidate surrogates, such as ex-security service members, may be considered more adept at maintaining operational security. Former members of the Soviet intelligence services that possess the requisite computer expertise and experience in the black arts of espionage may pose a real concern.[19] Terrorist groups may already have forged links with such potential allies. The subject deserves dedicated intelligence gathering efforts and analysis rather than simple hype.

Hacker Groups and Terrorism

Additionally, one must consider to what degree organized groups of hackers acting on their own accord pose a terrorist threat. For purposes of this analysis, hacker refers to persons or groups who gain access or break into digital systems, particularly networked computer and telecommunications systems. Hackers have a wide range of motivations including thrill seeking, knowledge, recognition, power, and friendship.[20] These individuals have also developed a sophisticated network to communicate ideas and coordinate activity through magazines such as *Phrack* and *2600*, stolen phone services, e-mail distribution lists, Usenet newsgroups, Internet chat rooms and even full-blown conferences such as DEFCON. According to one survey of hackers, over half of those asked said they work in teams, and more than a third indicated they belong to a specialized hacker group. Groups have names such as Legion of Doom, Masters

of Destruction, and Cult of the Dead Cow. These groups have been known to wage conflicts on each other using the public telecommunications networks as a battleground and touting their degree of illicit access as the source of bragging rights.[21] Many groups analyze software weakness and provide digital tools to exploit mainstream software applications such as Microsoft Windows operating systems. Additionally, hackers are dominantly males between the age of 15 and 25, often disaffected with the prevailing social and governmental order. This profile parallels those involved in terrorism.[22] The combination of technological skills and disaffection could make a sufficiently motivated and organized hacker group in a considerable cyberterrorist threat.

Numerous hacker groups have expressed deep animosity against the US and other governments over attempts to prosecute hackers, regulate activity on the Internet and other political issues. The hacker magazine *2600* has orchestrated a major campaign, including a fundraising campaign, to get the government to release Kevin Mitnick convicted of numerous violations of US computer crime laws.[23] In December, the group known as the Legion of the Underground (LoU) issued a "declaration of war" against the governments of the People's Republic of China and Iraq citing these regimes' repressive human rights policies. The LoU declared its intention to disrupt and disable the Internet in the two countries. [24] East Asia has also witnessed an exchange of digital intrusions targeted at defacing Taiwanese and People's Republic of China government web sites with nationalist symbols and slogans of the hacker's home state.[25]

Thankfully, however, typical terrorists and hackers also have significant differences. Terrorists are generally conservative regarding use of new technologies to conduct operations. [26] Some groups have even conducted attacks to specifically combat the spread of computer technology. A French group called the Computer Liquidation and Deterrence Committee attacked French and American computer companies during the 1980s because "the computer is the tool of the dominant. It is used to exploit, to put on file, to control, and to repress."[27]

Conversely, the Internet community has seen the rise of white-hat hacker groups with a range of objectives. Some such as the LoPht Heavy Industries group based in Boston simply seek to provide information on latest hacker tricks and security weakness in products. LoPht has also called for hackers to cease attacks against the US government and testified for the Senate on how to improve computer security efforts.[28] The hacker community has also demonstrated a willingness to impose discipline on its own against disruptive hacking when the potential government backlash may prove too severe. A coalition of hacker groups formally condemned the LoU's declaration of war. *2600* magazine declared "This type of threat, even if made idly, can only serve to further alienate hackers from mainstream society and help spread the misperceptions we're constantly battling."[29] So far, the hacker community has stopped shy of conducting activities constituting a serious cyberterrorist threat.

Means and Targets for Cyberterrorism

The headlong rush of the US and other advanced nations into the information age involves new risks. The information systems central to national security, the conduct of government and commerce have significant weaknesses that can be attacked. Yet, such attacks have achieved only limited impacts as we end the 20th Century. To analyze how cyberterrorists might attack the US, we must consider which groups might employ cyberterrorism and for what reasons.

Means for Digital Attack

Terrorists could attack US information infrastructures using a variety of mechanical, electromagnetic, or digital means. Information systems have long been targets of mechanical methods of disruption. Command and control systems can be bombed, fiber-optic cables cut, microwave antennas broken, and computers smashed or simply turned off. The electronic components and transmissions of information systems and networks are vulnerable to jamming, as well as electromagnetic pulses generated by nuclear explosions and other sorts of directed-energy weapons. The rise of digital means of encoding and transferring information has also created new ways to attack information systems. Impacts of digital attacks can range from total paralysis of networks to

intermittent shutdown, random data errors, information theft, and data corruption. The tools and techniques for attacking information systems have received detailed attention as the US government, commercial industry, and outside experts have begun to stress the possibilities of information warfare, digital espionage and computer crime.[30] The analysis below focuses on digital means as the new dimension of the equation appropriately labeled cyberterrorism. The possibility of synergistically employing all three types of attack also requires additional analysis beyond the scope of this chapter.

Cyberterrorists could cause disruption, damage, and destruction through achieving unauthorized access and control over a targeted information system through a vast array of intrusive tools and techniques, commonly referred to as "hacking." Means for successful intrusion range from compromised passwords to sophisticated software for identifying and exploiting known vulnerabilities in operating systems and application software. The difficulty of attaining access and time required to successfully "hack" a system will also depend on the targeted system's defensive measures including proper password and configuration management, patching of known vulnerabilities, and use of firewalls and intrusion detection systems. If control over a targeted computer or network is achieved, cyberterrorists could inflict a wide range of effects. Possibilities range from changing the graphics on a web page to corrupting the delivery schedules for medical supplies or military equipment to denying access to 911 services, air traffic control data, or disrupting telecommunications backbone networks. A principal advantage of intrusion for cyberterrorism is the potential for tight control over the timing, scope and effects of an attack. According to former Director of the Central Intelligence, John Deutch, "the electron is the ultimate precision weapon."[31]

Another well-known potential means for cyberterrorist attack would be the employment of malicious software code, more commonly referred to as viruses and worms. Malicious software can be broadly defined as software designed to make computer systems operate differently than intended. The effects of viruses and other malicious software range from benign messages

displayed at system start up to code that can cause hardware failures and wide-area network overloads. Concern over malicious software increased rapidly after the unintentional release of the Internet Worm by a Cornell graduate student in 1988 disrupted most Internet services for a period of days.[32] During the early 1990s, reacting to and mitigating the consequences of viruses was a major computer security focus. Development of anti-virus software capable of periodic updating has helped mitigate the virus threat. However, 1999 saw a series of virulent outbreaks, including the Melissa virus and Worm.ExploreZip that proved capable of disrupting government, commercial, and other private information systems. A major feature of these viruses has been traffic overloads that occur when the viruses propagate vast amounts of e-mail through networked systems. Creators of malicious software determine the intended impact of running their code. However, the degree of disruption and damage caused by viruses and other code which replicates and passes quickly across networked systems can be much more difficult to control. Cyberterrorists using malicious code created by others may have much less certainty regarding the effects of their attack.

Combining features of both intrusions and malicious code, cyberterrorists could also intentionally corrupt software programs in targeted information systems and infrastructures to cause desired effects. While access to rewrite software code could be achieved through an intrusion, a terrorist group may endeavor to corrupt software in the process of creation or production by emplacing backdoors for access or insert "trojan horses" to cause desired effects at a predetermined time or upon a given command. Software maintenance and updates also present opportunities for such activities. Software code creation and maintenance for systems employed across the globe occur in places like India, Ireland, and Israel. The possibility for insertion of corrupted code as part of the massive effort to update software to fix Year 2000 problems provided a major concern for all sectors of the US government and society.[33] The main protection against such activity would be rigorous quality control over software products used in key systems, but such a process is time-consuming

and expensive. As with intrusions, the degree of control possible through corrupted code can allow precision effects. Cyberterrorists could also achieve widespread effects by corrupting code in systems underpinning key information infrastructures. AT&T suffered nation-wide disruption of its telephone network in January 1990 due to a single line of faulty code in an upgrade to its primary switching software.[34] While this error was unintentional, the ability to attack the digital foundations of advanced information infrastructure presents sophisticated cyberterrorists with a significant means of attack.

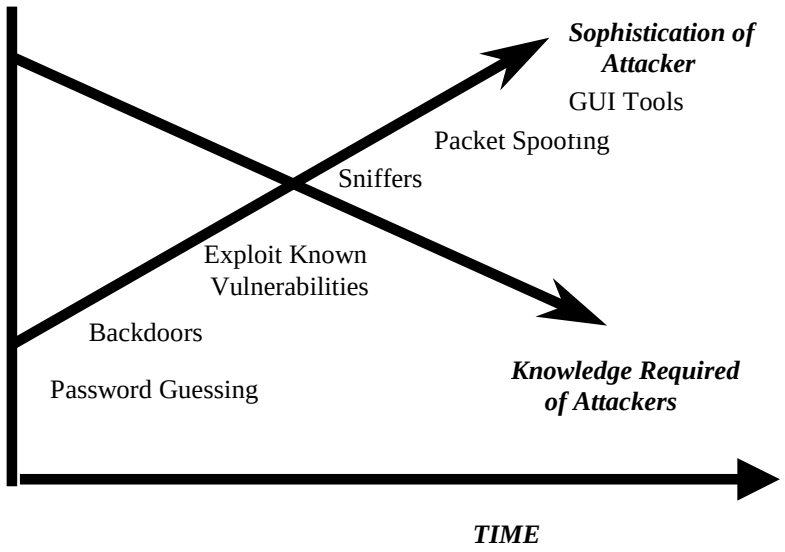
Cyberterrorists can also disrupt or disable information systems and networks using techniques generically labeled as denial-of-service (DOS) attacks. Common DOS techniques involve overloading targeted e-mail systems by employing automated software and exploiting features of the Internet communications protocol through "smurf" or "SYN flooding" attacks. In recent years, hackers and politically motivated groups have increasingly turned to DOS attacks as a means of responding to specific events and policies by harassing targeted organizations and to draw attention to their complaints. One well-known instance involves a group known as the Electronic Disturbance Theatre (EDT). In October 1998, the EDT targeted the computers of the US military and the Frankfurt Stock Exchange in an effort to overload servers in these networks with the goal of publicizing the cause of the Zapatista rebels in Mexico. Yet, while cyberterrorists can specifically target denial-of-services attacks against known systems connected to network accessible to the attackers, operators of the targeted systems can also modify their systems either preventively or in reaction to the attacks. The Defense Information Technology Center simply reconfigured the targeted computers to refuse to acknowledge the originating Internet addresses in response to the EDT attacks. The EDT computers were overloaded with return messages as a result of employing the automated FloodNet software and forced to reboot.[35] The cat and mouse game of offensive moves and defensive responses will continue to evolve as information technology advances and presents new vulnerabilities to exploit. Cyberterrorism

and other types of warfare, espionage, and crime waged in the digital realm will demonstrate this see-saw dynamic.

Another possible approach open to cyberterrorists would be to conduct hoax attacks, publicizing the possibility of intrusive activity and release of viruses. Virus scares can swamp help desks with requests for information. Users and system operators must ensure anti-virus software is up-to-date, creating an additional burden on the networks and wasting time. The Good Times scare in 1994 caused a massive reaction while only infecting a handful of computers.[36] Similarly, the possibility of intrusive activity requires system administrators and computer incident response teams to assume higher states of readiness with an attendant decline in attention to routine operations and maintenance. The US Department of Defense has instituted an Information Operations Condition (INFOCON) system of progressively higher levels to raise the awareness and preparedness of cyberdefenses similar to the THREATCON system use for responding to increased threat of terrorist attack.[37] Attaining the defensive posture called for by higher INFOCON levels would require substantial efforts for those responsible for the DoD information infrastructure and pose constraints on the use of the Department's information resources. Cyberterrorists focused less on high impact events and more on waging a protracted conflict could use hoaxes designed to cause the targeted adversary to waste significant effort without the terrorist having to run the risks of conducting actual attacks. Defensive efforts may suffer over the long-term if multiple hoaxes create a "cry wolf" syndrome regarding calls for increased protection. The impact of hoaxes will be magnified if terrorist groups develop a credible reputation for being able to conduct digital attacks.

Access and Expertise

To use any of the tools and techniques described above, cyberterrorists must have access to the means and the expertise to employ these tools effectively. The prevailing wisdom is that both are readily available. Well-known information warfare pundit, Winn Schwartau states, "Anyone can be an



information warrior…. Potentially, a hundred million information warriors are poised, and honing their skills while they wait."[38] Numerous analyses cite the vast number of web sites on which hacker tools and techniques can be found and downloaded, as well as the presence of Internet chat sites, conventions, catalogues, and publications in which hackers exchange information.[39] In a similar vein, most analyses also hold that the means for attacking information systems have become both more sophisticated and easier to use. The following figure from a 1996 GAO report entitled *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks* depicts the evolution of attack tools and required expertise as time has progressed.[40]

One way terrorists may build their expertise and understanding of the potential for digital attacks is through the use of cyberspace for other activities. Increasingly, terrorist groups including the Provisional IRA, Algerian extremists, HAMAS, and others are using the Internet and cellular phones to orchestrate their activities. Many groups have begun to use encryption technology to protect their digital communications. According to Arquilla,

> Egyptian "Afgan" computer experts have helped devise a communication network that relies on the World Wide Web, e-mail and electronic bulletin boards so that extremists can exchange information without a major risk of being intercepted by counterterrorism officials.[41]

The Provisional IRA uses computer databases to catalogue individuals, installations, and other targets.[42] Terrorists and associated groups have also begun to use the Internet as a mechanism for publicity, fundraising, and recruitment. The Zapatistas have established a major presence through the World-Wide Web supported by activists in the US, Europe, and elsewhere.[43] Drug cartels use the Internet in transactions with banks to launder money, and at least potentially, terrorists could use cybercrime to steal money to support their operations.[44] Terrorists may also use advanced information technology for intelligence gathering. Access to commercial satellite imagery may provide information for targeting physical attacks. Hacker and information warfare websites may provide conceptual approaches and even lists of targets for cyberterrorism. Evidence is clear that terrorist groups increasingly use advanced information technologies and are building an experiential base that could be used for cyberterrorism.

However, the utility of user-friendly attack technologies and general computer expertise to any terrorist group depends on the nature of the targeted infrastructure and intended effects. Denial of service attacks against Internet connections may require much less sophistication but achieve less controlled effects than attacks based on successful remote access and control of a targeted information system or network. Additionally, a defender's ability to assess vulnerabilities and deny access to known digital attack tools and techniques may also increase the level of technological knowledge required for attacking forces. If key information infrastructures are well protected, achieving surprise and inflicting disruption against significant centers of gravity may require cyberterrorists to employ more technological sophistication, time, and effort. The pool of human capital with the ability to develop sophisticated new attack tools or quietly probe strong, attentive defenses is much more limited than the

number of individuals capable of running scripted tools or sending multiple e-mail messages to an Internet address. The Center for Infrastructural Studies stated in early 1998, “According to recent studies, most attacks use standard or well-known script exploits. Our research reveals less than 1,000 hackers in the world who have the professional programming skills to create their own attack scripts.”[45]

For cyberterrorists, easily accessible and usable digital attack techniques may equate to more conventional hand grenades and pistols in terms of scale of effects and lack of precision. To develop the digital equivalent of weapons of mass destruction or achieve the precision of sniper rifles may require a much greater degree of technological sophistication and self-reliance on the part of cyberterrorists. Developing collection means and analytical techniques to understand the technological skill and resources of terrorists presents an important challenge for the US intelligence community.

Targets for Cyberterrorist Attacks

Since at least the early 1990s, the US government and outside experts have grown increasingly concerned about the possibility of cyberterrorist attacks as our society has become more reliant on information systems and infrastructure. The 1991 National Research Council *Computers at Risk* report finds, "The modern thief can steal more with a computer than a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than a bomb."[46]

The increasing ability of terrorists and others to attack US critical infrastructures through use of digital attacks has received the most attention.[47] In the wake of the Oklahoma City bombing in 1995, the President set up a Critical Infrastructure Working Group to address both physical and cyber threats. As a result of hacker incidents, Department of Defense exercises and Congressional prodding, the Presidential Commission on Critical Infrastructure Protection was set up to analyze the threat to US infrastructures and policy responses for their protection. The PCCIP's October 1997 report, entitled *Critical Foundations*, provides the most comprehensive analysis of the cyberthreat to US infrastructures "essential to minimum operations of the

economy and government."[48] The report stresses how the growing reliance on information systems that underpin a whole range of infrastructures including communications, electric power, transportation, and emergency services creates substantial risks for a wide range of digital attacks, including possible cyberterrorism. While a comprehensive discussion is beyond the scope here, possible targets for cyberterrorism include the Supervisory Control and Data Acquisition (SCADA) systems which govern the distribution of telecommunications, electric power, and other infrastructure-based services. The Global Positioning System (GPS) network of satellites, ground control stations, and signaling systems constitutes an infrastructure target whose role in military and civil navigation as well as broadcasting timing signals in cellular communications and other information networks could prove attractive to cyberterrorists. The disruption caused by the failure of a single PanAmSat communications satellite in May 1998 crippled most US paging services as well as a number of data and media communications feeds for hours and, in some cases, a couple days.

While attacking information systems underpinning critical infrastructures presents cyberterrorists with potentially high impact targets, important questions need to be addressed in order to adequately gauge the potential threat. One area of significant uncertainty is how fast infrastructures will be able to recover from digital attacks. Many analysts focus on how many infrastructures have single points of failure that can cause quickly cascading effects disrupting or disabling effects over a wide area. The Northwest power outage in August 1996 that affected hundreds of thousands of users began by a tree growing into a single power line. Others point to the ability of complex systems to adapt and recover.[49] In the cases of the AT&T switching failure, the Northwest power outage, and the PanAmSat satellite failure, the infrastructure operators were able to recover in a period of hours. What is clearly unknown is how such complex infrastructures would react to orchestrated cyberterrorist attacks instead of unintentional mishaps and accidents.

Another approach would be to attack organizations or institutions with high public visibility. Hackers have proven capable of repeatedly defacing the web pages of corporations such as DuPont and Ford as well as government agencies including the White House, FBI, NASA, and the Air Force. Cyberterrorist attacks may specifically be launched to garner media attention rather than cause physical damage or economic losses. Demonstrated ability to disrupt computerized inventory systems of Wal-Mart or corrupting medical records within a large health management organization would provide prime fodder for media attention. Newspapers have reported that the hacker group, RTMark, has endeavored to depress the stock price of eToys by disrupting the company's web site.[50] Financial institutions have often been listed as a potential target of cyberterrorism. Citigroup admitted in a highly publicized incident that a Russian hacker managed to electronically siphon off $12 million in funds in 1995. While Citigroup actually managed to recover all but $400,000 of this loss, competitors reportedly used the incident to convince commercial clients to switch banks due to the perceived greater insecurity of Citigroup information systems.[51] In 1996, the *London Times* reported that banks, brokerage house, and investment firms paid hundreds of millions of dollars in blackmail to extortionists to avoid cyberattacks whose capabilities had been demonstrated.[52] The high level of media attention to financial markets and the critical role of public confidence in their activities mark them as prime targets.

Terrorist groups could also conduct digital attacks against media outlets themselves. Indonesian media outlets had their computer systems attacked by hacker groups supporting the Timorese rebels.[53] However, cyberterrorism targeted with an eye towards garnering media attention rather than death and destruction may require more sophisticated targeting and digital attack capabilities than generic attacks against any open targets within the US infrastructure. The disruptive effects of such attacks may prove short-lived, but cyberterrorists could endeavor to shake public confidence in core institutions through such attacks.

Terrorist groups could also use digital attacks to support traditional terrorist operations. As monitoring and sensor systems for protecting people and facilities become increasingly reliant on information technology, digital attacks may prove a useful means of creating opportunities for conventional terrorism. In 1998, the *New York Times* reported a design flaw in a security system widely used in airports, prisons, financial institutions, and the US government allowing digital intruders to access secure areas, unlock doors, and erase evidence of changed access records.[54] Emergency 911 systems have been found vulnerable to computer intrusions and could be targeted by cyberterrorists. Paralyzing communications as a means of slowing emergency responses could plausibly enhance effectiveness of conventional or WMD terrorism. As with any potential tool, terrorist groups could employ cyberattacks synergistically along with other means to achieve their objectives.

Cyberterrorists may also endeavor to make use of "insiders." Reasons for assisting terrorists could include personal gain, revenge, or sheer destructiveness. The assistance of individuals knowledgeable of technical characteristics and operational significance of a targeted information and systems would prove of immense value to terrorist groups in launching all types of digital attacks. The threat posed by insiders with authorized access to information resources presents a fundamental information security concern.[55] A network programmer fired by Omega Engineering Corporation in 1996 provides an illustrative case. Upon his departure, the programmer activated a logic bomb that permanently deleted all the company design and production software used to produce high technology measurement and control instruments for the US Navy and NASA. Damage was estimated at $10 million.[56] The 1999 Computer Security Institute/Federal Bureau of Investigation "Computer Crime and Security" survey indicated sixty-five percent of organizations responding had suffered incidents involving insiders.[57] Cyberterrorists intent on causing widespread destruction and damage might use insiders to corrupt SCADA systems or plant viruses. The ability to effectively screen employees, discover attempts at outside recruitment, and identify and mitigate malicious activities

quickly will play a role in combating cyberterrorism as part of overall information security efforts

Thinking About Cyberterrorist Campaigns

With a wide range of available tools and potential targets, cyberterrorist groups may use very different types of campaign strategies to pursue objectives. So far, most attention focuses on the possibility of single events causing catastrophic physical effects such as a plane crash or the failure of control systems in a nuclear power plant. The assumed objective of the attack is widespread publicity for the group's cause and negotiating leverage against governments. A potentially more serious threat that receives less attention would involve cyberterrorist groups adopting a protracted war strategy similar to the ones used by Mao Tse Tung and Ho Chi Minh. Instead of striking the most dramatic target, terrorists waging a protracted guerilla campaign of cyberterror could strike targets of opportunity that also minimized the chance of discovery and retaliation. The objectives of such a campaign may well involve media attention but also target the will of an adversary's government and populace over the long-term.

Developing a strategy for dealing with single cyberterrorist events may focus on improving warning of attacks and the ability to manage the consequences of disasters. Responses to waging a prolonged conflict with cyberterrorists may be quite different. Fighting such adversaries will require improvement in defensive capabilities and recovery capacity of information infrastructures as well as improving means to track down and incapacitate attackers.

Outlining these two broad strategic approaches and their implications simply provides an illustration of the complex situation facing those responsible for dealing with cyberterrorism. The US government must develop a deeper understanding of how different cyberterrorist groups are most likely to operate, potential objectives and capabilities, the risks posed by attacks, and appropriate responses. This analysis must be based on fact, not speculation.

Cyberterrorism—What We Have Observed

Information infrastructures have long served as targets for adversaries in a conflict. Adversaries have always attempted to intercept messengers. The emergence of electronic communications resulted in cutting telegraph lines and underseas cables during wars. As more communications passed via electromagenetic transmissions, jamming, frequency hopping, and other techniques became a commonplace aspect of military operations known as electronic warfare.

Terrorists have also seen attacks against infrastructures as a means of achieving their traditional objectives. For example, the Provisional IRA in the early and mid-1990s launched major terrorist attacks against transportation and commercial targets in U.K. with the intent of maximizing societal disruption. In April 1993, a bomb detonated in London caused massive commercial disruption by causing the temporary closure of key financial markets.[58] In the 1970s, the Italian Red Brigades specified destruction of computer systems and installations as a way of striking at the state. They conducted numerous attacks against businesses in the elctronics and computer industries.[59] As the functioning of information systems and infrastructures becomes increasingly fundamental to US and other societies, the appeal for terrorists to attack such targets will increase. Lessons learned about what constitutes key features of an adversary's information infrastructure necessary for the conduct of conventional attacks would also prove useful to cyberterrorists considering the use of digital attacks.

Hackers and hacker groups so far have not proven to be significant cyberterrorist actors in terms of conducting digital attacks to create intentional death, destruction, or disruption. While there have been occasional declarations of intent to wage "cyberwar" against the US government, corporations or other entities, these threats have not resulted in serious campaigns to achieve political or even anarchical objectives. However, the dearth of cyberterrorism by hackers so far does not mean they are not capable of inflicting severe damage via digital attacks. Hackers have intentionally disrupted 911 services, launched viruses degrading the information processing of major corporate and government

organizations, and gained access to key computer systems such as domain name servers which underpin information infrastructures in such organizations. A good example of the potential for hackers to become cyberterrorists is provided by an incident in March 1997. In this instance, a teenage hacker penetrated and disabled Bell Atlantic telecommunication switches in the Northeastern US One of the disabled switches provided phone and data services to the Worchester, Massachusetts airport control tower, and the incident shut down the airport for many hours.[60] If such an attack were purposely targeted and timed when air traffic control was already difficult due to weather or volume of traffic, the difference between what happened in Worchester and a cyberterrorist attack would only be a matter of intent.

An increasingly common phenomena related to cyberterrorism is hacking by technologically literate groups in support of insurgent, environmental, or other political movements. Hacking into and defacing Web pages has proven a most common means to express discontent. However, the rise of purposeful denial-of-service attacks such as the one by the EDT has also caused increased concern. So far, such activities have proven at most temporary nuisances rather than real problems that might coerce targeted governments to change policies. Yet, reacting to such threats already involves increasing resource commitments by organizations such as the Department of Defense and FBI. Such activity clearly falls within the boundaries of terrorist intent discussed earlier. The real question is when does the level of disruption rise to a standard appropriately labeled as terrorism instead of mischief.

In terms of known terrorist groups using digital attacks for cyberterrorism, we have only begun to see such activity occur. The most well-known case has involved the Internet Black Tigers, an offshoot of the Sri Lankan rebel group Liberation Tigers of Tamil Elam. The Internet Black Tigers swamped the e-mail services of numerous Sri Lankan embassies for a period of approximately two weeks.[61] Yet, such attacks comprised a relatively insignificant aspect of the overall terrorist campaign of these rebels and arguably were principally for publicity rather than disruptive objectives.

A major terrorist campaign waged principally or solely via digital attacks has not occurred. As with other forms of conflict, cyberterrorism will likely evolve as another tool for groups to achieve their objectives rather than springing into life in full bloom. That said, successful cyberterrorist attacks could also provoke a rapid rise in activity once such means are a proven way to achieve terrorist goals. The focus for US policy should be to understand the goals of groups who are most likely to employ such a new approach and potential vulnerabilities arising from possible cyberterrorist attacks.

The US Response

The US national government has recognized the growing threat posed by cyberterrorism. A detailed development of US policy and organizational responses to cyberterrorism is beyond the scope here. The section below presents a brief overview of what has been accomplished and what is yet to be done.

Over the past decade, a confluence of concern with information warfare, terrorism against US targets at home and abroad, and the recognition of the increasing reliance on critical infrastructures all have made dealing with cyberterrorism a higher priority on the national security agenda. A spate of books and articles in the mid-1990s focused on the possibility of a digital Pearl Harbor facing the US The President established a Critical Infrastructure Working Group in 1995 in the wake of the Oklahoma City bombing to address both physical and cyber terrorist threats under the leadership of the Justice Department. Congressional inquires and GAO reports have described the vulnerabilities of our digital infrastructure to hackers and called on the President to details plans to develop cyber defenses. Such threats have been examined through RAND "Day After in Cyberspace…" wargames and DoD exercises such as Eligible Receiver. These evaluations demonstrated significant national and DoD vulnerabilities that would arise from a structured cyberattack.[62]

Growing demands for a comprehensive response have resulted in the US government putting increasing energy behind its response to possible cyberattacks. In the summer of 1996, the President's Commission of Critical

Infrastructure Protection was formed to conduct a comprehensive review and recommend national policy for protecting critical infrastructures against physical and cyber threats. The PCCIP's efforts formed the basis for Presidential Decision Directive 63 "Critical Infrastructure Protection" issued in May 1998. In combination with PDD-62 "Protection Against Unconventional Threats to the Homeland and Americans Overseas," the two directives establish a system of organizations, roles, and responsibilities through which the US will respond to terrorism and protect its critical infrastructures during peace and war.

Since the spring of 1998, national efforts against digital attacks have focused on implementing the construct laid out in PDD-63. The Directive created a National Coordinator for Security, Infrastructure Protection and Counterterrorism on the National Security Council. Departments and agencies within the Federal government have developed sector-specific protection plans across the range of identified critical infrastructures. The Critical Infrastructure Assurance Office (CIAO) in the Commerce Department assists in sectoral planning efforts and their integration into a national plan. The private sector has also started to establish Information Sharing and Analysis Centers (ISACs) as called for in PDD-63. As of late 1999, the first ISAC was established in the banking and finance sector with other ISAC plans under development.[63]

On the operational side, the National Infrastructure Protection Center was established even prior to the issuance of PDD-63 in February 1998.[64] As staffing and resources have increased over the past few years, the NIPC and Federal government agencies have initiated numerous efforts to coordinate activities in response to cyber threats. The NIPC and CIAO are endeavoring to establish linkages with state and local governments as well as the private sector. Yet, the hurdles to improve cyberdefenses are substantial and resources remain limited.

Challenges in Responding to Cyberterrorism

The US intelligence community must play a key role in understanding the threat posed by cyberterrorism. Effective responses require the US both to understand the potential capabilities of cyberterrorist groups and develop advanced warning

regarding their intent to use such capabilities. Cyberterrorism presents a very difficult intelligence target. The highly developed imagery and signal intelligence capabilities used to characterize Cold War threats and nation-state military capabilities have limited applicability in providing information to assess whether terrorist groups can effectively employ digital attacks. Also, the skill sets of intelligence analysts required to understand digital communications systems and techniques for exploiting computer weaknesses are not the same as those to characterize capabilities of ballistic missiles and the strength of ground forces. Also, the new skill sets are in high demand in the private sector making them even harder to create and sustain within the US government.[65]

To provide strategic warning of cyberterrorism, the intelligence and defense communities require insight into activities of adversary groups to develop profiles of preparatory steps for digital attacks. In the cyberrealm, distinguishing potential terrorist activity from normal system failures, exploratory hacking, and other threats such as espionage is very difficult. In the spring of 1998, the Department of Defense was initially concerned that hacking activity eventually tracked down to teenagers might have been state-sponsored activity related to US military activities in the Persian Gulf.[66] Conducting counterterrorism involves close coordination between organizations responsible for intelligence, counterintelligence, and combating computer crime. Potential terrorist activity in cyberspace presents particularly acute requirements for such cooperation.

PDD-63 and other policy directives have set in place the organizations and responsibilities. At the national level, the NIPC has primary leadership for detecting and responding to digital attacks. The Defense Department established a Joint Task Force - Computer Network Defense to provide centralized capability for the same missions to protect the Defense Information Infrastructure. A program to create a comprehensive Federal Intrusion Detection Network (FIDNet) system under the authority of GSA exists.[67] Other organizations in the public and private sectors have established efforts to achieve similar objectives. In addition to the ISACs, a number of computer

security associations and consulting firms strive to improve computer and information security in the private sector. These organizations generally work closely with a community of Computer Emergency/Incident Response Teams known as CERTs or CIRTs established by many organizations in both the government and in the private sector.

Yet, despite the presence of such organizations, those responsible for US cyberdefense at all levels have very limited capability to provide tactical warning of impending attacks or assess attacker motivations and objectives. Defensive tools, primarily in the form of various types of intrusion detection systems, have been developed to help identify presence and intent of malicious digital activity. However, current IDS technology relies on identifying known types of exploits and can not easily identify new types of digital attacks, even those based on modifying previous types of exploits.[68] Adequate attack assessment is even tougher. Owners, operators, and defenders of information systems and infrastructures rarely have an adequate picture of what they are protecting. Defenders not only need to understand physical and logical interconectivity, they also need to understand the operational significance of information and systems which are under attack to properly prioritize their warning, detection, and response efforts.

In specific circumstances, CERT and law enforcement agencies have proven capable of tracking down and punishing attackers. However, the timelines to identify and prosecute responsible individuals in most well-known hacker incidents have been lengthy and the punishments meted out fairly light. The capacity of the NIPC, the JTF-CND, and other organizations to handle big events involving large numbers of sophisticated attackers is unproven. Legal and policy considerations also place constraints on such agencies attempting to precisely identify individuals and organizations responsible for malicious activity in cyberspace. Law enforcement and computer network defense organizations are not allowed to hack back though computer systems to follow the electronic trail of intruders without express permission of system owners or authorized search warrants.[69] Yet, most digital intruders utilize multiple hops

through cyberspace before conducting intrusive activity. Also, the CERT and law enforcement communities most closely involved with leading responses to computer intrusions tend to focus on single incidents. Defending against cyberterrorists with long-term objectives and significant attack capabilities will require fighting a campaign, a perspective significantly different than a law enforcement effort focused on building a court case.

Federal government plans also have identified organizations responsible for responding if a cyberterrorist attack caused significant disruption or destruction to mitigate effects and restore capabilities. Under the authority of PDD-63, the Federal Emergency Management Agency (FEMA) would lead consequence management efforts in conjunction with the NIPC, FBI, and state/local authorities. US national-level planning for how to deal with major disruptions to information systems and infrastructures was accelerated due to the requirement to be ready for Year 2000 events. Yet, a continuing consequence management challenge is the lack of detailed knowledge of the network connectivity, information system characteristics, and operational significance of assets that may suffer a cyberterrorist attack. Lack of adequate information infrastructure "mapping" will hamper the prioritization of reconstitution efforts and deployment of available resources. Establishing effective consequence management capabilities also faces difficulties in terms of running operational exercises to simulate large-scale terrorist attacks against complex, interconnected, privately owned and operated information infrastructures. Currently, organizations responsible for responding to cyberterrorism lack understanding of possible modes of system failure and the ability of infrastructures and operating organizations to recover from attacks. Again, those responsible for consequence management efforts should leverage knowledge gleaned from Y2K preparations and experiences with failure and recovery characteristics from Y2K events.[70]

The final step in defending against cyberterrorism is to improve the strength of our information infrastructures against digital attack. The NIPC, in conjunction with sector leads and the ISACs, has the role of identifying critical

vulnerabilities and implementing mitigation plans. However, networked information systems and infrastructure at the end of the 20th Century present easy prey for digital intrusion and disruption. The complexity of operating systems such as Windows NT or Linux and applications such as Microsoft Office or SCADA systems combined with the speed of development and new product releases results in foundational pieces of the information infrastructure that have numerous security flaws. These flaws are discovered and disseminated at a rapid pace by the hacker community. As with intrusion detection systems, defensive tools such as firewalls, virus checkers, and network analyzers usually lag development of new attack techniques. Cyberterrorists are among the spectrum of adversaries who can exploit this basic weakness.

The process presently used by many government organizations involves instituting notification and tracking systems to ensure owner/operators of information infrastructures fix known vulnerabilities and update virus defenses to make digital intrusion and disruption more difficult for cyberterrorists and others. For example, the Department of Defense has instituted an Information Assurance Vulnerability Alert system that requires all DoD organizations to patch certain identified vulnerabilities and report compliance within specified timeframes.[71] However, this approach constitutes a rearguard action whose prospects for success are limited. Its success relies heavily on reacting to vulnerabilities after their weakness has already been demonstrated. More fundamentally, the "patching" process means those defending critical US information infrastructures must discover vulnerabilities, notify users, and track the implementation of fixes throughout a extremely diverse infrastructure comprised of and operated by thousands of organizations using thousands of different products implemented and modified by hundreds of thousands of individuals. So far, the procedures and resources employed to reduce infrastructure vulnerabilities to digital attack fall far short of denying access to potential cyberterrorists.

An alternative approach would involve ensuring that key systems and infrastructures were built to make digital attack difficult from the beginning of

system concept and design. Such an approach would help mitigate a wide range of threats including cyberterrorism but also address concerns ranging from unintentional problems to cybercrime to information warfare. Yet, US government plans as articulated in PDD-63 and other directives show little desire to pursue such an approach. Huge difficulty faces implementation of a national cyberdefense strategy based on migrating to more stout digital foundations. Fundamentally, the government would have to ensure that owner/operators of key systems and infrastructures employed more secure products. Yet, the forces of technological innovation and competition in the information technology industry have forced commercial producers to move firmly in the direction of deploying products as quickly as possible with a minimum of security and other testing. The booming US economy increasingly relies on this sector as a source of fundamental strength. With the exception of encryption policy, the Clinton Administration avoided any significant moves to interfere with the telecommunications and information technologies industries under the guise of national security.[72] This choice means that the threat from digital attacks will remain significant for the indefinite future.

The US has proactively begun dealing with cyberterrorism as a part of national security. Given that dramatic events have yet to occur to prompt action, such efforts should be lauded. However, while policy directives establish authorities and organizations to provide capabilities to counter cyberterrorism, the US is a long way from having effective defenses against the potential threat. Efforts throughout government and the private sector vary greatly in depth and focus. Human and financial resources are lacking everywhere. Technological and economic considerations limit the government's ability to protect our information systems and infrastructures. The nature of US society and protection of civil liberties also present difficulties for those responsible for protecting US in national security in cyberspace.

Policy Options

Improving US capabilities to deal with cyberterrorism will intertwine with a number of other efforts related to information warfare, critical infrastructure protection, and countering computer crime. This section lays out recommendations designed to make cyberterrorism more difficult and dangerous for perpetrators.

US strategy must include efforts to make information systems and infrastructures more robust. The first step in this process is to improve the basic understanding of the technological underpinnings and operational characteristics of our informational centers of gravity. The US government or private sector organizations can not afford to provide robust protection to any and all information resources. Defenders must catalogue key assets and prioritize the deployment of available resources. Such an undertaking will require significant resource investment in organizations such as the NIPC, by government agencies responsible for specific infrastructure sectors, and in the private sector ISACs to create and sustain knowledge of what ought to be protected and how to most effectively accomplish this task. This type of investment would not only serve to counter cyberterrorism but would improve US defensive information warfare and critical infrastructure protection programs at the same time. The US should incorporate lessons from preparing for and responding to Y2K events.

Additionally, identifying key assets and how to effectively protect them must extend beyond the critical infrastructures identified in PDD-63. Most importantly, the US government must find ways to motivate information technology producers to raise the priority of system reliability and security in the production and fielding of new products. Legislative and policy approaches must consider both carrots and sticks. Innovative ideas might include providing the private sector tax breaks for improving protection in key technologies or legislation that establishes liability for losses due to digital intrusions and disruption if companies do not meet proscribed security standards.[73] These efforts would involve economic and social tradeoffs that require thorough evaluation. Yet, despite obstacles, proactively limiting the opportunities

presented to terrorists and other digital attackers by building strong information infrastructures will leverage limited resources much more effectively than trying to patch the holes after systems are in place.

The second set of policy initiatives to address cyberterrorism should focus on steps to make it more dangerous for its perpetrators. Cyberterrorism offers opportunities for attackers to remain anonymous or at least unlocated. The US must improve national security, intelligence, counterintelligence, and law enforcement capabilities to track and identify cyberattackers. To achieve this goal, the US must first improve the exchange of information and cooperation across these communities. The NIPC was created to accomplish this task, but long-standing differences in organizational orientations and cultures must be surmounted. Providing these communities with adequate technological tools, organizational capabilities to fuse information, and skilled people to accomplish the mission will prove costly. While discussions of cyberdefense tend to focus on the technological, more difficult will be justifying the resources necessary to recruit and retain sufficient skilled personnel. The defense, intelligence, and law enforcement communities are losing personnel with computer and information security expertise as fast or faster than they can be trained. Establishing effective analytical methodologies for tracking and hunting down cyberterrorists also requires more attention. Finally, the legal context for US government intelligence and law enforcement efforts intended to combat cyberterrorism and other malicious activity requires examination for possible modification. Initiatives could include enabling the courts to issue a single warrant for law enforcement agencies tracking suspects through multiple locations in cyberspace. Cyberterrorists fearful of rapid identification and response by the US government may well have to modify their tactics and strategies substantially.

Finally, the US government must implement a more proactive education and public awareness strategy. At a minimum, such a strategy must stress awareness of individual and organizational responsibilities and liabilities associated with conducting business, recreation, or other activities in

cyberspace. Through the PDD-63 system of organizations, the government needs to establish and promulgate best practices for information system and infrastructure security. Going farther, the Federal government should implement a plan to limit confusion and hype in the event of cyberterrorist attacks. The government can potentially play a key role in identifying and limiting the impact of hoaxes. The most important task of the government at all levels if a cyberterrorist adversary was to wage a sustained campaign of disruption might simply be to provide accurate information about events and responses. In our open society, the US will continue to live with risks from cyberterrorism. The government role must focus on effectively mitigating these risks with the least impact on society as possible.

Conclusion

Much of the current hype about cyberterrorism is built on fear of the unknown. We need to move beyond simple speculation to more structured analysis of the threat and appropriate US responses. We do have sufficient reasons to believe cyberterrorism will become a more significant national security concern. The means are available but employing digital attacks to achieve specific terrorist objectives faces multiple obstacles. Within the US government, the challenge presented by the threat has received increasing attention. Plans have been formulated to address cyberterrorism as a part of the national critical infrastructure protection effort. Yet, these efforts are hampered by the narrow scope of defense efforts and inadequate resources. Developing robust defenses will continue to prove difficult. The most effective approaches to protect against cyberterrorism through establishing secure information systems and infrastructures must contend with technological and economic imperatives at the end of the 20th Century that cut in other directions. Improving the ability to track attackers involves issues of civil liberties and the role of government that require extensive public debate. Most clearly, US efforts to mitigate cyberterrorism will have to advance incrementally on a combination of fronts. We have no silver bullets for combating cyberterrorism. Rather, our nation must remain alert, learn, and invest wisely.

[1] The possibility of digital warfare and terrorism became a widespread concern in the early 1990s largely as a result of reports such as National Research Council, Computers at Risk: Safe Computing in the Information Age (Washington, DC: National Academy Press, 1991) and books such as Alvin Toffler and Heidi Toffler, War and Anti-War: Survival at the Dawn of the 21st Century (Boston: Little, Brown and Company, 1993).

[2] Quoted in Michael Evans, "War Planners Warn of Digital Armageddon" *London Times*, 20 November 1999.

[3] Walter Laquer, "Post Modern Terrorism" *Foreign Affairs* Vol. 75, No. 5 (September-October 1996), 35

[4] John Arquilla, David Ronfeldt and Michelle Zaninni, "Networks, Netwar and Information Age Terrorism" in *Countering the New Terrorism* (Washington DC: RAND Corporation, 1998), 71.

[5] See Bruce Hoffman and Caleb Carr, "Terrorism: Who is Fighting Whom?" *World Policy Journal*, Vol. 14, No.1 (Spring 1997), 97-104.

[6] This definition is based on that provided by Ian O. Lesser, "Countering the New Terrorism: Implications for Strategy" in *Countering the New Terrorism* (Washington DC: RAND Corporation, 1998), 85.

[7] As of the end of 1999, there are no publicly known examples of purposeful digital attacks disrupting train services or stock markets. However, computer systems failures in Washington DC disrupted early morning Metro service for a period of hours on 20 September 1999. The different US financial markets have shut down at times for short periods due to loss of necessary computer and information services. Reasons for these shut downs vary from backhoes cutting fiber-optic cables in New Jersey to floods in Chicago.

[8] On the possibility of use of use of weapons of mass destruction by terrorists, see Aston Carter, John Deutch and Phillip Zelikow, "Countering Catastrophic Terrorism" *Foreign Affairs* 77, No. 6 (November/December 1998): 80-94; and Richard Falkenrath, Robert D. Neuman and Bradley Thayer, Chapter 3 "The Threat of Nuclear, Biological, or Chemical Attack by Non-State Actors" in *America's Achilles' Heel* (Cambridge MA: MIT Press, 1998), 167-216.

[9] This perspective is exemplified by the annual State Department Report, *Patterns of Global Terrorism*.

[10] Robert Kaplan "The Coming Anarchy," *Atlantic Monthly* (February 1994), 44-76; and Martin Van Creveld, "What War is Fought For" *The Transformation of War* (New York: The Free Press, 1991), 124-156.

[11] Walter Laquer, *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (Oxford: Oxford University Press, 1999)

[12] Caleb Carr, "Terrorism as Warfare" *World Policy Journal* 13, No. 4 (Winter 1996-1997): 1-12.

[13] On the general concept of netwar, see John Arquilla and David Ronfeldt, *The Advent of Netwar* (Washington DC: RAND Corporation, 1996). As applied to terrorism, see Arquilla, et al, "Networks, Netwar and Information Age Terrorism."

[14] My analysis of the pros and cons of such an approach are fully elaborated in the forthcoming *Strategic Warfare in Cyberspace* (Cambridge MA: MIT Press, 2000).

[15] Clifford Stoll, *The Cuckoo's Egg* (New York: Simon & Schuster, Inc., 1989) contains an extensive description of the activities, discovery, and eventually apprehension of the hackers involved in this incident.

[16] General Accounting Office, *Computer Security: Hackers Penetrate DOD Computer Systems* (Washington, DC: GAO/T-IMTEC-92-5), 20 November 1991.

[17] See for example, Winn Schwartau, *Cyber Terrorism: Protecting Your Personal Security in the Electronic Age* (New York: Thunder Mouth Press, 1996), especially on pp. 543-544.

[18] This challenge is discussed in Andrew Rathmell, Richard Overill, Lorenzo Valeri and John Gearson, "The IW Threat from Sub-State Groups" in *Proceedings of the Third International Symposium on Command and Control Research and Technology* (Washington, DC: National Defense University, June 1997), 170.

[19] See *Cybercrime, Cyberterrorism and Cyberwarfare: Averting an Electronic Waterloo* (Washington DC: The Center for Strategic and International Studies, December 1998).

[20] Bruce Sterling, *The Hacker Crackdown: Law and Order on the Electronic Frontier* (New York: Bantam Books, 1992), 41-145 provides a lucid description of the hacker culture. Also see Dorothy E. Denning, *Information Warfare and Security* (Reading MA: Addison-Wesley, 1999), 46-50, for a concise summary of empirical studies on hacker motivations.

[21] See Michelle Satalla and Joshua Quittner, *Masters of Deception: The Gang That Ruled Cyberspace* (New York: Harper Collins Publishing, 1995) for descriptions of such activities.

[22] See Nicholas Chantler, "Profile of a Computer Hacker," available at http://www.infowar.com.

[23] See information at www.2600.com/home.html.

[24] "Call in the Goon Squad" C/NET Dispatches, 18 January 1999, available at hongkong1.cnet.com/Briefs/ Dispatches/China/990118/ss02.html.

[25] Associate Press release, "Chinese Cyber Battle: Hackers Put Taiwanese Symbols on Internet Sites" 12 August 1999, available at www.freedomforum.org/international/1999/8/12tapei.asp.

[26] See Jessica Stern, *The Ultimate Terrorists* (Cambridge MA: Harvard University Press, 1999), 74-75. Rathmell, et al, 176.

[27] Denning, 160.

[28] US Congress, Senate, Committee on Governmental Affairs, Testimony of Lopht Heavy Industries on Computer Security, 106th Congress, 2nd Session, 19 May 1998.

[29] See previously cited 2600 web site address.

[30] As examples of such studies see National Research Council, *Computers at Risk*; Defense Science Board Task Force, *Information Warfare—Defense* (Washington DC: Department of Defense, November 1996); President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington DC: President's Commission on Critical Infrastructure Protection, October 1997); and Statement of Michael A. Vatis, Director, National Infrastructure Protection Center "NIPC Cyber Threat Assessment" to US Senate, Judiciary Committee, Subcommittee on Technology and Terrorism, 6 October 1999.

[31] This quote was provided in Captain (USN) Richard P. O'Neill's presentation at an Institute for Foreign Policy Analysis conference on "War in the Information Age," Cambridge, MA, 15 November 1995.

[32] Anne W. Branscomb, *Rogue Computer Programs—Viruses, Worms Trojan Horses and Time Bombs: Pranks, Prowess, Protection or Prosecution* (Cambridge MA: Harvard University, Program on Information Resources Policy, I-89-3, September 1989), 1-5.

[33] A good analysis is provided by Neil Winton, "Y2K Seen As Possible Cover for Cyberwars" Reuters report on WWW at http://www.zdnet.com/intweek/stories/news/, posted 8 October 1999.

[34] Sterling, *The Hacker Crackdown*, 1-39.

[35] "Pentagon Beats Back Internet Attack" *Wired News*, 10 September 1998 and George I Seffers, "Hackers Take Offense at Pentagon Defense," *Defense News*, September 1998, 1.

[36] Information on this incident and other virus hoaxes can be found on the Internet at the Department of Energy Computer Incident Advisory Capability (CIAC) web site, ciac.llnl.gov.

[37] Chairman of the Joint Chiefs of Staff Memo CM-510-99, "Information Operations Condition," 10 Mar 99 provided the initial directive guidance regarding the establishment of a DoD INFOCON system.

[38] Winn Schwartau "An Introduction to Information Warfare" in Robert L. Pfaltzgraff, Jr. and Richard P. Shultz Jr., eds. *War in the Information Age: New Challenges for US Security* (London: Brassey's, 1997), 58.

[39] This assertion is made in a number of authoritative studies including 1996 Defense Science Board study, *Information Warfare—Defense*, 2-16, and the PCCIP, *Critical Foundations*, 19. This conclusion is also prevalent in the author's discussions with representatives of Software Engineering Institute's Network Survivability and Security Program and CERT Coordinating Center, the Defense Information Systems Agency's Automated Systems Security Incident Support Team (ASSIST), the Air Force Information Warfare Center.

[40] General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks* (Washington DC: GAO/AMID-96-84, May 1996), 15.

[41] Arquilla, et al, " Networks, Netwar and Information Age Terrorism," 65-66.

[42] Denning, 68.

[43] See Charles Swett, "The Role of the Internet in International Politics" in Robert L. Pfaltzgraff, Jr. and Richard P. Shultz Jr., eds., *War in the Information Age: New Challenges for US Security* (London: Brassey's, 1997), 292-293; and David Ronfeldt, John Arquilla, Graham Fuller and Melissa Fuller, *The Zapatista Social Netwar in Mexico* (Washington DC: Rand Corporation, 1999).

[44] Phil Williams, "Transnational Criminal Organizations and International Security" *Survival*, Vol 36, No. 1 (Spring 1994), 96-113.

[45] CIWARS Intelligence Report, 4 January 1998, vol. 2, no. 1 published by the Centre for Infrastructural Warfare, available on the Internet at WWW site at www.iwars.org, accessed 10 February 1998.

[46] National Research Council, *Computer at Risk*, 7.

[47] History of US efforts to deal with digital warfare and terrorism is discussed in depth in Chapter Five of my *Strategic Warfare in Cyberspace*.

[48] *Critical Foundations*, 2.

[49] See Office of Science and Technology Policy, *Cybernation: The American Infrastructure in the Information Age* (Washington, DC: The White House, April 1997) for an in-depth analysis of the significance of system complexity related to critical infrastructure protection.

[50] "Activist Hackers Target On-Line Toy Company," *Financial Times*, 19 December 1999.

[51] Richard Behar, "Who's Reading Your E-Mail," *Fortune* (3 February 1997): 64.

[52] Denise Shelton, "Banks Appease On-Line Terrorists" at news.cnet.com, posted 3 June 1996.

[53] The Toxyn hacker group published a call for attacks against Indonesian government sites on their web site at toxyn.pt.eu.org beginning in October 1997. The hacker magazine 2600 posted an example of a modified web page at their site at www.2600.com/east_timor/after.html.

[54] John Markoff, "Airports Told of Flaw in Security System" *New York Times*, 8 February 1998.

[55] See extensive discussion in Fredrick B. Cohen, *Protection and Security on the Information Highway* (New York: John Wiley & Sons, 1995), 33-78.

[56] "Fired Programmer Zaps Old Firm," on the Internet at biz.yahoo.com/upi/98/02/17/general _state_and_regional_news/nyzap_1.htm, accessed 10 March 1998.

[57] Computer Security Institute/Federal Bureau of Investigation, *Computer Crime and Security Survey* (San Francisco: Computer Security Institute, 1999), 4.

[58] Rathmell, 174-5.

[59] Denning, 69.

[60] Statement of Michael Vatis to Senate Judiciary Committee, 6 October 1999.

[61] William Church, *CIWARS Intelligence Report*, 10 May 1998.

[62] The history of US efforts to develop a national response to the threat of digital attacks is detailed in Chapter Five of this author's forthcoming *Strategic Warfare in Cyberspace*.

[63] This information was provided by the National Coordinator for Security, Infrastructure and Counterterrorism, Richard Clarke, at the "Preparing for Cyberwar" Conference, Arlington VA, 5 October 1999.

[64] National Infrastructure Protection Center Fact Sheet, 1999.

[65] The problems confronted by the US government in keeping skilled computer security personnel are illuminated by an article by Elizabeth Shogren, "U.S. Tries to Plug Computer Worker Drain," *Los Angeles Times*, 23 November 1999, 1.

[66] For descriptions of the incident, see Bradley Graham, "11 US Military Computer Systems Breached This Month," *Washington Post*, 26 February 1998, A01; James Glave, "DOD-Cracking Team Used Common Bug," on *Wired Internet* at www.wired.com, accessed 10 May 1998; and James Glave, "Pentagon Hacker Speaks Out," on *Wired Internet* at www.wired.com, accessed 10 May 1998.

[67] See Declan McCullagh, "Surveillance Network Draws Fire" from Wired News Online, 29 July 1999 at www.wired.com/news/news/politics/story/20994.html.

[68] Software Engineering Institute, *Detecting Signs of Intrusion* (Pittsburgh PA: Carnegie Mellon University, August 1997).

[69] See Office of the Staff Judge Advocate, AF Office of Special Investigations, "Computer Crime Investigator's Handbook" (Andrews AFB MD: AF Office of Special Investigations, May 1999) for detailed explanation of these constraints.

[70] This case is strongly stated in the Government Accounting Office study, *Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences* (Washington DC: GAO/AIMD-00-01, 1999). The US Air

Force and the National Research Council have instituted a joint effort to conduct a study along these lines.

[71] Specifics on the IAVA system are provided by Lt. Beth A Evans, Technical Analysis Division Chief, DoD CERT, "DoD's IAVA Process" *IAnewsletter* 3, No. 1 (Summer 1999): 8-9.

[72] A detailed analysis of this tension is provided in Chapter 5 of *Strategic Warfare in Cyberspace*. The debates within the US over encryption policy are fully addressed in Susan Landau and Whitfield Diffie, *Privacy on the Line: The Politics of Wire Tapping and Encryption*, (Cambridge MA: MIT Press, 1998).

[73] An analysis of such approaches in provided in Stephen J. Lusiak, *Public and Private Roles in the Protection of Critical Information-Dependent Infrastructures* (Palo Alto, CA: Stanford University, Center for International Security and Arms Control, March 1997).

Chapter Five

The Cyberterrorism Threat

Gregory J. Rattray

The last decade of the 20th Century has seen the rising concern over a new form of conflict, usually referred to as information warfare. As the US and other nations race forward into an information age, reliance on advanced information systems and infrastructures has grown significantly. Cyberspace has become a new realm for the exchange of digital information to conduct commerce, provide entertainment, pursue education, and a wide range of other activities. Information systems, in particular computer software and hardware, now serve as both weapons and targets of warfare.[1] The possibility of warfare in cyberspace presents opportunity but also involves significant new security risks. As the world's leading military power and the society most reliant on its information systems and infrastructures, the US may well face adversaries searching to find new weaknesses. These adversaries may include terrorists.

Similar to political assassination and car bombs, cyberterrorism could provide a new set of weapons for the weak to challenge the strong. Rapid technological developments based on the Internet and other information infrastructures through the end of the 20th Century create an attractive environment for groups who can not directly confront the US government, yet are willing to use death, destruction and disruption to achieve their objectives. Increasingly, cyberterrorists can achieve effects in the US from nearly anywhere on the globe. Terrorist groups can access global information infrastructures owned and operated by the governments and corporations they want to target. Digital attackers have a wide variety of means to cause disruption and/or destruction. Response in kind by the US government against sophisticated attackers is near impossible due to the difficulty of pinpointing activity in cyberspace and legal strictures on tracing attackers.

The possibility of cyberterrorism receives much attention. The Director of Central Intelligence, George Tenet, cautions about "a growing cyberthreat, the threat from so-called weapons of mass disruption."[2] Noted terrorism expert Walter Laquer observes "… why assassinate a politician or indiscriminately kill people when an attack on electronic switching will produce far more dramatic and long-lasting results."[3] A RAND study on terrorism produced for the US Air Force outlines the possibilities of "cybotage—acts of disruption and destruction against information infrastructures."[4] Yet, so far the US has suffered very little from cyberterrorism despite continuing conflicts with numerous adversaries, including those who employ terrorist means. Improved understanding of cyberterrorism must address why it has yet to fully emerge as a prevalent terrorist strategy. US policymakers need to understand constraints on its conduct as well as possibilities for its use.

What do we know? Evidence exists that cyberterrorism can occur. Government and commercial web sites are defaced almost daily. Computer systems suffer disruptions from intentional e-mail overloads and eruptions of viruses. Hackers of many stripes continue to prove capable of intruding on and exploiting a wide range of computer networks. These incidents can cause significant disruption and financial costs. However, cyberattacks have so far proved at most a nuisance for the US and its national security.

Looking to the future, we can expect cyberterrorism to become a more significant national security concern. Many assert that the US must expect a growth in the number of adversaries willing to use terrorist means.[5] The effectiveness of digital attack means will increase. So will US vulnerabilities to cyberterrorism. Terrorist organizations that wish to use these means can be expected to become smarter about both technological tools and effective targeting strategies. Limits to hitting back against cyberterrorism will remain a difficult problem.

Yet, cyberterrorists too will face significant challenges. When terrorists will develop requisite capabilities to conduct significant cyberattacks remains highly uncertain. The calculus of how cyberterrorism fits in with other

terrorist tools, including conventional weapons, weapons of mass disruption, and other techniques will determine the future significance of cyberterrorism. Cyberterrorism may well become a supplement to other terrorist means similar to how information warfare operations complement conventional military forces.

The US President, Congress and many others have clearly recognized concerns raised by cyberterrorism. The Federal government has initiated planning, assigning responsibility, and begun development of organizations to protect the US from cyberattack. However, these efforts are in early stages and must surmount considerable hurdles. The speculative hype combined with lack of real experience with this emerging phenomenon compounds the difficulty. A sound US policy to combat cyberterrorism and investment decisions must emerge from a balanced understanding of the potential threat and its limits.

Cyberterrorism—What Is It and Who Does It?

In general, terrorism proves a difficult topic to set boundaries around. One common approach to defining cyberterrorism is broad inclusiveness in addressing the actors, means and goals involved. My approach endeavors to delineate the threat in terms of factors relevant to evaluating US policy and organizational responses. Definitions and boundaries prove critical in establishing policy, defining organizational responsibilities and addressing resource allocation. So while arguably an artificial exercise, we will begin by answering two key questions—"What types of acts constitute cyberterrorism?" and "Who conducts cyberterrorism?"

This analysis of cyberterrorism centers on the activities of organized, non-state actors pursuing political or systematic objectives against the US[6] The activities of states conducting hostile activities in cyberspace against the US fall outside the realm of cyberterrorism into areas which can be labeled information warfare, espionage, or public diplomacy. However, we will consider the possibility that states may be associated with non-state actors in the furtherance of cyberterrorism. I also do not consider activities of individuals in the furtherance of personal objectives. However, because even individuals can

cause disruption and destruction in cyberspace, the possibility of cyberterrorists cooperating with individuals must be addressed. Also, while cyberespionage and cybercrime should not be lumped in with cyberterrorism, both types of activity could be used to support cyberterrorism.

Taking a stab at what acts constitute "cyberterrorism" involves addressing even fuzzier boundaries. From the traditional perspective, consideration of terrorism focuses on acts or threats of violence calculated to create an atmosphere of fear or alarm. For example, cyberattacks could cause train accidents with large death counts through tampering with digital signaling systems. Additionally, cyberspace presents myriad opportunities to commit acts that cause significant disruption to society without direct loss of life, injury, or harm to material objects. For example, digital attacks might cause stock market disruptions by denying service to computer and communications systems.[7] This analysis of cyberterrorism includes both acts that involve physical violence and those causing significant social disruption based on attacking information systems and infrastructures.

Additionally, cyberterrorists could conduct attacks with the goal of corrupting key information within a system that requires high confidence for its use. Corrupting information about blood types within a hospital data base or strike prices within the stock trade settlement systems would involve much more recovery time and effort than a simple denial of service attack on the same target. Such an attack would inflict direct economic costs from system downtime, checking and correcting data and settling disputes. Successful cyberterrorist attacks of this sort may also degrade user confidence in provision of services of fundamental importance to society.

Activities labeled as cyberterrorism must include recognition of both destructive and disruptive components. An open question is whether the potential for "mass disruption" created by reliance on information systems in the US will hold even greater appeal than attacks of "mass destruction" through the use of chemical, biological, and nuclear means.[8] Terrorists may prefer cyberattacks capable of causing widespread, observable impact but not

involving death and physical disruption rather than use of WMD or even conventional attacks in terms of limiting moral outrage and managing public opinion. Alternatively, "mass disruption" inflicted via cyberterrorism may prove too ephemeral to achieve desired effects. Governments and societies subject to cyber-based "mass disruption" may quickly learn to react and respond to such attacks, potentially even building up psychological resistance to such attacks.

Delineating the scope of activities that constitute cyberterrorism is difficult. The information age may well provide terrorist groups new ways to discredit governments and disrupt society to achieve their objectives. Therefore, cyberterrorism should be analyzed in light of the objectives sought.

Motives and Accountability

The nature of cyberterrorist campaigns, the means used, and the targets attacked will all depend on the motives of those groups considering the use of cyberterror means. Traditional analysis of terrorism has concentrated on groups with well-defined purposes for using violence as a means of political coercion.[9] Many terrorist groups such as the Weathermen within the US or the Red Brigade in Italy have engaged in efforts to overthrow or substantially change a political regime. Attacks are launched to undermine the legitimacy of the targeted government and garner support among a disaffected populace. Secessionist groups seeking the creation of new states or political autonomy for an ethnic/religious group also may use terrorist means to publicize their cause. Groups utilizing terrorist means to achieve such objectives include the Popular Front for the Liberation of Palestine and the Provisional IRA. A key feature of terrorism for political coercion is the willingness of groups to take credit for their attacks. The ability to inflict pain provides the principal source of leverage in negotiating with governments to achieve their objectives. Given the desire to secure the support of the general population and possibly to negotiate with governments, such groups may have self-imposed limits in terms of how vigorously and indiscriminately they choose to employ violence.

Taking a broader perspective on the issue of objectives, the use of terrorism by groups with millennial or anarchical objectives has become a

source of increasing concern.[10] Rather than pursuing a specific political agenda, such groups may use indiscriminate violence to create a general environment of fear and chaos prior to a general overthrow of Western political order or may even simply seek anarchy as a goal. The Aum Shinrikyo cult took no credit for the use of sarin gas by the in Tokyo subways. Laquer has highlighted the potential for such groups to view "superviolence" as an appropriate means to undermine the world political system in seeking their goals.[11]

A new thread in the analysis of terrorist motivations has received the label "war paradigm."[12] This paradigm holds that certain terrorist groups without the ability to confront opponents directly will take a strategic approach to conducting terrorist acts without making specific demands on the opponent. For example, Ramsey Yousef and others who executed the World Trade Center bombing had no known intent to acknowledge their role. The goal of such groups is to inflict damage and wear down opponents as part of an eventual victory in a long-term struggle. The focus of these analyses has been on groups motivated by Muslim fundamentalism, especially those associated with the Saudi jihadist Osama bin Laden. The attacks seen during the second half of 1990s on US military forces at Khobar Towers and embassies in Nairobi and Dar-es-Saalam may constitute such a campaign. Terrorists waging such campaigns may also see little constraint on inflicting damage or destruction against opponents.

Organization

Changes in the way terrorist groups organize will also impact their motives and perceptions of accountability. Traditional terrorist groups associated with the PLO and IRA relied heavily on tight central control over acts committed by the organization as part of an orchestrated pressure campaign against adversaries. However, the looser organizational structures of groups such as HAMAS, and Afgan Arabs may be enabled by the pursuit of less controlled, more destructive activities conducted by groups with anarchist or religious objectives. The "networked" organization of terrorist groups financially supported by Osama bin Laden has increasingly become the archetype for describing a new form of

terrorist organization with no clear center of control. John Arquilla and David Ronfeldt have strongly touted the strengths of such an organizational form for terrorists. Networked terrorist organizations could establish alliances of convenience with state sponsors, criminal organizations (especially those involved in the drug trade), and potentially with hacker groups.[13]

The utility for terrorist groups to employ the services of hackers as surrogates in the conduct of cyberterrorism has also received growing attention.[14] Hacker groups have demonstrated a willingness to sell their services to outsiders. In the most well known instance, hackers in Hannover, Germany during the late 1980s sold information they obtained through access to computer systems in Departments of Energy and Defense, defense contractors and NASA to the Soviet KGB.[15] These intruders first began to obtain access in 1986. After their initial discovery in 1988, the process of identification and apprehension of the Hannover hackers by the US and German intelligence and law enforcement agencies took over 18 months. During the Persian Gulf War, a group of Dutch hackers who had intruded into Department of Defense systems attempted to sell their services to the Iraqis but were apprehended by Dutch police.[16]

Most analyses of hackers as cybersurrogates for terrorism generally stress the ease and advantages of such activity.[17] It is presumed that terrorist groups will be able to easily contact hackers for hire while keeping their direct involvement hidden through the use of cut-outs and proxies. These hacker groups could then be employed to reconnoiter adversary information systems to identify targets and means of access. If hacker groups can be employed to actually commit acts of cyberterrorism, terrorist groups may improve their ability to avoid culpability or blame.

However, employing cybersurrogates would also involve important risks and disadvantages. Attempting to employ hackers to commit acts of significant disruption that may involve killing people would likely prove much more difficult than buying information for the purposes of intelligence gathering. Contacting and employing hackers would also involve major operational security risks for a terrorist group.[18] At a minimum, the intelligence

activities of hackers could be discovered and undermine planned operations. Terrorists without adequate leverage to control cybersurrogates run the risk of hackers being turned into double agents by hostile governments. The costs to a terrorist group of having an operation blown or providing adversaries information regarding their location or the identity of members would weigh heavily against use of such means. Both the German and Dutch hackers were eventually discovered, albeit after fairly long periods of activity and investigation.

The dearth of evidence means the calculus of terrorists considering use of cybersurrogates remains highly speculative at this point. One area for greater consideration is identifying which potential partners terrorist sponsors would consider more trustworthy. Some candidate surrogates, such as ex-security service members, may be considered more adept at maintaining operational security. Former members of the Soviet intelligence services that possess the requisite computer expertise and experience in the black arts of espionage may pose a real concern.[19] Terrorist groups may already have forged links with such potential allies. The subject deserves dedicated intelligence gathering efforts and analysis rather than simple hype.

Hacker Groups and Terrorism

Additionally, one must consider to what degree organized groups of hackers acting on their own accord pose a terrorist threat. For purposes of this analysis, hacker refers to persons or groups who gain access or break into digital systems, particularly networked computer and telecommunications systems. Hackers have a wide range of motivations including thrill seeking, knowledge, recognition, power, and friendship.[20] These individuals have also developed a sophisticated network to communicate ideas and coordinate activity through magazines such as *Phrack* and *2600*, stolen phone services, e-mail distribution lists, Usenet newsgroups, Internet chat rooms and even full-blown conferences such as DEFCON. According to one survey of hackers, over half of those asked said they work in teams, and more than a third indicated they belong to a specialized hacker group. Groups have names such as Legion of Doom, Masters

of Destruction, and Cult of the Dead Cow. These groups have been known to wage conflicts on each other using the public telecommunications networks as a battleground and touting their degree of illicit access as the source of bragging rights.[21] Many groups analyze software weakness and provide digital tools to exploit mainstream software applications such as Microsoft Windows operating systems. Additionally, hackers are dominantly males between the age of 15 and 25, often disaffected with the prevailing social and governmental order. This profile parallels those involved in terrorism.[22] The combination of technological skills and disaffection could make a sufficiently motivated and organized hacker group in a considerable cyberterrorist threat.

Numerous hacker groups have expressed deep animosity against the US and other governments over attempts to prosecute hackers, regulate activity on the Internet and other political issues. The hacker magazine *2600* has orchestrated a major campaign, including a fundraising campaign, to get the government to release Kevin Mitnick convicted of numerous violations of US computer crime laws.[23] In December, the group known as the Legion of the Underground (LoU) issued a "declaration of war" against the governments of the People's Republic of China and Iraq citing these regimes' repressive human rights policies. The LoU declared its intention to disrupt and disable the Internet in the two countries. [24] East Asia has also witnessed an exchange of digital intrusions targeted at defacing Taiwanese and People's Republic of China government web sites with nationalist symbols and slogans of the hacker's home state.[25]

Thankfully, however, typical terrorists and hackers also have significant differences. Terrorists are generally conservative regarding use of new technologies to conduct operations. [26] Some groups have even conducted attacks to specifically combat the spread of computer technology. A French group called the Computer Liquidation and Deterrence Committee attacked French and American computer companies during the 1980s because "the computer is the tool of the dominant. It is used to exploit, to put on file, to control, and to repress."[27]

Conversely, the Internet community has seen the rise of white-hat hacker groups with a range of objectives. Some such as the LoPht Heavy Industries group based in Boston simply seek to provide information on latest hacker tricks and security weakness in products. LoPht has also called for hackers to cease attacks against the US government and testified for the Senate on how to improve computer security efforts.[28] The hacker community has also demonstrated a willingness to impose discipline on its own against disruptive hacking when the potential government backlash may prove too severe. A coalition of hacker groups formally condemned the LoU's declaration of war. *2600* magazine declared "This type of threat, even if made idly, can only serve to further alienate hackers from mainstream society and help spread the misperceptions we're constantly battling."[29] So far, the hacker community has stopped shy of conducting activities constituting a serious cyberterrorist threat.

Means and Targets for Cyberterrorism

The headlong rush of the US and other advanced nations into the information age involves new risks. The information systems central to national security, the conduct of government and commerce have significant weaknesses that can be attacked. Yet, such attacks have achieved only limited impacts as we end the 20th Century. To analyze how cyberterrorists might attack the US, we must consider which groups might employ cyberterrorism and for what reasons.

Means for Digital Attack

Terrorists could attack US information infrastructures using a variety of mechanical, electromagnetic, or digital means. Information systems have long been targets of mechanical methods of disruption. Command and control systems can be bombed, fiber-optic cables cut, microwave antennas broken, and computers smashed or simply turned off. The electronic components and transmissions of information systems and networks are vulnerable to jamming, as well as electromagnetic pulses generated by nuclear explosions and other sorts of directed-energy weapons. The rise of digital means of encoding and transferring information has also created new ways to attack information systems. Impacts of digital attacks can range from total paralysis of networks to

intermittent shutdown, random data errors, information theft, and data corruption. The tools and techniques for attacking information systems have received detailed attention as the US government, commercial industry, and outside experts have begun to stress the possibilities of information warfare, digital espionage and computer crime.[30] The analysis below focuses on digital means as the new dimension of the equation appropriately labeled cyberterrorism. The possibility of synergistically employing all three types of attack also requires additional analysis beyond the scope of this chapter.

Cyberterrorists could cause disruption, damage, and destruction through achieving unauthorized access and control over a targeted information system through a vast array of intrusive tools and techniques, commonly referred to as "hacking." Means for successful intrusion range from compromised passwords to sophisticated software for identifying and exploiting known vulnerabilities in operating systems and application software. The difficulty of attaining access and time required to successfully "hack" a system will also depend on the targeted system's defensive measures including proper password and configuration management, patching of known vulnerabilities, and use of firewalls and intrusion detection systems. If control over a targeted computer or network is achieved, cyberterrorists could inflict a wide range of effects. Possibilities range from changing the graphics on a web page to corrupting the delivery schedules for medical supplies or military equipment to denying access to 911 services, air traffic control data, or disrupting telecommunications backbone networks. A principal advantage of intrusion for cyberterrorism is the potential for tight control over the timing, scope and effects of an attack. According to former Director of the Central Intelligence, John Deutch, "the electron is the ultimate precision weapon."[31]

Another well-known potential means for cyberterrorist attack would be the employment of malicious software code, more commonly referred to as viruses and worms. Malicious software can be broadly defined as software designed to make computer systems operate differently than intended. The effects of viruses and other malicious software range from benign messages

displayed at system start up to code that can cause hardware failures and wide-area network overloads. Concern over malicious software increased rapidly after the unintentional release of the Internet Worm by a Cornell graduate student in 1988 disrupted most Internet services for a period of days.[32] During the early 1990s, reacting to and mitigating the consequences of viruses was a major computer security focus. Development of anti-virus software capable of periodic updating has helped mitigate the virus threat. However, 1999 saw a series of virulent outbreaks, including the Melissa virus and Worm.ExploreZip that proved capable of disrupting government, commercial, and other private information systems. A major feature of these viruses has been traffic overloads that occur when the viruses propagate vast amounts of e-mail through networked systems. Creators of malicious software determine the intended impact of running their code. However, the degree of disruption and damage caused by viruses and other code which replicates and passes quickly across networked systems can be much more difficult to control. Cyberterrorists using malicious code created by others may have much less certainty regarding the effects of their attack.

Combining features of both intrusions and malicious code, cyberterrorists could also intentionally corrupt software programs in targeted information systems and infrastructures to cause desired effects. While access to rewrite software code could be achieved through an intrusion, a terrorist group may endeavor to corrupt software in the process of creation or production by emplacing backdoors for access or insert "trojan horses" to cause desired effects at a predetermined time or upon a given command. Software maintenance and updates also present opportunities for such activities. Software code creation and maintenance for systems employed across the globe occur in places like India, Ireland, and Israel. The possibility for insertion of corrupted code as part of the massive effort to update software to fix Year 2000 problems provided a major concern for all sectors of the US government and society.[33] The main protection against such activity would be rigorous quality control over software products used in key systems, but such a process is time-consuming

and expensive. As with intrusions, the degree of control possible through corrupted code can allow precision effects. Cyberterrorists could also achieve widespread effects by corrupting code in systems underpinning key information infrastructures. AT&T suffered nation-wide disruption of its telephone network in January 1990 due to a single line of faulty code in an upgrade to its primary switching software.[34] While this error was unintentional, the ability to attack the digital foundations of advanced information infrastructure presents sophisticated cyberterrorists with a significant means of attack.

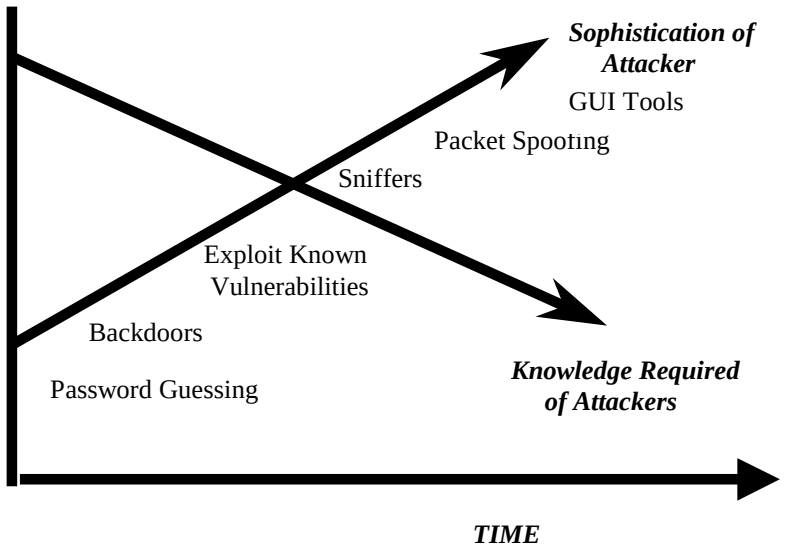
Cyberterrorists can also disrupt or disable information systems and networks using techniques generically labeled as denial-of-service (DOS) attacks. Common DOS techniques involve overloading targeted e-mail systems by employing automated software and exploiting features of the Internet communications protocol through "smurf" or "SYN flooding" attacks. In recent years, hackers and politically motivated groups have increasingly turned to DOS attacks as a means of responding to specific events and policies by harassing targeted organizations and to draw attention to their complaints. One well-known instance involves a group known as the Electronic Disturbance Theatre (EDT). In October 1998, the EDT targeted the computers of the US military and the Frankfurt Stock Exchange in an effort to overload servers in these networks with the goal of publicizing the cause of the Zapatista rebels in Mexico. Yet, while cyberterrorists can specifically target denial-of-services attacks against known systems connected to network accessible to the attackers, operators of the targeted systems can also modify their systems either preventively or in reaction to the attacks. The Defense Information Technology Center simply reconfigured the targeted computers to refuse to acknowledge the originating Internet addresses in response to the EDT attacks. The EDT computers were overloaded with return messages as a result of employing the automated FloodNet software and forced to reboot.[35] The cat and mouse game of offensive moves and defensive responses will continue to evolve as information technology advances and presents new vulnerabilities to exploit. Cyberterrorism

and other types of warfare, espionage, and crime waged in the digital realm will demonstrate this see-saw dynamic.

Another possible approach open to cyberterrorists would be to conduct hoax attacks, publicizing the possibility of intrusive activity and release of viruses. Virus scares can swamp help desks with requests for information. Users and system operators must ensure anti-virus software is up-to-date, creating an additional burden on the networks and wasting time. The Good Times scare in 1994 caused a massive reaction while only infecting a handful of computers.[36] Similarly, the possibility of intrusive activity requires system administrators and computer incident response teams to assume higher states of readiness with an attendant decline in attention to routine operations and maintenance. The US Department of Defense has instituted an Information Operations Condition (INFOCON) system of progressively higher levels to raise the awareness and preparedness of cyberdefenses similar to the THREATCON system use for responding to increased threat of terrorist attack.[37] Attaining the defensive posture called for by higher INFOCON levels would require substantial efforts for those responsible for the DoD information infrastructure and pose constraints on the use of the Department's information resources. Cyberterrorists focused less on high impact events and more on waging a protracted conflict could use hoaxes designed to cause the targeted adversary to waste significant effort without the terrorist having to run the risks of conducting actual attacks. Defensive efforts may suffer over the long-term if multiple hoaxes create a "cry wolf" syndrome regarding calls for increased protection. The impact of hoaxes will be magnified if terrorist groups develop a credible reputation for being able to conduct digital attacks.

Access and Expertise

To use any of the tools and techniques described above, cyberterrorists must have access to the means and the expertise to employ these tools effectively. The prevailing wisdom is that both are readily available. Well-known information warfare pundit, Winn Schwartau states, "Anyone can be an



information warrior…. Potentially, a hundred million information warriors are poised, and honing their skills while they wait."[38] Numerous analyses cite the vast number of web sites on which hacker tools and techniques can be found and downloaded, as well as the presence of Internet chat sites, conventions, catalogues, and publications in which hackers exchange information.[39] In a similar vein, most analyses also hold that the means for attacking information systems have become both more sophisticated and easier to use. The following figure from a 1996 GAO report entitled *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks* depicts the evolution of attack tools and required expertise as time has progressed.[40]

One way terrorists may build their expertise and understanding of the potential for digital attacks is through the use of cyberspace for other activities. Increasingly, terrorist groups including the Provisional IRA, Algerian extremists, HAMAS, and others are using the Internet and cellular phones to orchestrate their activities. Many groups have begun to use encryption technology to protect their digital communications. According to Arquilla,

> Egyptian "Afgan" computer experts have helped devise a communication network that relies on the World Wide Web, e-mail and electronic bulletin boards so that extremists can exchange information without a major risk of being intercepted by counterterrorism officials.[41]

The Provisional IRA uses computer databases to catalogue individuals, installations, and other targets.[42] Terrorists and associated groups have also begun to use the Internet as a mechanism for publicity, fundraising, and recruitment. The Zapatistas have established a major presence through the World-Wide Web supported by activists in the US, Europe, and elsewhere.[43] Drug cartels use the Internet in transactions with banks to launder money, and at least potentially, terrorists could use cybercrime to steal money to support their operations.[44] Terrorists may also use advanced information technology for intelligence gathering. Access to commercial satellite imagery may provide information for targeting physical attacks. Hacker and information warfare websites may provide conceptual approaches and even lists of targets for cyberterrorism. Evidence is clear that terrorist groups increasingly use advanced information technologies and are building an experiential base that could be used for cyberterrorism.

However, the utility of user-friendly attack technologies and general computer expertise to any terrorist group depends on the nature of the targeted infrastructure and intended effects. Denial of service attacks against Internet connections may require much less sophistication but achieve less controlled effects than attacks based on successful remote access and control of a targeted information system or network. Additionally, a defender's ability to assess vulnerabilities and deny access to known digital attack tools and techniques may also increase the level of technological knowledge required for attacking forces. If key information infrastructures are well protected, achieving surprise and inflicting disruption against significant centers of gravity may require cyberterrorists to employ more technological sophistication, time, and effort. The pool of human capital with the ability to develop sophisticated new attack tools or quietly probe strong, attentive defenses is much more limited than the

number of individuals capable of running scripted tools or sending multiple e-mail messages to an Internet address. The Center for Infrastructural Studies stated in early 1998, “According to recent studies, most attacks use standard or well-known script exploits. Our research reveals less than 1,000 hackers in the world who have the professional programming skills to create their own attack scripts.”[45]

For cyberterrorists, easily accessible and usable digital attack techniques may equate to more conventional hand grenades and pistols in terms of scale of effects and lack of precision. To develop the digital equivalent of weapons of mass destruction or achieve the precision of sniper rifles may require a much greater degree of technological sophistication and self-reliance on the part of cyberterrorists. Developing collection means and analytical techniques to understand the technological skill and resources of terrorists presents an important challenge for the US intelligence community.

Targets for Cyberterrorist Attacks

Since at least the early 1990s, the US government and outside experts have grown increasingly concerned about the possibility of cyberterrorist attacks as our society has become more reliant on information systems and infrastructure. The 1991 National Research Council *Computers at Risk* report finds, "The modern thief can steal more with a computer than a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than a bomb."[46]

The increasing ability of terrorists and others to attack US critical infrastructures through use of digital attacks has received the most attention.[47] In the wake of the Oklahoma City bombing in 1995, the President set up a Critical Infrastructure Working Group to address both physical and cyber threats. As a result of hacker incidents, Department of Defense exercises and Congressional prodding, the Presidential Commission on Critical Infrastructure Protection was set up to analyze the threat to US infrastructures and policy responses for their protection. The PCCIP's October 1997 report, entitled *Critical Foundations*, provides the most comprehensive analysis of the cyberthreat to US infrastructures "essential to minimum operations of the

economy and government."[48] The report stresses how the growing reliance on information systems that underpin a whole range of infrastructures including communications, electric power, transportation, and emergency services creates substantial risks for a wide range of digital attacks, including possible cyberterrorism. While a comprehensive discussion is beyond the scope here, possible targets for cyberterrorism include the Supervisory Control and Data Acquisition (SCADA) systems which govern the distribution of telecommunications, electric power, and other infrastructure-based services. The Global Positioning System (GPS) network of satellites, ground control stations, and signaling systems constitutes an infrastructure target whose role in military and civil navigation as well as broadcasting timing signals in cellular communications and other information networks could prove attractive to cyberterrorists. The disruption caused by the failure of a single PanAmSat communications satellite in May 1998 crippled most US paging services as well as a number of data and media communications feeds for hours and, in some cases, a couple days.

While attacking information systems underpinning critical infrastructures presents cyberterrorists with potentially high impact targets, important questions need to be addressed in order to adequately gauge the potential threat. One area of significant uncertainty is how fast infrastructures will be able to recover from digital attacks. Many analysts focus on how many infrastructures have single points of failure that can cause quickly cascading effects disrupting or disabling effects over a wide area. The Northwest power outage in August 1996 that affected hundreds of thousands of users began by a tree growing into a single power line. Others point to the ability of complex systems to adapt and recover.[49] In the cases of the AT&T switching failure, the Northwest power outage, and the PanAmSat satellite failure, the infrastructure operators were able to recover in a period of hours. What is clearly unknown is how such complex infrastructures would react to orchestrated cyberterrorist attacks instead of unintentional mishaps and accidents.

Another approach would be to attack organizations or institutions with high public visibility. Hackers have proven capable of repeatedly defacing the web pages of corporations such as DuPont and Ford as well as government agencies including the White House, FBI, NASA, and the Air Force. Cyberterrorist attacks may specifically be launched to garner media attention rather than cause physical damage or economic losses. Demonstrated ability to disrupt computerized inventory systems of Wal-Mart or corrupting medical records within a large health management organization would provide prime fodder for media attention. Newspapers have reported that the hacker group, RTMark, has endeavored to depress the stock price of eToys by disrupting the company's web site.[50] Financial institutions have often been listed as a potential target of cyberterrorism. Citigroup admitted in a highly publicized incident that a Russian hacker managed to electronically siphon off $12 million in funds in 1995. While Citigroup actually managed to recover all but $400,000 of this loss, competitors reportedly used the incident to convince commercial clients to switch banks due to the perceived greater insecurity of Citigroup information systems.[51] In 1996, the *London Times* reported that banks, brokerage house, and investment firms paid hundreds of millions of dollars in blackmail to extortionists to avoid cyberattacks whose capabilities had been demonstrated.[52] The high level of media attention to financial markets and the critical role of public confidence in their activities mark them as prime targets.

Terrorist groups could also conduct digital attacks against media outlets themselves. Indonesian media outlets had their computer systems attacked by hacker groups supporting the Timorese rebels.[53] However, cyberterrorism targeted with an eye towards garnering media attention rather than death and destruction may require more sophisticated targeting and digital attack capabilities than generic attacks against any open targets within the US infrastructure. The disruptive effects of such attacks may prove short-lived, but cyberterrorists could endeavor to shake public confidence in core institutions through such attacks.

Terrorist groups could also use digital attacks to support traditional terrorist operations. As monitoring and sensor systems for protecting people and facilities become increasingly reliant on information technology, digital attacks may prove a useful means of creating opportunities for conventional terrorism. In 1998, the *New York Times* reported a design flaw in a security system widely used in airports, prisons, financial institutions, and the US government allowing digital intruders to access secure areas, unlock doors, and erase evidence of changed access records.[54] Emergency 911 systems have been found vulnerable to computer intrusions and could be targeted by cyberterrorists. Paralyzing communications as a means of slowing emergency responses could plausibly enhance effectiveness of conventional or WMD terrorism. As with any potential tool, terrorist groups could employ cyberattacks synergistically along with other means to achieve their objectives.

Cyberterrorists may also endeavor to make use of "insiders." Reasons for assisting terrorists could include personal gain, revenge, or sheer destructiveness. The assistance of individuals knowledgeable of technical characteristics and operational significance of a targeted information and systems would prove of immense value to terrorist groups in launching all types of digital attacks. The threat posed by insiders with authorized access to information resources presents a fundamental information security concern.[55] A network programmer fired by Omega Engineering Corporation in 1996 provides an illustrative case. Upon his departure, the programmer activated a logic bomb that permanently deleted all the company design and production software used to produce high technology measurement and control instruments for the US Navy and NASA. Damage was estimated at $10 million.[56] The 1999 Computer Security Institute/Federal Bureau of Investigation "Computer Crime and Security" survey indicated sixty-five percent of organizations responding had suffered incidents involving insiders.[57] Cyberterrorists intent on causing widespread destruction and damage might use insiders to corrupt SCADA systems or plant viruses. The ability to effectively screen employees, discover attempts at outside recruitment, and identify and mitigate malicious activities

quickly will play a role in combating cyberterrorism as part of overall information security efforts

Thinking About Cyberterrorist Campaigns

With a wide range of available tools and potential targets, cyberterrorist groups may use very different types of campaign strategies to pursue objectives. So far, most attention focuses on the possibility of single events causing catastrophic physical effects such as a plane crash or the failure of control systems in a nuclear power plant. The assumed objective of the attack is widespread publicity for the group's cause and negotiating leverage against governments. A potentially more serious threat that receives less attention would involve cyberterrorist groups adopting a protracted war strategy similar to the ones used by Mao Tse Tung and Ho Chi Minh. Instead of striking the most dramatic target, terrorists waging a protracted guerilla campaign of cyberterror could strike targets of opportunity that also minimized the chance of discovery and retaliation. The objectives of such a campaign may well involve media attention but also target the will of an adversary's government and populace over the long-term.

Developing a strategy for dealing with single cyberterrorist events may focus on improving warning of attacks and the ability to manage the consequences of disasters. Responses to waging a prolonged conflict with cyberterrorists may be quite different. Fighting such adversaries will require improvement in defensive capabilities and recovery capacity of information infrastructures as well as improving means to track down and incapacitate attackers.

Outlining these two broad strategic approaches and their implications simply provides an illustration of the complex situation facing those responsible for dealing with cyberterrorism. The US government must develop a deeper understanding of how different cyberterrorist groups are most likely to operate, potential objectives and capabilities, the risks posed by attacks, and appropriate responses. This analysis must be based on fact, not speculation.

Cyberterrorism—What We Have Observed

Information infrastructures have long served as targets for adversaries in a conflict. Adversaries have always attempted to intercept messengers. The emergence of electronic communications resulted in cutting telegraph lines and underseas cables during wars. As more communications passed via electromagenetic transmissions, jamming, frequency hopping, and other techniques became a commonplace aspect of military operations known as electronic warfare.

Terrorists have also seen attacks against infrastructures as a means of achieving their traditional objectives. For example, the Provisional IRA in the early and mid-1990s launched major terrorist attacks against transportation and commercial targets in U.K. with the intent of maximizing societal disruption. In April 1993, a bomb detonated in London caused massive commercial disruption by causing the temporary closure of key financial markets.[58] In the 1970s, the Italian Red Brigades specified destruction of computer systems and installations as a way of striking at the state. They conducted numerous attacks against businesses in the elctronics and computer industries.[59] As the functioning of information systems and infrastructures becomes increasingly fundamental to US and other societies, the appeal for terrorists to attack such targets will increase. Lessons learned about what constitutes key features of an adversary's information infrastructure necessary for the conduct of conventional attacks would also prove useful to cyberterrorists considering the use of digital attacks.

Hackers and hacker groups so far have not proven to be significant cyberterrorist actors in terms of conducting digital attacks to create intentional death, destruction, or disruption. While there have been occasional declarations of intent to wage "cyberwar" against the US government, corporations or other entities, these threats have not resulted in serious campaigns to achieve political or even anarchical objectives. However, the dearth of cyberterrorism by hackers so far does not mean they are not capable of inflicting severe damage via digital attacks. Hackers have intentionally disrupted 911 services, launched viruses degrading the information processing of major corporate and government

organizations, and gained access to key computer systems such as domain name servers which underpin information infrastructures in such organizations. A good example of the potential for hackers to become cyberterrorists is provided by an incident in March 1997. In this instance, a teenage hacker penetrated and disabled Bell Atlantic telecommunication switches in the Northeastern US One of the disabled switches provided phone and data services to the Worchester, Massachusetts airport control tower, and the incident shut down the airport for many hours.[60] If such an attack were purposely targeted and timed when air traffic control was already difficult due to weather or volume of traffic, the difference between what happened in Worchester and a cyberterrorist attack would only be a matter of intent.

An increasingly common phenomena related to cyberterrorism is hacking by technologically literate groups in support of insurgent, environmental, or other political movements. Hacking into and defacing Web pages has proven a most common means to express discontent. However, the rise of purposeful denial-of-service attacks such as the one by the EDT has also caused increased concern. So far, such activities have proven at most temporary nuisances rather than real problems that might coerce targeted governments to change policies. Yet, reacting to such threats already involves increasing resource commitments by organizations such as the Department of Defense and FBI. Such activity clearly falls within the boundaries of terrorist intent discussed earlier. The real question is when does the level of disruption rise to a standard appropriately labeled as terrorism instead of mischief.

In terms of known terrorist groups using digital attacks for cyberterrorism, we have only begun to see such activity occur. The most well-known case has involved the Internet Black Tigers, an offshoot of the Sri Lankan rebel group Liberation Tigers of Tamil Elam. The Internet Black Tigers swamped the e-mail services of numerous Sri Lankan embassies for a period of approximately two weeks.[61] Yet, such attacks comprised a relatively insignificant aspect of the overall terrorist campaign of these rebels and arguably were principally for publicity rather than disruptive objectives.

A major terrorist campaign waged principally or solely via digital attacks has not occurred. As with other forms of conflict, cyberterrorism will likely evolve as another tool for groups to achieve their objectives rather than springing into life in full bloom. That said, successful cyberterrorist attacks could also provoke a rapid rise in activity once such means are a proven way to achieve terrorist goals. The focus for US policy should be to understand the goals of groups who are most likely to employ such a new approach and potential vulnerabilities arising from possible cyberterrorist attacks.

The US Response

The US national government has recognized the growing threat posed by cyberterrorism. A detailed development of US policy and organizational responses to cyberterrorism is beyond the scope here. The section below presents a brief overview of what has been accomplished and what is yet to be done.

Over the past decade, a confluence of concern with information warfare, terrorism against US targets at home and abroad, and the recognition of the increasing reliance on critical infrastructures all have made dealing with cyberterrorism a higher priority on the national security agenda. A spate of books and articles in the mid-1990s focused on the possibility of a digital Pearl Harbor facing the US The President established a Critical Infrastructure Working Group in 1995 in the wake of the Oklahoma City bombing to address both physical and cyber terrorist threats under the leadership of the Justice Department. Congressional inquires and GAO reports have described the vulnerabilities of our digital infrastructure to hackers and called on the President to details plans to develop cyber defenses. Such threats have been examined through RAND "Day After in Cyberspace…" wargames and DoD exercises such as Eligible Receiver. These evaluations demonstrated significant national and DoD vulnerabilities that would arise from a structured cyberattack.[62]

Growing demands for a comprehensive response have resulted in the US government putting increasing energy behind its response to possible cyberattacks. In the summer of 1996, the President's Commission of Critical

Infrastructure Protection was formed to conduct a comprehensive review and recommend national policy for protecting critical infrastructures against physical and cyber threats. The PCCIP's efforts formed the basis for Presidential Decision Directive 63 "Critical Infrastructure Protection" issued in May 1998. In combination with PDD-62 "Protection Against Unconventional Threats to the Homeland and Americans Overseas," the two directives establish a system of organizations, roles, and responsibilities through which the US will respond to terrorism and protect its critical infrastructures during peace and war.

Since the spring of 1998, national efforts against digital attacks have focused on implementing the construct laid out in PDD-63. The Directive created a National Coordinator for Security, Infrastructure Protection and Counterterrorism on the National Security Council. Departments and agencies within the Federal government have developed sector-specific protection plans across the range of identified critical infrastructures. The Critical Infrastructure Assurance Office (CIAO) in the Commerce Department assists in sectoral planning efforts and their integration into a national plan. The private sector has also started to establish Information Sharing and Analysis Centers (ISACs) as called for in PDD-63. As of late 1999, the first ISAC was established in the banking and finance sector with other ISAC plans under development.[63]

On the operational side, the National Infrastructure Protection Center was established even prior to the issuance of PDD-63 in February 1998.[64] As staffing and resources have increased over the past few years, the NIPC and Federal government agencies have initiated numerous efforts to coordinate activities in response to cyber threats. The NIPC and CIAO are endeavoring to establish linkages with state and local governments as well as the private sector. Yet, the hurdles to improve cyberdefenses are substantial and resources remain limited.

Challenges in Responding to Cyberterrorism

The US intelligence community must play a key role in understanding the threat posed by cyberterrorism. Effective responses require the US both to understand the potential capabilities of cyberterrorist groups and develop advanced warning

regarding their intent to use such capabilities. Cyberterrorism presents a very difficult intelligence target. The highly developed imagery and signal intelligence capabilities used to characterize Cold War threats and nation-state military capabilities have limited applicability in providing information to assess whether terrorist groups can effectively employ digital attacks. Also, the skill sets of intelligence analysts required to understand digital communications systems and techniques for exploiting computer weaknesses are not the same as those to characterize capabilities of ballistic missiles and the strength of ground forces. Also, the new skill sets are in high demand in the private sector making them even harder to create and sustain within the US government.[65]

To provide strategic warning of cyberterrorism, the intelligence and defense communities require insight into activities of adversary groups to develop profiles of preparatory steps for digital attacks. In the cyberrealm, distinguishing potential terrorist activity from normal system failures, exploratory hacking, and other threats such as espionage is very difficult. In the spring of 1998, the Department of Defense was initially concerned that hacking activity eventually tracked down to teenagers might have been state-sponsored activity related to US military activities in the Persian Gulf.[66] Conducting counterterrorism involves close coordination between organizations responsible for intelligence, counterintelligence, and combating computer crime. Potential terrorist activity in cyberspace presents particularly acute requirements for such cooperation.

PDD-63 and other policy directives have set in place the organizations and responsibilities. At the national level, the NIPC has primary leadership for detecting and responding to digital attacks. The Defense Department established a Joint Task Force - Computer Network Defense to provide centralized capability for the same missions to protect the Defense Information Infrastructure. A program to create a comprehensive Federal Intrusion Detection Network (FIDNet) system under the authority of GSA exists.[67] Other organizations in the public and private sectors have established efforts to achieve similar objectives. In addition to the ISACs, a number of computer

security associations and consulting firms strive to improve computer and information security in the private sector. These organizations generally work closely with a community of Computer Emergency/Incident Response Teams known as CERTs or CIRTs established by many organizations in both the government and in the private sector.

Yet, despite the presence of such organizations, those responsible for US cyberdefense at all levels have very limited capability to provide tactical warning of impending attacks or assess attacker motivations and objectives. Defensive tools, primarily in the form of various types of intrusion detection systems, have been developed to help identify presence and intent of malicious digital activity. However, current IDS technology relies on identifying known types of exploits and can not easily identify new types of digital attacks, even those based on modifying previous types of exploits.[68] Adequate attack assessment is even tougher. Owners, operators, and defenders of information systems and infrastructures rarely have an adequate picture of what they are protecting. Defenders not only need to understand physical and logical interconectivity, they also need to understand the operational significance of information and systems which are under attack to properly prioritize their warning, detection, and response efforts.

In specific circumstances, CERT and law enforcement agencies have proven capable of tracking down and punishing attackers. However, the timelines to identify and prosecute responsible individuals in most well-known hacker incidents have been lengthy and the punishments meted out fairly light. The capacity of the NIPC, the JTF-CND, and other organizations to handle big events involving large numbers of sophisticated attackers is unproven. Legal and policy considerations also place constraints on such agencies attempting to precisely identify individuals and organizations responsible for malicious activity in cyberspace. Law enforcement and computer network defense organizations are not allowed to hack back though computer systems to follow the electronic trail of intruders without express permission of system owners or authorized search warrants.[69] Yet, most digital intruders utilize multiple hops

through cyberspace before conducting intrusive activity. Also, the CERT and law enforcement communities most closely involved with leading responses to computer intrusions tend to focus on single incidents. Defending against cyberterrorists with long-term objectives and significant attack capabilities will require fighting a campaign, a perspective significantly different than a law enforcement effort focused on building a court case.

Federal government plans also have identified organizations responsible for responding if a cyberterrorist attack caused significant disruption or destruction to mitigate effects and restore capabilities. Under the authority of PDD-63, the Federal Emergency Management Agency (FEMA) would lead consequence management efforts in conjunction with the NIPC, FBI, and state/local authorities. US national-level planning for how to deal with major disruptions to information systems and infrastructures was accelerated due to the requirement to be ready for Year 2000 events. Yet, a continuing consequence management challenge is the lack of detailed knowledge of the network connectivity, information system characteristics, and operational significance of assets that may suffer a cyberterrorist attack. Lack of adequate information infrastructure "mapping" will hamper the prioritization of reconstitution efforts and deployment of available resources. Establishing effective consequence management capabilities also faces difficulties in terms of running operational exercises to simulate large-scale terrorist attacks against complex, interconnected, privately owned and operated information infrastructures. Currently, organizations responsible for responding to cyberterrorism lack understanding of possible modes of system failure and the ability of infrastructures and operating organizations to recover from attacks. Again, those responsible for consequence management efforts should leverage knowledge gleaned from Y2K preparations and experiences with failure and recovery characteristics from Y2K events.[70]

The final step in defending against cyberterrorism is to improve the strength of our information infrastructures against digital attack. The NIPC, in conjunction with sector leads and the ISACs, has the role of identifying critical

vulnerabilities and implementing mitigation plans. However, networked information systems and infrastructure at the end of the 20th Century present easy prey for digital intrusion and disruption. The complexity of operating systems such as Windows NT or Linux and applications such as Microsoft Office or SCADA systems combined with the speed of development and new product releases results in foundational pieces of the information infrastructure that have numerous security flaws. These flaws are discovered and disseminated at a rapid pace by the hacker community. As with intrusion detection systems, defensive tools such as firewalls, virus checkers, and network analyzers usually lag development of new attack techniques. Cyberterrorists are among the spectrum of adversaries who can exploit this basic weakness.

The process presently used by many government organizations involves instituting notification and tracking systems to ensure owner/operators of information infrastructures fix known vulnerabilities and update virus defenses to make digital intrusion and disruption more difficult for cyberterrorists and others. For example, the Department of Defense has instituted an Information Assurance Vulnerability Alert system that requires all DoD organizations to patch certain identified vulnerabilities and report compliance within specified timeframes.[71] However, this approach constitutes a rearguard action whose prospects for success are limited. Its success relies heavily on reacting to vulnerabilities after their weakness has already been demonstrated. More fundamentally, the "patching" process means those defending critical US information infrastructures must discover vulnerabilities, notify users, and track the implementation of fixes throughout a extremely diverse infrastructure comprised of and operated by thousands of organizations using thousands of different products implemented and modified by hundreds of thousands of individuals. So far, the procedures and resources employed to reduce infrastructure vulnerabilities to digital attack fall far short of denying access to potential cyberterrorists.

An alternative approach would involve ensuring that key systems and infrastructures were built to make digital attack difficult from the beginning of

system concept and design. Such an approach would help mitigate a wide range of threats including cyberterrorism but also address concerns ranging from unintentional problems to cybercrime to information warfare. Yet, US government plans as articulated in PDD-63 and other directives show little desire to pursue such an approach. Huge difficulty faces implementation of a national cyberdefense strategy based on migrating to more stout digital foundations. Fundamentally, the government would have to ensure that owner/operators of key systems and infrastructures employed more secure products. Yet, the forces of technological innovation and competition in the information technology industry have forced commercial producers to move firmly in the direction of deploying products as quickly as possible with a minimum of security and other testing. The booming US economy increasingly relies on this sector as a source of fundamental strength. With the exception of encryption policy, the Clinton Administration avoided any significant moves to interfere with the telecommunications and information technologies industries under the guise of national security.[72] This choice means that the threat from digital attacks will remain significant for the indefinite future.

The US has proactively begun dealing with cyberterrorism as a part of national security. Given that dramatic events have yet to occur to prompt action, such efforts should be lauded. However, while policy directives establish authorities and organizations to provide capabilities to counter cyberterrorism, the US is a long way from having effective defenses against the potential threat. Efforts throughout government and the private sector vary greatly in depth and focus. Human and financial resources are lacking everywhere. Technological and economic considerations limit the government's ability to protect our information systems and infrastructures. The nature of US society and protection of civil liberties also present difficulties for those responsible for protecting US in national security in cyberspace.

Policy Options

Improving US capabilities to deal with cyberterrorism will intertwine with a number of other efforts related to information warfare, critical infrastructure protection, and countering computer crime. This section lays out recommendations designed to make cyberterrorism more difficult and dangerous for perpetrators.

US strategy must include efforts to make information systems and infrastructures more robust. The first step in this process is to improve the basic understanding of the technological underpinnings and operational characteristics of our informational centers of gravity. The US government or private sector organizations can not afford to provide robust protection to any and all information resources. Defenders must catalogue key assets and prioritize the deployment of available resources. Such an undertaking will require significant resource investment in organizations such as the NIPC, by government agencies responsible for specific infrastructure sectors, and in the private sector ISACs to create and sustain knowledge of what ought to be protected and how to most effectively accomplish this task. This type of investment would not only serve to counter cyberterrorism but would improve US defensive information warfare and critical infrastructure protection programs at the same time. The US should incorporate lessons from preparing for and responding to Y2K events.

Additionally, identifying key assets and how to effectively protect them must extend beyond the critical infrastructures identified in PDD-63. Most importantly, the US government must find ways to motivate information technology producers to raise the priority of system reliability and security in the production and fielding of new products. Legislative and policy approaches must consider both carrots and sticks. Innovative ideas might include providing the private sector tax breaks for improving protection in key technologies or legislation that establishes liability for losses due to digital intrusions and disruption if companies do not meet proscribed security standards.[73] These efforts would involve economic and social tradeoffs that require thorough evaluation. Yet, despite obstacles, proactively limiting the opportunities

presented to terrorists and other digital attackers by building strong information infrastructures will leverage limited resources much more effectively than trying to patch the holes after systems are in place.

The second set of policy initiatives to address cyberterrorism should focus on steps to make it more dangerous for its perpetrators. Cyberterrorism offers opportunities for attackers to remain anonymous or at least unlocated. The US must improve national security, intelligence, counterintelligence, and law enforcement capabilities to track and identify cyberattackers. To achieve this goal, the US must first improve the exchange of information and cooperation across these communities. The NIPC was created to accomplish this task, but long-standing differences in organizational orientations and cultures must be surmounted. Providing these communities with adequate technological tools, organizational capabilities to fuse information, and skilled people to accomplish the mission will prove costly. While discussions of cyberdefense tend to focus on the technological, more difficult will be justifying the resources necessary to recruit and retain sufficient skilled personnel. The defense, intelligence, and law enforcement communities are losing personnel with computer and information security expertise as fast or faster than they can be trained. Establishing effective analytical methodologies for tracking and hunting down cyberterrorists also requires more attention. Finally, the legal context for US government intelligence and law enforcement efforts intended to combat cyberterrorism and other malicious activity requires examination for possible modification. Initiatives could include enabling the courts to issue a single warrant for law enforcement agencies tracking suspects through multiple locations in cyberspace. Cyberterrorists fearful of rapid identification and response by the US government may well have to modify their tactics and strategies substantially.

Finally, the US government must implement a more proactive education and public awareness strategy. At a minimum, such a strategy must stress awareness of individual and organizational responsibilities and liabilities associated with conducting business, recreation, or other activities in

cyberspace. Through the PDD-63 system of organizations, the government needs to establish and promulgate best practices for information system and infrastructure security. Going farther, the Federal government should implement a plan to limit confusion and hype in the event of cyberterrorist attacks. The government can potentially play a key role in identifying and limiting the impact of hoaxes. The most important task of the government at all levels if a cyberterrorist adversary was to wage a sustained campaign of disruption might simply be to provide accurate information about events and responses. In our open society, the US will continue to live with risks from cyberterrorism. The government role must focus on effectively mitigating these risks with the least impact on society as possible.

Conclusion

Much of the current hype about cyberterrorism is built on fear of the unknown. We need to move beyond simple speculation to more structured analysis of the threat and appropriate US responses. We do have sufficient reasons to believe cyberterrorism will become a more significant national security concern. The means are available but employing digital attacks to achieve specific terrorist objectives faces multiple obstacles. Within the US government, the challenge presented by the threat has received increasing attention. Plans have been formulated to address cyberterrorism as a part of the national critical infrastructure protection effort. Yet, these efforts are hampered by the narrow scope of defense efforts and inadequate resources. Developing robust defenses will continue to prove difficult. The most effective approaches to protect against cyberterrorism through establishing secure information systems and infrastructures must contend with technological and economic imperatives at the end of the 20th Century that cut in other directions. Improving the ability to track attackers involves issues of civil liberties and the role of government that require extensive public debate. Most clearly, US efforts to mitigate cyberterrorism will have to advance incrementally on a combination of fronts. We have no silver bullets for combating cyberterrorism. Rather, our nation must remain alert, learn, and invest wisely.

[1] The possibility of digital warfare and terrorism became a widespread concern in the early 1990s largely as a result of reports such as National Research Council, Computers at Risk: Safe Computing in the Information Age (Washington, DC: National Academy Press, 1991) and books such as Alvin Toffler and Heidi Toffler, War and Anti-War: Survival at the Dawn of the 21st Century (Boston: Little, Brown and Company, 1993).

[2] Quoted in Michael Evans, "War Planners Warn of Digital Armageddon" *London Times*, 20 November 1999.

[3] Walter Laquer, "Post Modern Terrorism" *Foreign Affairs* Vol. 75, No. 5 (September-October 1996), 35

[4] John Arquilla, David Ronfeldt and Michelle Zaninni, "Networks, Netwar and Information Age Terrorism" in *Countering the New Terrorism* (Washington DC: RAND Corporation, 1998), 71.

[5] See Bruce Hoffman and Caleb Carr, "Terrorism: Who is Fighting Whom?" *World Policy Journal*, Vol. 14, No.1 (Spring 1997), 97-104.

[6] This definition is based on that provided by Ian O. Lesser, "Countering the New Terrorism: Implications for Strategy" in *Countering the New Terrorism* (Washington DC: RAND Corporation, 1998), 85.

[7] As of the end of 1999, there are no publicly known examples of purposeful digital attacks disrupting train services or stock markets. However, computer systems failures in Washington DC disrupted early morning Metro service for a period of hours on 20 September 1999. The different US financial markets have shut down at times for short periods due to loss of necessary computer and information services. Reasons for these shut downs vary from backhoes cutting fiber-optic cables in New Jersey to floods in Chicago.

[8] On the possibility of use of use of weapons of mass destruction by terrorists, see Aston Carter, John Deutch and Phillip Zelikow, "Countering Catastrophic Terrorism" *Foreign Affairs* 77, No. 6 (November/December 1998): 80-94; and Richard Falkenrath, Robert D. Neuman and Bradley Thayer, Chapter 3 "The Threat of Nuclear, Biological, or Chemical Attack by Non-State Actors" in *America's Achilles' Heel* (Cambridge MA: MIT Press, 1998), 167-216.

[9] This perspective is exemplified by the annual State Department Report, *Patterns of Global Terrorism*.

[10] Robert Kaplan "The Coming Anarchy," *Atlantic Monthly* (February 1994), 44-76; and Martin Van Creveld, "What War is Fought For" *The Transformation of War* (New York: The Free Press, 1991), 124-156.

[11] Walter Laquer, *The New Terrorism: Fanaticism and the Arms of Mass Destruction* (Oxford: Oxford University Press, 1999)

[12] Caleb Carr, "Terrorism as Warfare" *World Policy Journal* 13, No. 4 (Winter 1996-1997): 1-12.

[13] On the general concept of netwar, see John Arquilla and David Ronfeldt, *The Advent of Netwar* (Washington DC: RAND Corporation, 1996). As applied to terrorism, see Arquilla, et al, "Networks, Netwar and Information Age Terrorism."

[14] My analysis of the pros and cons of such an approach are fully elaborated in the forthcoming *Strategic Warfare in Cyberspace* (Cambridge MA: MIT Press, 2000).

[15] Clifford Stoll, *The Cuckoo's Egg* (New York: Simon & Schuster, Inc., 1989) contains an extensive description of the activities, discovery, and eventually apprehension of the hackers involved in this incident.

[16] General Accounting Office, *Computer Security: Hackers Penetrate DOD Computer Systems* (Washington, DC: GAO/T-IMTEC-92-5), 20 November 1991.

[17] See for example, Winn Schwartau, *Cyber Terrorism: Protecting Your Personal Security in the Electronic Age* (New York: Thunder Mouth Press, 1996), especially on pp. 543-544.

[18] This challenge is discussed in Andrew Rathmell, Richard Overill, Lorenzo Valeri and John Gearson, "The IW Threat from Sub-State Groups" in *Proceedings of the Third International Symposium on Command and Control Research and Technology* (Washington, DC: National Defense University, June 1997), 170.

[19] See *Cybercrime, Cyberterrorism and Cyberwarfare: Averting an Electronic Waterloo* (Washington DC: The Center for Strategic and International Studies, December 1998).

[20] Bruce Sterling, *The Hacker Crackdown: Law and Order on the Electronic Frontier* (New York: Bantam Books, 1992), 41-145 provides a lucid description of the hacker culture. Also see Dorothy E. Denning, *Information Warfare and Security* (Reading MA: Addison-Wesley, 1999), 46-50, for a concise summary of empirical studies on hacker motivations.

[21] See Michelle Satalla and Joshua Quittner, *Masters of Deception: The Gang That Ruled Cyberspace* (New York: Harper Collins Publishing, 1995) for descriptions of such activities.

[22] See Nicholas Chantler, "Profile of a Computer Hacker," available at http://www.infowar.com.

[23] See information at www.2600.com/home.html.

[24] "Call in the Goon Squad" C/NET Dispatches, 18 January 1999, available at hongkong1.cnet.com/Briefs/ Dispatches/China/990118/ss02.html.

[25] Associate Press release, "Chinese Cyber Battle: Hackers Put Taiwanese Symbols on Internet Sites" 12 August 1999, available at www.freedomforum.org/international/1999/8/12tapei.asp.

[26] See Jessica Stern, *The Ultimate Terrorists* (Cambridge MA: Harvard University Press, 1999), 74-75. Rathmell, et al, 176.

[27] Denning, 160.

[28] US Congress, Senate, Committee on Governmental Affairs, Testimony of Lopht Heavy Industries on Computer Security, 106th Congress, 2nd Session, 19 May 1998.

[29] See previously cited 2600 web site address.

[30] As examples of such studies see National Research Council, *Computers at Risk*; Defense Science Board Task Force, *Information Warfare—Defense* (Washington DC: Department of Defense, November 1996); President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (Washington DC: President's Commission on Critical Infrastructure Protection, October 1997); and Statement of Michael A. Vatis, Director, National Infrastructure Protection Center "NIPC Cyber Threat Assessment" to US Senate, Judiciary Committee, Subcommittee on Technology and Terrorism, 6 October 1999.

[31] This quote was provided in Captain (USN) Richard P. O'Neill's presentation at an Institute for Foreign Policy Analysis conference on "War in the Information Age," Cambridge, MA, 15 November 1995.

[32] Anne W. Branscomb, *Rogue Computer Programs—Viruses, Worms Trojan Horses and Time Bombs: Pranks, Prowess, Protection or Prosecution* (Cambridge MA: Harvard University, Program on Information Resources Policy, I-89-3, September 1989), 1-5.

[33] A good analysis is provided by Neil Winton, "Y2K Seen As Possible Cover for Cyberwars" Reuters report on WWW at http://www.zdnet.com/intweek/stories/news/, posted 8 October 1999.

[34] Sterling, *The Hacker Crackdown*, 1-39.

[35] "Pentagon Beats Back Internet Attack" *Wired News*, 10 September 1998 and George I Seffers, "Hackers Take Offense at Pentagon Defense," *Defense News*, September 1998, 1.

[36] Information on this incident and other virus hoaxes can be found on the Internet at the Department of Energy Computer Incident Advisory Capability (CIAC) web site, ciac.llnl.gov.

[37] Chairman of the Joint Chiefs of Staff Memo CM-510-99, "Information Operations Condition," 10 Mar 99 provided the initial directive guidance regarding the establishment of a DoD INFOCON system.

[38] Winn Schwartau "An Introduction to Information Warfare" in Robert L. Pfaltzgraff, Jr. and Richard P. Shultz Jr., eds. *War in the Information Age: New Challenges for US Security* (London: Brassey's, 1997), 58.

[39] This assertion is made in a number of authoritative studies including 1996 Defense Science Board study, *Information Warfare—Defense*, 2-16, and the PCCIP, *Critical Foundations*, 19. This conclusion is also prevalent in the author's discussions with representatives of Software Engineering Institute's Network Survivability and Security Program and CERT Coordinating Center, the Defense Information Systems Agency's Automated Systems Security Incident Support Team (ASSIST), the Air Force Information Warfare Center.

[40] General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks* (Washington DC: GAO/AMID-96-84, May 1996), 15.

[41] Arquilla, et al, " Networks, Netwar and Information Age Terrorism," 65-66.

[42] Denning, 68.

[43] See Charles Swett, "The Role of the Internet in International Politics" in Robert L. Pfaltzgraff, Jr. and Richard P. Shultz Jr., eds., *War in the Information Age: New Challenges for US Security* (London: Brassey's, 1997), 292-293; and David Ronfeldt, John Arquilla, Graham Fuller and Melissa Fuller, *The Zapatista Social Netwar in Mexico* (Washington DC: Rand Corporation, 1999).

[44] Phil Williams, "Transnational Criminal Organizations and International Security" *Survival*, Vol 36, No. 1 (Spring 1994), 96-113.

[45] CIWARS Intelligence Report, 4 January 1998, vol. 2, no. 1 published by the Centre for Infrastructural Warfare, available on the Internet at WWW site at www.iwars.org, accessed 10 February 1998.

[46] National Research Council, *Computer at Risk*, 7.

[47] History of US efforts to deal with digital warfare and terrorism is discussed in depth in Chapter Five of my *Strategic Warfare in Cyberspace*.

[48] *Critical Foundations*, 2.

[49] See Office of Science and Technology Policy, *Cybernation: The American Infrastructure in the Information Age* (Washington, DC: The White House, April 1997) for an in-depth analysis of the significance of system complexity related to critical infrastructure protection.

[50] "Activist Hackers Target On-Line Toy Company," *Financial Times*, 19 December 1999.

[51] Richard Behar, "Who's Reading Your E-Mail," *Fortune* (3 February 1997): 64.

[52] Denise Shelton, "Banks Appease On-Line Terrorists" at news.cnet.com, posted 3 June 1996.

[53] The Toxyn hacker group published a call for attacks against Indonesian government sites on their web site at toxyn.pt.eu.org beginning in October 1997. The hacker magazine 2600 posted an example of a modified web page at their site at www.2600.com/east_timor/after.html.

[54] John Markoff, "Airports Told of Flaw in Security System" *New York Times*, 8 February 1998.

[55] See extensive discussion in Fredrick B. Cohen, *Protection and Security on the Information Highway* (New York: John Wiley & Sons, 1995), 33-78.

[56] "Fired Programmer Zaps Old Firm," on the Internet at biz.yahoo.com/upi/98/02/17/general _state_and_regional_news/nyzap_1.htm, accessed 10 March 1998.

[57] Computer Security Institute/Federal Bureau of Investigation, *Computer Crime and Security Survey* (San Francisco: Computer Security Institute, 1999), 4.

[58] Rathmell, 174-5.

[59] Denning, 69.

[60] Statement of Michael Vatis to Senate Judiciary Committee, 6 October 1999.

[61] William Church, *CIWARS Intelligence Report*, 10 May 1998.

[62] The history of US efforts to develop a national response to the threat of digital attacks is detailed in Chapter Five of this author's forthcoming *Strategic Warfare in Cyberspace*.

[63] This information was provided by the National Coordinator for Security, Infrastructure and Counterterrorism, Richard Clarke, at the "Preparing for Cyberwar" Conference, Arlington VA, 5 October 1999.

[64] National Infrastructure Protection Center Fact Sheet, 1999.

[65] The problems confronted by the US government in keeping skilled computer security personnel are illuminated by an article by Elizabeth Shogren, "U.S. Tries to Plug Computer Worker Drain," *Los Angeles Times*, 23 November 1999, 1.

[66] For descriptions of the incident, see Bradley Graham, "11 US Military Computer Systems Breached This Month," *Washington Post*, 26 February 1998, A01; James Glave, "DOD-Cracking Team Used Common Bug," on *Wired Internet* at www.wired.com, accessed 10 May 1998; and James Glave, "Pentagon Hacker Speaks Out," on *Wired Internet* at www.wired.com, accessed 10 May 1998.

[67] See Declan McCullagh, "Surveillance Network Draws Fire" from Wired News Online, 29 July 1999 at www.wired.com/news/news/politics/story/20994.html.

[68] Software Engineering Institute, *Detecting Signs of Intrusion* (Pittsburgh PA: Carnegie Mellon University, August 1997).

[69] See Office of the Staff Judge Advocate, AF Office of Special Investigations, "Computer Crime Investigator's Handbook" (Andrews AFB MD: AF Office of Special Investigations, May 1999) for detailed explanation of these constraints.

[70] This case is strongly stated in the Government Accounting Office study, *Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences* (Washington DC: GAO/AIMD-00-01, 1999). The US Air

Force and the National Research Council have instituted a joint effort to conduct a study along these lines.

[71] Specifics on the IAVA system are provided by Lt. Beth A Evans, Technical Analysis Division Chief, DoD CERT, "DoD's IAVA Process" *IAnewsletter* 3, No. 1 (Summer 1999): 8-9.

[72] A detailed analysis of this tension is provided in Chapter 5 of *Strategic Warfare in Cyberspace*. The debates within the US over encryption policy are fully addressed in Susan Landau and Whitfield Diffie, *Privacy on the Line: The Politics of Wire Tapping and Encryption*, (Cambridge MA: MIT Press, 1998).

[73] An analysis of such approaches in provided in Stephen J. Lusiak, *Public and Private Roles in the Protection of Critical Information-Dependent Infrastructures* (Palo Alto, CA: Stanford University, Center for International Security and Arms Control, March 1997).

Chapter Six

Domestic Preemption

Robert M. Blitzer

This chapter's focus is the preemption of acts of Domestic Terrorism (DT). The last fifteen years, from a historical perspective, have recorded a substantial and devastating number of "mass casualty" terrorist attacks both here and abroad. This pattern of activity will not change appreciably over the next ten to fifteen years because the United States is and will remain the foremost military power on the globe. With that basic thought in mind consider the hypothesis that terrorist adversaries, whether they are directed by forces at home or by forces abroad, will find ways to punish the United States through various forms of violent acts. Such acts will include both conventional and non-conventional attacks that cause maximum casualties with minimum risk.

While there is no standardized definition of terrorism, the Federal Bureau of Investigation (FBI), "defines terrorism as, the unlawful use of force or violence against persons or property to intimidate or coerce a Government, the civilian population, or any segment thereof, in furtherance of political or social objectives." Beyond this definition the FBI further breaks terrorism into two distinct categories. They are Domestic Terrorism (DT) and International Terrorism (IT).

- Domestic terrorism involves groups or individuals who are based and operate entirely within the United States and Puerto Rico without foreign direction and whose acts are directed at elements of the US Government or population.

- International terrorism is the unlawful use of force or violence committed by a group or individual, who has some connection to a foreign power or whose activities transcend national boundaries, against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

The information contained in this chapter falls mainly under the DT definition and should be considered by the reader in that light. Thus, the above DT definition frames the discussion as we consider the topic of preemption of terrorist operations. Preemption is one of the most difficult aspects of countering terrorism. It is particularly difficult when dealing with domestic groups or individuals that are almost always US citizens.

From 1993 through 1998 there were fourteen acts of domestic terrorism recorded within the United States. During this same time period twenty-six acts of domestic terrorism were preempted through aggressive and careful law enforcement actions. This nearly two-to-one ratio may seem astounding to some, however within law enforcement circles these statistics are well known. At the end of 1998 there were some eighteen FBI Joint Terrorism Task Forces (JTTF) spread strategically around the country. The JTTFs are staffed by members of the local, State, and Federal law enforcement family and are financially supported by the Department of Justice, through the FBI. Many of these task forces have been in place for over ten years and all have contributed to countering the domestic terrorism threat. Without question preempting or preventing acts of terrorism is the highest of priority within the United States counterterrorism community.

Four investigations are highlighted below to illustrate for the reader the "high profile" dangers and difficulties that arise as law enforcement engages in terrorist preventions:

- In late 1995 and early 1996 the FBI, working with State and local authorities, initiated an investigation of

an organization known as the Freemen. This organization had engaged in extensive use of white-collar criminal actions over the course of many months. The Freeman considered themselves as sovereign citizens who filed illegal liens and threatened to arrest several local and Federal officials. An FBI undercover operation was begun for the purpose of developing evidence against the group. An Agent posing as a follower of the Freeman successfully penetrated the group. Based upon his investigation and other law enforcement activity the leaders of the Freeman were arrested without incident on March 25, 1996. Following these arrests several other members of the Freeman barricaded themselves within a ranch compound near Brusett, Montana. An 81-day standoff ensued than ended peacefully with the surrender of some 16 people on June 13, 1996. Although the Freemen had not engaged in serious violent behavior, their surrender ended what was viewed by many in the local community as a reign of terror. Several convictions were obtained in this case.

- The West Virginia Mountaineer Militia (TMM), a right-wing paramilitary organization located in north central West Virginia, came to the attention of the FBI in early 1996. Critical information about the group and its intentions was developed by a confidential source. Based upon source information, the FBI developed an undercover operation to penetrate and develop evidence against the group. Based upon the undercover Agent's activity one of the leaders of the TMM paid $50,000 for a package of photographs of the FBI's Criminal Justice Information Services facility in Clarksburg, West Virginia. There had been a number of discussions about placing explosive charges in critical locations at the facility in order to cripple it. After the payment was made several conspirators were quickly taken into custody. All have been convicted of their crimes.

- In early February, 1998, a white supremacist group calling themselves The New Order (TNO) planned to rob an armored car, kill a prominent civil rights attorney, poison the water supply of a large city, and conduct a wave of murders and bombings for their cause. After an intensive FBI-led investigation of their activities, several members of the group were arrested. "Searches of their residences revealed explosive power, bomb-making materials, firearms, hand grenades and a pipe-bomb."

- Two members of the Republic of Texas were arrested in July 1998 after being charged Federally with threatening to use a Weapon of Mass Destruction. The Republic of Texas members had plotted to construct a device that would deploy lethal biological substances. The devices would be used to infect selected government officials. After obtaining sufficient probable cause, an interagency law enforcement team arrested both men without incident. Both men were found guilty in Federal court in late 1998.

Preventing terrorists from conducting a violent operation is a delicate and sometimes frustrating endeavor. The FBI, and FBI-led JTTFs, are required to conduct investigations within the Attorney General Guidelines on General Crimes, Racketeering enterprises, and Domestic Security/Terrorism Investigations established in 1976 by then Attorney General Levi. These Guidelines have been updated several times since 1976; however, they remain essentially the same.

The Guidelines were developed in order to protect the rights of all US citizens. Additionally, they serve to provide a way for law enforcement to act when domestic terrorists plan to attack our nation. Pursuant to the Guidelines there must be sufficient criminal predication present before investigators can begin to collect information relating to the activities of persons who may be engaging in or preparing for acts of domestic terrorism. Rhetoric alone will not trigger an investigative response by law enforcement unless other information is provided that reasonably indicates that criminal activity is being conducted or is about to be conducted. That is the fine line that various law enforcement agencies must walk when dealing with potential domestic terrorists.

Overall the Guidelines allow for the collection of criminal intelligence information against United States citizens when two or more individuals are preparing for or engaged in a domestic terrorism attack in violation of state or Federal laws. Through this mechanism organizational, financial, structural and criminal activity of the organization can be developed and acted upon. Once there is sufficient predication to initiate a domestic

terrorism investigation, standard investigative techniques including, but not limited to, background checks, physical and electronic surveillance, development of human sources, and undercover operations can be employed with appropriate administrative and judicial authorities.

The bombing of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma on April 19, 1995 was of major historical significance in terms of domestic terrorist actions within this nation. Not only did it awaken the country as a whole to the fact that our own citizens could act in such a horrific manner, but law enforcement was caught off-guard, stunned, and deeply affected by this attack. The impact of this bombing served to educate our citizens about the potential magnitude of future attacks, and it provided law enforcement the realization that no one agency could "go it alone" in terms of managing the crisis and consequences of such a disaster. Like the bombing of the World Trade Center in 1993, fire, emergency services, medical, and many other organizations were called into service.

We have to do better a better job at preventing this kind of attack from ever happening again. While the JTTFs have done much to provide a mechanism for prevention, they do not cover the entire country. We remain vulnerable, particularly to the "loners," the one or two persons that have the capability to mount a major bombing or other kind of terrorist operation.

After the Oklahoma City bombing Attorney General Janet Reno and FBI Director Louis Freeh conducted an intensive review of the overall domestic and international terrorism threat within our borders. There was a clear recognition within both the Executive and Legislative branches of the government that more needed to be done to counter the increasing threats we were facing as a nation.

Subsequent to the above review Director Freeh established the FBI’s Counterterrorism Center (CTC) at FBI Headquarters (FBIHQ). Further, he asked the Congress to "double the shoe leather" with respect to the number of FBI Field Agents needed to counter this threat. The FBI’s CTC included an infusion of well-educated analysts whose mission was to better support both FBIHQ and FBI field operations. Their skills have been put to excellent use over the past several years and they have proven their worth over and over again. With an increase of both FBI Agents and analysts post-1995, the FBI has had an increase of preventions. These preventions, in the writer’s opinion, are directly attributable to the actions taken by Attorney General Reno and Director Freeh in the closing months of 1995.

From 1996 until the end of 1998 the writer served as Chief of the Domestic Terrorism/Counterterrorism Planning Section, National Security Division, at FBIHQ. It was during that time that the FBI began to enter into a new era in terms of its ever-expanding Counterterrorism mandate. Field investigators, ever mindful of the Oklahoma City bombing and the challenging nature of Counterterrorism investigations, began to develop more and more expertise in both domestic and international terrorism matters. At the same time new threats, the threats of the new century, were beginning to emerge.

As we considered the future we looked to the past and tried to learn from history. In 1986, then Vice President George Bush issued a report on terrorism. Within this document, for the first time, there was a discussion of the potential for attacks on our critical infrastructure as well as attacks on our population using unconventional weapons of mass destruction. Until that time there had been little thought about the kinds of future world threats the Counterterrorism community might face in the years to come. The report was prophetic in many ways. Beginning in 1988-1989 efforts were begun in a small way to come to terms with attacks against the critical infrastructure and unconventional weapons.

> Infrastructure is the system of interdependent networks which is made up of identifiable industries and institutions that provide a continual flow of goods and services essential to the security and welfare of this country. The critical infrastructures include electrical power, gas and oil, transportation, telecommunications banking and finance, continuity of government, water supply systems, and emergency services.

What started as a small program to protect the physical infrastructure of the nation has emerged now as an expanding interagency program to help prevent attacks by terrorists at home. Today a large entity within the FBI called the National Infrastructure Protection Center (NIPC) has been established and funded by the Congress. With the emergence of the Internet and the technology boom of the past few years much of the Center's business is focused on cyber terrorism and cyber crime.

On March 10, 2000 Michael A. Vatis, Director, NIPC, appeared before the Senate Armed Service Committee, Subcommittee on Emerging Threats and Capabilities. Mr. Vatis testified that today we are faced with a broad spectrum of threats against the information technology portion of our critical infrastructure. The major sources of these threats are: 1) Insiders—disgruntled former employees of companies; 2) Hackers—persons who attack networks mostly for the thrill of it; 3) Virus Transmitters—people who insert computer viruses into systems; 4) Criminal Groups—persons and groups who use technology to steal and exploit information from various sources; 5) Terrorists—who for some time have used the Internet to communicate, and for other related purposes; 6) Foreign Intelligence Services—who use cyber tools to collect intelligence against both friends and foes; and 7) Information Warfare—foreign militaries who are devising ways to use information technology to attack our critical infrastructures in time of war.

The above testimony certainly is a look into the future, as we now battle a new form of terrorism. The ability to prevent these kinds of attacks has not been refined, and presently law enforcement and the intelligence community are developing the tools and technology that will be needed in this century to counter this new area of threat. This demands new organizations, interagency cooperation, and cooperation from private corporations and the public at large. Perhaps the most interesting part of this new information-driven Internet world is that after all is said and done, the investigator is left with following a high-tech trail back to identify the perpetrator. Investigations will still involve a lot of traditional work in the field. However, with the advent of cyber attacks against our critical infrastructure, the stakes from an economic, social, and military standpoint are greater than ever. Thus, the issue of preventing attacks before they happen, and/or mitigating an attack, looms larger than ever for the law enforcement and intelligence community.

The challenges ahead will require support from the Executive and Legislative Branches of Government. It is critical that the American people not be fooled by a booming economy. Enemies remain with new tools of terror.

Chapter Seven

Combating International Terrorism

David Tucker

The Terrorist Threat

The American way of war relies on technology to generate overwhelming force to defeat our enemies while limiting casualties to as great a degree as possible. Derived from our founding principles and made possible as a practical matter by our historical and geographical isolation, it is a way of war that accepts and encourages a sharp distinction between diplomacy and force and civilians and soldiers and has traditionally focused on military victory at the expense of political consequences. The NATO campaign against Serbia in the Spring of 1999 epitomized this way of war. Its characteristics were again evident as NATO policed up the battlefield. Drawing on their experience in Northern Ireland, the British patrolled on foot aggressively in their area of responsibility in order to suppress arson and protect those Serbs who remained, while the Americans in their sector were using the otherwise unused Apache helicopter and its technologically advanced night vision capabilities to spot arsonists as they set fire to buildings and collect evidence against them to be used in court.

The American way of war, which is one way of understanding the necessary and complex relationship between politics and force, bodes ill for American efforts to deal with terrorism, which rests on an altogether different understanding of this relationship. The United States separates politics and violence as much as possible, remaining deeply suspicious of their mixing despite its own violent revolutionary origins, and attempts to make every use of force in politics a criminal matter. Terrorism deliberately combines politics and violence on grounds similar to those that justified the American Revolution and defy simple criminalization. As part of its effort to subdue force or power in politics, the United States operates with a government of divided and competing powers, which makes coordinating government efforts against terrorists difficult, and under legal restraints that limit the effective use of its power. Even the most bureaucratic terrorist organizations are more nimble than the U.S. government and, as challengers of the legal order, not bound by the same restraints. With their technological might, U.S. Armed Forces want to engage an enemy’s forces decisively and destroy them. Terrorists possess no forces to engage or land to take, as they work effectively with the simple technologies of the gun or bomb. Compared with the terrorists it confronts, the United States appears clumsy, constrained, uneasy in the presence of its own revolutionary principles, and unable to bring to bear its preferred form of violence.

America’s disadvantages when confronting terrorism—and the irrelevance of what it has learned about fighting terrorism over the past 25 years—seem even greater with the advent of the so-called new terrorism. This terrorism is reputedly distinguished from the old by a new structure, a new kind of personnel, and a new attitude toward violence. The new structure is a network, the new personnel are amateurs, and the new attitude an increased willingness to cause mass casualties, perhaps by using chemical, biological or nuclear weapons. Taken together, network organization and amateur participation suggest that the "new terrorists" no longer need state sponsorship as much as their predecessors did to carry out their attacks. Before deciding how disadvantageous our position or irrelevant our experience in the face of this new terrorism, we should assess the claims made about it.

The New Terrorism?

Terrorists are able and willing to develop network forms of organization for the same reason that businesses are. The information revolution allows organizations to push functions outside a controlling hierarchical structure. Organizations can thus flatten out and approach a network form, a group of more or less autonomous, dispersed entities, linked by advanced communications. Motivating or compelling the move from hierarchy to network are the advantages that an organization acquires as it transforms itself. It becomes more flexible, adaptive and resilient because each of its units senses and reacts on its own in loose coordination with the others. This multiplies the opportunities for the organization to learn, making it more flexible and adaptive. The organization becomes more resilient because if one or even several of its constituent entities are destroyed, the others carry on. A network, unlike a hierarchy, cannot be destroyed through decapitation. By adopting network structures, terrorists increase their advantages over the U.S. government, which appears more and more to be a hierarchical industrial-age dinosaur.

One result or manifestation of this networking is the proliferation of the amateur terrorist and the ad hoc terrorist group. Amateurs come together with the like-minded to conduct a terrorist attack and then disband. They do not receive training or other logistical support from state-sponsors but learn the little they need to know from publications or the world-wide web or perhaps from demobilized soldiers. Because they have no organization or permanent existence, it is difficult to spot such groups and take steps to counteract them. As transitory groups, they have no infrastructure, and do not benefit from a state sponsor’s infrastructure, the sort of assets that U.S. power can place at risk.

The U.S. government’s disadvantages when confronting amateur networked terrorists are all the more sobering because of the apparent increasing willingness of terrorists to inflict mass casualties. Analysts explain this trend by pointing to a number of factors, such as the diffusion of lethal technologies; the erosion of taboos against the use of weapons of mass destruction; the absence of restraint on amateur terrorists who, having no organization or sponsor to protect, see no reason to limit extreme violence that might generate a backlash; and the continuing need of terrorists to find new ways of attracting attention. In addition to these factors, analysts have tended to emphasize the importance of religion. Religiously motivated terrorists are thought more likely to conduct mass casualty attacks because, unlike politically motivated terrorists, they are not constrained by the fear that excessive violence will offend some constituency. Nor, unlike politically motivated terrorists, is their intent to pressure or persuade their opponents. For religious terrorists, the world is divided into "us" and "them," the saved and the damned, and the damned are to be destroyed. This is especially so if the religious impulse takes on a millennial character and the desire for a new order makes plausible the destruction of the old. This has led some to speculate that religiously motivated terrorists might even be willing to use weapons of mass destruction in their attacks, as might others whose purpose is not to intimidate or persuade but rather simply to destroy. Such urges, coupled with the increased availability of more potent weapons, suggests that terrorists arrayed in a network or as a network of networks have apparently become opponents whose ability to dance circles around us is surpassed only by the increased lethality of their punch.

The new terrorists appear to be formidable enemies. But are the disadvantages we labor under with regard to them quite as severe as this brief sketch suggests? For that matter, is the new terrorism new? To answer both of these questions, we may start with the question of network structure. The striking thing about the networked structure of the new terrorism is that it differs little from the structure of the old terrorism. The Palestine Liberation Organization (PLO), for example, was itself an umbrella group, whose constituent parts have had different relations with each other, splintering and adhering and developing different policies and strategies. Furthermore, the PLO was networked, by some reports, with up to 21 different organizations that the PLO had previously trained or supplied with weapons and other logistical support. Marxist or left-wing revolutionary groups also became network-like as ideological differentiation led to structural complexity. Many of these groups, such as the Red Army Faction (RAF),

were, despite the hierarchical connotation of the word "army," not very hierarchical at all. The RAF spawned second and third generations haphazardly and remained more a collection of terrorists than a hierarchical organization. And these collectivities, too, were parts of a larger network, getting support, for example, from Warsaw Pact members and training from Middle Eastern terrorist groups. The role of Osama bin Laden as a wealthy patron of loosely affiliated terrorists connected by a common purpose rather than organizational structure has a precedent in the work of Giangiacomo Feltrinelli in the 1960s and early 1970s. Modern communications may allow a looser form of network now than they did twenty or thirty years ago, but the difference appears to be one of degree, rather than kind. Indeed, in 1983, reflecting on 30 years study of "extralegal violent organizations," and five years experience in the Polish underground during Word War II, one analyst concluded that these organizations possessed a network structure similar to that considered new by other analysts in the late 1990s.

If networks are such powerful tools, and terrorists have been networked for thirty years or more, how has the United States survived this long encounter with them? There are two reasons: despite its hierarchical structure, the U.S. government is itself a network and is networked with other governments; and networks have weaknesses. Of Hizballah it has been said that "the formal structure is highly bureaucratic [but] interactions among members are volatile and do not form rigid lines of control." The very same could be said of the structure of the federal government’s Executive branch, not to mention relations between this branch and its legislative counterpart or those between the federal and state governments. In the Executive branch, no one is in charge except the President and he is too busy. Thus, autonomous agencies pursue their objectives without the benefit of "rigid lines of control." True to its network structure, the U.S. government has shown notable adaptiveness in dealing with terrorism. Until recently without any formal central direction, coordinated only by a committee of equals, its constituent agencies have developed a series of new ways to combat terrorism, from international conventions against highjacking, to a hostage rescue capability, to economic sanctions, to military retaliation, and then renditions, as terrorism changed and old capabilities appeared to lose effectiveness. Moreover, to counter terrorism, this network called the U.S. government linked itself bilaterally and multilaterally in networks with other governments and international organizations.

The survival and successes of the United States in its confrontation with terrorism thus validates the notion that it takes a network to fight a network. But we should not think of such fights as struggles of invincible titans. Networks have weaknesses. Their virtues are, from another perspective, vices. As autonomous units, network members can sense and respond independently, which increases adaptability. At the same time, however, this autonomy diminishes control and coordination. Diminished control and coordination, in turn, can increase the difficulty of accomplishing complex tasks and the likelihood that an ill-judged action will undermine the entire network. Martha Crenshaw, for example, argues that the entire Front for the Liberation of Quebec (FLQ) suffered a serious setback in 1970 when one of its independent cells kidnapped and murdered Pierre Laporte, the Quebec Minister of Labor. Divisions within the PLO network have caused similar problems for Yasir Arafat and the Palestinian cause.

Perhaps even more important than control over tactical and strategic decisions for the success or failure of a terrorist organization is control over communications. As it increases the autonomy of its members, a network structure leads to diminished control over the number and kinds of communications that take place in the network. This increases entry opportunities for those outside the network, including its enemies. This characteristic of network organization imposes a high cost on terrorist groups who adopt such a structure, since communicating is the greatest vulnerability of a clandestine organization. Being part of a network or building one, therefore, will be very risky for terrorists. Ramzi Yousef, the very model of a new terrorist, was undone by a new component of his network who turned him in. Even the more hierarchically structured terrorist groups are likely to be networked with concentric circles of

supporters and then sympathizers, with whom they must communicate. Good tradecraft and encryption can limit the risks of such communication but cannot completely remove them. For any organization with something to hide, an organizational form that diminishes control over communication increases risk. If terrorist networking is looser now than it was in the past, then terrorists are increasing their operational risks. The quick arrests following the embassy bombings in Africa in 1998 resulted from luck but also, apparently, from the fact that the loose, networked structure of bin Laden's organization allowed outsiders a number of different opportunities to gather information about it.

Like the networked terrorism to which it is related, amateur terrorism provides advantages that from another perspective become disadvantages. Amateurs are hard to spot and hard to threaten because they have no organization and infrastructure; but because they have no organization and infrastructure, they have no opportunity to develop counterintelligence or other skills. They are, therefore, easier to penetrate than professionals and liable to make shocking blunders, as the history of the group that bombed the World Trade Center indicates.

Given the weaknesses of amateurs, it may well be to our advantage if terrorists are now more amateurish than they were. But this is unlikely. All terrorists are amateurs when they begin. If their mistakes are not fatal, they may learn and survive long enough to become professionals. If we are seeing amateur terrorists among Islamists, it may be because the international Islamic movement (as opposed to nationalist movements like HAMAS and Hizballah) is relatively young. As the principle of the survival of the proficient operates, we may see the number of amateurs decline. As the pressure brought to bear against these groups increases, we are also likely to see that state sponsorship or support will become more important to them. Indeed, this already seems to be happening to bin Laden. He has found state support beneficial, if not necessary, as have most terrorists.

If the new terrorism is not simply more formidable than the old, it does appear to be more lethal or more likely to cause mass casualties. We can construct what we might call a lethality index by dividing the number of fatalities in any given period by the total number of incidents in the same period. Using this method, the period 1969–1980 has a lethality index of .61, while the recent period 1987–1998 has a lethality index of .73, a 20% increase. Evidence of a tendency toward mass casualties is evident, if we construct an index that combines fatalities and casualties. For 1969-1980, the index is 1.8, while for 1987-1999, the index is 5.2, a 188% increase. A similar picture emerges if we look at five year periods. The fatalities and casualties index for 1969-1973 is 1.02; for 1976-1980, it is 2.6; for 1986-1990, it is 3.04; for 1990-1994, it is 2.02; and for 1995-1999, it is 10.6. The only mitigating factor here is that three events in the period 1995-1999 or .17% of events caused 67% of the casualties. (The three events are Aum Shinrikyo's sarin attack in the Tokyo Subway [1995, 5,500 casualties], the Tamil Tiger truck bombing of the Central Bank in Colombo [1996, 1400 casualties] and the truck bombing of the U.S. Embassy in Nairobi [1998, 5000 casualties]). Still, even if these three events are removed from the calculation, the fatalities and casualties index for this five year period is still 3.7, .66 higher than the period 1986-1990. At best, we could argue that terrorism over the last five years has returned to a plateau of increased lethality and mass casualties first reached ten years before.

Such indexes must be treated with caution. One particularly lethal year can strongly affect statistics for terrorism but a particularly lethal year may not be a trend or even the beginning of a trend in increased lethality. Furthermore, the number of terrorist attacks in a given period "is strongly correlated to wars, major regional crises, and other divisive world events" and so may reflect not underlying trends in terrorism but "fluctuations in inter-state tensions." Finally, this index is not the only way to measure the lethality of terrorism. It is a measure of lethality, nonetheless, and based on this measure, it would be difficult to deny the tendency toward increased lethality or mass casualties.

If we accept that terrorism is more lethal now, must we accept the connection between this increased lethality and religiously motivated terrorism, accepting that such terrorists have a greater willingness to kill indiscriminately and even use weapons of mass destruction? To the extent that terrorists with religious motivations also have political and social agendas—for example, the establishment of an Islamic state—they will labor under the same kinds of constraints that terrorists with political motivations labor under both as they struggle to achieve their political goals and once they have achieved them. This does not mean that a religious group or a political group would never commit mass casualty attacks. It means only that they have reasons not to do so. Even if religiously inspired terrorists do not have political goals, politics will not leave them alone. Whether or not they had political objectives or thought about them, Islamic fundamentalists in Egypt and Algeria were undone in part by the political problems that arose from their extreme violence. Over time, even militant Islamist groups will learn a lesson about the use of extreme violence—there are good reasons to avoid it—or suffer a decline in life expectancy.

It may well be true that religious fanatics are intolerant; and the intolerant may be more ruthless than the tolerant; and the more ruthless more willing to inflict mass casualties. But if this line of reasoning is true, it is just as true of Marxists as it is of Islamists. Yet, no one ever thought it made sense to argue that Marxist terrorists would use weapons of mass destruction just because they were Marxists. To repeat, Marxist as well as Islamist terrorists have political agendas and to that extent reasons to constrain their use of violence. Religiously motivated terrorists may now be involved in most of those incidents that take human life or even in those that in any given year take the most lives, but that is because of the increase in religiously motivated terrorism, not because those with a religious motivation are necessarily more ruthless than other terrorists. In general, the most lethal attacks by religious groups now do not take more lives than those committed in the 1970s and 1980s by nationalist or revolutionary terrorists, who were then the most active terrorists.

Another way to approach this issue is to look at recent examples of mass casualty attacks. Over the past several years, such attacks have been committed by Hizballah; the group associated with Ramzi Yousef; Aum Shinrikyo, the Japanese sect; the Tamil Tigers; Kach, a Jewish extremist group; and terrorists associated with Osama bin Laden. Religiously motivated terrorists figure prominently in this list but all of their attacks, with one clear exception and another possibly, are similar in method (bombing, shooting) and results (over a hundred casualties) to attacks carried out in the past by groups that did not have a religious motivation. Mass casualty attacks and religious motivation are not necessarily connected.

The two events that are not analogous to past terrorist events are the bombing of the World Trade Center by Ramzi Yousef and his colleagues and the attack on the Tokyo subway by Aum Shinrikyo. In the first case, the method employed, a truck bomb, was not new, although the claimed intent—to kill 250,000—set this act apart from others. In the second case, the method (the use of a chemical weapon) and presumed intent (truly mass casualties) were unlike previous terrorist attacks. In the first case, it is not clear whether the unprecedented characteristics of the attack, if true, tell us something about the consequences of religious motivation or only about the peculiar psychology of Ramzi Yousef. In the second case, we are dealing with a kind of religious experience that may in fact encourage mass casualty attacks. Millennial sects like Aum, unlike other religiously motivated groups, may be sufficiently divorced from this world and so intent on another that it makes sense to them to create casualties more massive than any we have seen, and thus to use weapons of mass destruction. This may be the only case in which religious motivation and such terrible weapons go together. Fortunately, in this case, precisely the psychology that makes the use of weapons of mass destruction plausible to such a group—alienation,

paranoia, delusions, inflexible devotion to the rulings of a leader—may make it less capable of the engineering and planning necessary to use them.

More tightly framing the possible association of a religious impulse to violence with weapons of mass destruction should not be understood as a denial that a WMD terrorist attack might occur. The other reasons cited by analysts to explain why such an attack might happen remain valid. In addition, since conventional war has become more lethal, we might suspect that unconventional war will as well. It may be that 1998, the most lethal year for terrorism on record, is the beginning of a long-term trend that will see unconventional means of political violence follow the trail blazed by conventional means. Even if does not, it remains true that the likelihood of WMD use has increased. The increase may not be as great as some suppose. It does not have to be great, however, to be significant.

In sum, the one thing new about the new terrorism is the increased likelihood of the use of WMD. Terrorists have always been networked and, initially, amateurish. They may now be no more lethal than before. Indeed, if bin Laden's organization is different from most other terrorist organizations, it is not because it is amateurish and loosely networked but because its personnel are more professional (or at least experienced—from conflict in Afghanistan and elsewhere) and better organized, not to mention better financed, than many of its predecessors.

The most important point in assessing the threat posed by terrorist groups, however, is not whether they are networked or hierarchical. Since networks and hierarchies have different strengths and weaknesses and are thus suited for different environments and tasks, the most important point is whether terrorists can adapt their structure and strategy to their environment, including the degree and kind of pressure that governments can bring to bear against them. Basque Fatherland and Liberty (ETA), for example, "reorganized itself from a largely decentralized system" to a more centrally controlled one in 1974 "to survive government repression and heavy attrition of membership ranks." Those terrorists that are adaptable in this way are likely to survive the longest, become more professional and, over the long-term, more lethal.

The American Response

Based on this brief survey of the current state of terrorism, we can suggest some general principles that should guide the U.S. government response to international terrorism, as well as some more specific ways to improve that response. We should note first that much of what the United States has done over the past 30 years to combat terrorism remains relevant because the new terrorism is not fundamentally different from the old. Terrorism has been networked and lethal from our first encounter with it. The recent appearance of amateurs is also not unprecedented. States continue to support both traditional, professional groups and their new, more loosely organized colleagues. The increased likelihood of a WMD attack presents new problems, it is true, to which we must adapt, but methods developed over the past 30 years are still useful against this threat, as we shall argue. We can still apply today, therefore, lessons we have learned, or should have learned, during the past three decades.

Perhaps no aspect of our effort to combat terrorism over the past 30 years has received more criticism than the ways we have organized to do it. Much has been written lately about the need to make the interagency community more cohesive and coordinated so that it is better able to respond to terrorism and other post-Cold War threats. All of this writing overlooks the fact that the loosely coordinated interagency process with which we have lived for many years is actually well-suited to our current situation. In the Cold War, a greater emphasis on hierarchy would have been better because decisiveness and crisis response were more important. Today, as far as our national security is concerned, in most

respects, the most important thing is adaptability, since we face a variety of threats but no dominant one and the future is uncertain. Therefore, we should be putting greater emphasis on decentralization and the networked character of the interagency community. In principle, this will increase the chances that in the future we will adapt, as we have in the past, as terrorism changes.

The need to retain the networked character of the interagency process does not mean that efforts to improve coordination, for example, by creating a so-called "terrorism czar," are necessarily bad ideas. Responding to terrorism requires some degree of integration of the heterogeneous skills, principles, and standard operating procedures that make up the U.S. government, and this is something that a network will not do well, if at all. Furthermore, responding to terrorism does require crisis management, which again is typically a strength not of networks but of hierarchical organizations. Responding to terrorism, which requires the ability both to adapt over time and to respond immediately, requires that the U.S. government exploit both the hierarchical and networked character of the interagency process. This will necessitate constantly adjusting the balance between the two organizational aspects of the interagency, something unlikely to occur if we forget that the interagency is a network and call only for clearing up lines of authority and tightening command and control.

One area where the balance among U.S. government agencies may be in danger of slipping is in the roles and responsibilities of the military and law enforcement. Over the past two decades, the FBI has assumed a much more important role in combating terrorism outside the United States than it has had before in this or any other area of criminal activity. Lately, some have been arguing that the U.S. military should become more involved in combating terrorism in the United States. In the former case, this trend has probably gone too far and in the latter, it is about to.

The emphasis on international terrorism as a criminal matter and the resulting decision to use the FBI against it resulted from the coincidence of two separate, uncoordinated developments in the mid-1980s: the State Department’s search for an alternative to previous policies discredited by the Iran-Contra Affair and the Justice Department’s interest in applying its expertise to one of the most important issues facing the Reagan Administration. The result was an extension of the jurisdiction of our terrorism laws beyond our borders and the use of the FBI to arrest terrorists overseas who had broken these laws in order to return them to the United States for trial. This law enforcement approach has now become, along with sanctions, the principal way that the United States responds to terrorism.

The legal approach to international terrorism has produced results. The State Department lists 12 terrorists as having been returned to the United States for trial since 1993. Not only do such proceedings take terrorists out of action, they may well deter others from committing terrorist acts. At a time when state support for terrorism may be indirect or more hidden than it once was, going after individual terrorists through arrest and trial may be one of the few ways that we can put at risk something the terrorists value, namely their freedom, if not their lives. Extending our legal net around the world may also impair the ability of terrorists to operate, as well as deter them from doing so, if it makes it more difficult for them to travel by creating the fear that they will be arrested when they do so.

Despite these benefits, a response to terrorism dominated by law enforcement has its drawbacks. In the first place are its practical limitations. Its success depends on the cooperation of other nations. This may not always be forthcoming. To proceed without it may threaten our relations with countries whose goodwill and cooperation we may need in a host of matters as important as the fight against terrorism. A more important consideration is that the legal process points to individuals, as it did in the case of Pan Am 103, even though they may be acting on behalf of a state. If the individuals are found guilty in this case, what action will we take against Libya and its leader? Will we indict him? Will we reimpose

sanctions? After so much time has passed and we have punished two individuals, what sort of support will such a sanctions regime or any action against Libya receive? The law enforcement response to terrorism does not touch the political and strategic aspects of terrorism that derive from state-sponsorship, which remain critical. Indeed, because the legal response takes precedence over any other response, it crowds out other options and limits our flexibility in responding to the political-military aspects of terrorism.

The legal approach need not have this precedence. In adopting a judicial approach to a foreign policy issue, we raise the bar to the use of force by the state abroad as high as we do at home. At home the bar must be high because the state is so powerful within its own domain. Abroad it is not, and there is no reason, moral or otherwise, why we must restrain force abroad as carefully as we do at home. No other nation has done this, and it is likely that we have done it and can afford to do it only because we are now so powerful in comparison to other states. But when we are no longer, we may regret that we have set a precedent for the powerful to extend the sway of their law over the territory of others.

The limits on the law enforcement response to terrorism suggest not that we give up this response but that we rely on it less reflexively. The FBI is appropriately the lead agency for terrorist acts in the United States but not necessarily for those abroad, whether or not U.S. laws are broken.

As we have extended the authority of our laws and the FBI abroad, we are now contemplating extending the role of the Department of Defense (DoD) at home. The rising threat of terrorist use of weapons of mass destruction has led to calls for DoD's resources and expertise to be integrated into our domestic response to terrorism in some comprehensive and permanent way. The most typical criticism of this idea is that it would violate our traditional separation of civil and military authority embodied, for example, in the Posse Comitatus act. This is an important objection, since the separation of civil and military authority is an essential component of a limited form of government. Some have argued that, in effect, this separation is a luxury we can no longer afford because there has been recently a blurring of military and criminal activities that requires some similar merging of response capabilities on our part. In fact, throughout human history military and criminal enterprise have most often been merged or at least were indistinguishable. Separating them and giving to separate agencies of government the responsibility for dealing with them is one of the triumphs of our way of life. Even assuming that the threat of WMD terrorism in the United States is high and growing, we should only consider diminishing this triumph if there is no other way to deal with this threat. But there is. DoD can transfer the expertise it has to an appropriate non-military agency, such as FEMA, which the Congress can then appropriately fund.

The constitutional issues raised by DoD's involvement in responding to domestic terrorism are not the only reasons to judge such involvement unwise. It could also have adverse consequences for DoD and our national security. Permanent, extensive DoD involvement in domestic matters will distract DoD from its core mission and may make DoD more like domestic, civilian institutions. This will degrade military professionalism, an outcome no one could approve of. Furthermore, if it is known that homeland defense is a core mission for DoD, this could increase the chances of domestic attacks, even with WMD, as a diversionary measure. If DoD must respond to domestic attacks, our enemies will have increased reason to see such attacks as a way to engage DoD's resources and attention far from the foreign theatre that is their principal concern. For constitutional and national security reasons, therefore, it would be best to keep DoD's focus not on the domestic but on the foreign response to terrorism.

Emphasizing the role of DoD in responding to foreign terrorism is not the same as touting the usefulness of military retaliation for terrorist attacks. Such retaliation is not useless but is probably best applied in a very circumspect way. In retrospect, we can see that the raid on Libya in 1986 had a

deterrent effect. Governments that supported terrorism curtailed their support and inhibited terrorist activity in the aftermath of the raid. This resulted, we may surmise, in the lives of an unknown number of Americans being saved. Allies also increased their cooperation with us in response to the raid, again inhibiting state sponsors and their clients. Yet the fact remains that more Americans died from Libyan sponsored terrorism in the years after the raid than before it, even without counting the lives lost on Pan Am 103. This suggests the fundamental problem with responding to terrorism by using military force, whether air strikes or, the new favorite, cruise missiles: we operate under much greater constraint with regard to the use of force than terrorists do and present a much greater number of targets to them than they do to us. Thus, in any violent action-response spiral, we are likely to come out on the loosing end. Although there may be occasions when we should respond to terrorism with conventional military attacks, they are likely to be rare.

If responding to terrorism with the traditional uses of military force seems unwise, the increased likelihood of WMD attacks suggests that unconventional approaches may now be more important. At issue here are not just clandestine raids or acts of sabotage but the overt seizure of ships at sea, for example, that we suspect of carrying WMD or what is necessary to make them. Any such acts should be undertaken only with a careful assessment of the possible risks and benefits associated with it. This is obvious. What is less obvious is that this balancing of risks and benefits must be thought through from the beginning to the end of the acquisition or development cycle. Such assessments are necessary because of the dilemma of counterproliferation: acting early entails great political risk because the threat is not evident; acting later, when the threat is evident, may be impossible or pose extremely high risks to the success of the operation and those who undertake it. Considered at any one moment, the risks may always seem higher than the benefits but considered over time, there may be a point where the balance of risks and benefits allows us to identify an optimum moment to act. Developing an analysis that identifies that moment, particularly with regard to specific programs, and gives decisionmakers enough confidence in it to act upon its recommendations, will require intensive gaming involving an interagency array of civilian and military officials. If this is not done, we are likely to continue with a situation in which our capability to operate successfully exceeds our ability to choose rationally.

Discussing the role of DoD in responding to terrorism leads inevitably it seems to dramatic images, such as U.S. aircraft streaking through the sky or ships being raided on the high seas. Such events, however, will never make up more than a small portion of what we do to combat terrorism. For the most part, we will engage in the less dramatic but demonstrably effective business of using non-military means of force and persuasion. One of these means, economic sanctions, is often criticized as ineffective, but the aptness of the criticism depends on the definition of effectiveness. Economic sanctions are unlikely by themselves to change the behavior of a state. This does not mean they are ineffective. They impose costs on the target country and so detract from its ability to support terrorism or carry on other activities. Combined with diplomatic sanctions, sanctions on travel, arms embargoes and other measures, economic sanctions can create a sense of isolation among and increase pressure on the elites in a target country. Sanctions do typically impose greater costs on the mass of people than on their elites. While this may not lead to popular revolt, increased disaffection will require the target government to devote more attention and resources to internal security, diverting resources from international pursuits, including terrorism. Again, none of this will necessarily mean a quick end to support for terrorism. As the case of Libya shows, however, sanctions can work over time. In many cases, given that the alternative may be less effective (a diplomatic démarche) or more risky (military action), economic sanctions will be the best way to respond to states that support terrorism.

Economic incentives can also be used directly against terrorists, whether they are part of traditional organizations or amateurs. Ramzi Yousef, the World Trade Center bomber, was caught because the U.S.

government's reward program led someone to turn him in. Mir Aimal Kansi, who shot five people, killing two, outside the headquarters of the Central Intelligence Agency, was also arrested with the help of information provided in return for a reward. What happened to Yousef and Kansi can happen to any terrorist. While it may be true that the members of some millennial groups, for example, are cut off from the world and invulnerable to financial inducement, even these groups and their members will have contact with some people outside the group. This is a vulnerability that a reward program can exploit.

More generally, it may be possible to use sanctions and incentives to develop a strategy of "in group" policing, in which a larger religious or ethnic community or a government is induced to control its more radical and violent members. Carrying out such a strategy requires appealing to a moderate element (even if it is only moderate in comparison to the radicals) and creating incentives (threatened punishments or promised rewards) for it to suppress radicals. This is in effect the strategy we are following with regard to the Taliban and its protection of Osama bin Laden. We should look for other opportunities to apply it. It will be difficult to do so for a number of reasons: moderates may not exist, or may be too few or too afraid to do anything; we may not be able to provide sufficient incentives; or the moderates may demand what we should not give. But the U.S. government probably has now a greater array of tools with which to construct such a strategy than any other government on earth.

What we may lack is the flexibility to do it, for such a strategy will most likely require that we make concessions on certain issues that the radicals or terrorists have demanded. Making such concessions will violate a policy that for 25 years has been the bedrock, at least in word, on which the U.S. government's effort to combat terrorism stands, the policy of not making concessions to the demands of terrorists. The argument for this policy is that making concessions rewards terrorists and that any behavior that is rewarded will be repeated. Thus, making concessions, while it may resolve the immediate terrorist incident, will simply encourage more terrorism in the long term.

This argument was probably never as sound as was supposed. As a practical matter, making concessions does not always generate more demands. The arms-for-hostages deal with Iran, for example, did not lead to increased terrorist attacks on or more hostage-taking of Americans. There are many reasons for this and similar instances where concessions or deal making have not encouraged more terrorism, ranging from the psychology of terrorists (they are not always primarily concerned with having demands met, even when they make them) to geopolitics (declining support from a state-sponsor). Less important in the struggle against terrorism than supposed, the policy of no-concessions is also now less relevant. It was first articulated when terrorism was principally a means of contesting for political legitimacy and conceding to terrorists tantamount to granting it to them. Terrorism is now typically either an act of vengeance in which demands and concessions do not figure or part of a foreign policy incentive system, in which making concessions is not so much a question of legitimizing a political movement as conducting negotiations, implicitly or explicitly, with established states. Given its weakness in principle and its irrelevance in practice, we should not be constrained from pursuing more flexible means of dealing with terrorism by an overly rigid adherence to a policy of no concessions.

The increased likelihood that weapons of mass destruction will be used should also make us question the relevance of the no-concessions policy. As Philip Heymann has argued, "concessions may be sensible where the disparity between what is threatened and what is sought is immense. That will occur when the threat is catastrophic and also when the concession sought is trivial." With this principle in mind, especially when attempting to stop the proliferation or use of weapons of mass destruction, but also to combat terrorism more generally, we should not allow scruples about making concessions deter us from seeking opportunities to make "in group" policing and other flexible approaches to terrorism

work. As we do so, we should, as Heymann notes, "keep the ‘account books’ open" so that if our flexibility does not evoke a suitable response, we can "find ways to assure . . . a net loss to the terrorists" and, of course, to their supporters.

In all the measures to combat terrorism that we have so far discussed, intelligence on terrorist groups and their sponsors is critical. We cannot deter their activities or their support if we do not know who they and their supporters are and what they hold dear. We cannot preempt terrorist acts or instances of proliferation if we do not know they are occurring. We cannot disrupt terrorist organizations—degrade their financial infrastructure, curtail their state support, and compromise their personnel—as we did with success on at least one occasion, unless we know in detail who they are and how their organizations are structured and function. This is why over the years, every analysis of our ability to counter terrorism has included a call for improved intelligence. Often such calls focus on the importance of human intelligence because much of what we need to know about terrorism we are unlikely to get through technical means alone. The call for improvement is made so often, however, because it never seems to be heeded. How bad the situation really is no one can say with certainty because we have no sure standard against which to measure the performance of our human intelligence service. Apparently there have been some successes; undoubtedly there have been many failures, since terrorists are often a truly hard target. It seems unlikely, however, that we will see much improvement without a fundamental reform of the CIA’s Directorate of Operations, a reform that would change the character of the organization by restructuring incentives and career paths. Such reforms are rare and take time. There is no sign that such a reform is now underway. There is hope, however, since the FBI, confronted with similar problems, was able to reform itself in the 1970s. In the meantime, we will have to live with the human intelligence capability that we have. This is not necessarily a catastrophic situation because our intelligence capabilities, human and otherwise, are not negligible and, especially when networked with the capabilities of others around the world, can be effective against terrorists.

The difficulties our human intelligence service has with terrorism are not entirely of its own making, of course. In addition to the asymmetry with regard to the use of force, our struggle against terrorism is marked by another, an asymmetry with regard to the availability of information. It is harder for us to learn about the terrorists than it is for them to learn about us. Like the force asymmetry, this intelligence asymmetry derives from the difference between what we are and what the terrorists are. Such asymmetries, important as they are, do not mean that the balance of forces favors the terrorists. By any measure, the creative power of our economy, the resilience of our society, and the essential justness of our way of life give us resources that vastly outstrip those of the terrorists. As long as we have a national security strategy and structure that allow us to adapt, allocate these resources sensibly, and employ our political, diplomatic, military, intelligence and informational instruments so that the asymmetries favor us, we should be able to limit the effect that terrorism has on us, even if a future terrorist attack in the United States takes place with a weapon of mass destruction.

One effect of such an attack will probably be beyond our power to limit, however, because global economic and geopolitical change is working to produce the same result. As conventional war becomes increasingly remote from the experience of the vast majority of Americans and its professional practitioners prepare to fight it at lightning speed far from their homeland, unconventional war threatens to draw nearer to Americans in a particularly virulent form, destroying any last pretense of isolation. In these circumstances, the traditional American way of war may have to change. Since that way of war derives from our principles as well as our previous geographical isolation, what that change will mean for us and the world is unclear. But we should begin thinking about it, just as we should be preparing for the political consequences of a WMD attack in the United States. Indeed, political consequence management, at all levels, is what an effective response to terrorism most requires and what we are least

prepared to do.

SUGGESTED READING

Crenshaw, Martha. "How Terrorism Declines." *Terrorism and Political Violence* 3 (Spring, 1991).

_____. "An Organizational Approach to the Analysis of Political Terrorism." *Orbis* 29 (Fall. 1985).

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

Hoffman, Bruce. *Inside Terrorism*. New York: Columbia University Press, 1998.

Laqueur, Walter. *The Age of Terrorism*. Boston: Little, Brown and Company, 1987.

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

Martin, David C., and John Walcott. *Best Laid Plans, The Inside Story of America's War Against Terrorism*. New York: Harper and Row, 1988.

Tucker, David. *Skirmishes at the End of Empire, the United States and International Terrorism*. Westport, Connecticut: Praeger, 1997.

U.S. Department of State. *Patterns of Global Terrorism, 1998*. Washington, D.C., April, 1999.

Chapter Eight

Antiterrorism via Counterproliferation

James J. Wirtz

Does US counterproliferation policy or the concept of counterproliferation help prevent terrorists from launching chemical, biological, or nuclear attacks? Is there a relationship between US counterproliferation and antiterrorism policies? The answers to these questions are not at all obvious. Counterproliferation and antiterrorism cut across existing conceptual, policy and organizational boundaries. Identifying relationships between antiterrorism and counterproliferation thus represents a research question of immediate theoretical and policy significance, especially since some analysts believe that terrorists might increasingly be willing to arm themselves with nuclear, chemical or biological weapons.

Both officials and theorists treat counterproliferation and antiterrorism as separate issues. Counterproliferation largely deals with the struggle between those militaries or sovereign states that want to acquire, threaten to use, or actually employ chemical, biological, or nuclear weapons to achieve political or military objectives, and those that want to stop them. Antiterrorism is a term generally used to describe the efforts of states against non-state actors (criminal organizations, separatist groups, fanatics, etc.) that intend or try to use violence against civilian targets to achieve political objectives or to create death and destruction for ideological or millenarian reasons. This theoretical and policy compartmentalization is in turn reflected by the division of responsibility for antiterrorism and counterproliferation among competing organizations within the US government. The intelligence community, police agencies, and special operations units are generally concerned with preventing or responding to terrorist attacks against US interests at home or abroad. By contrast, counterproliferation is a Department of Defense (DoD) activity that is intended to eliminate or contain the threat posed by weapons of mass destruction (WMD) primarily to US military forces. Recent efforts to evaluate the WMD threat continue to treat US terrorism and counterproliferation policy as separate topics.

Even though theoretical concepts and bureaucratic preferences can explain why no one has asked how counterproliferation contributes to or detracts from antiterrorism efforts, it is equally clear that no good logical or empirical reason emerges to dismiss the issue out of hand. In their December 1999 report to President Clinton, for example, the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, chaired by James Gilmore (hereafter referred to as the Gilmore report), offered judgments about the nature of the terrorist threat. These judgements were based on the presence of an effective US counterproliferation capability, although Gilmore and his colleagues failed to note specifically the way counterproliferation helped to constrain the terrorist threat. Theory, policy, and organization have blinded us both to the way that US counterproliferation efforts help to deter or prevent chemical, biological, and nuclear terrorism and to the negative interaction between counterproliferation and antiterrorism policies.

Counterproliferation and antiterrorism are related in at least four ways. First, counterproliferation policy has bounded the terrorist threat by cutting supplies to black markets and by reducing the incentives for state sponsorship of WMD terrorism. Second, superior US conventional military capabilities, which are bolstered in several ways by counterproliferation policies, force determined US adversaries to seek asymmetric responses, including terrorism. To the extent that counterproliferation

policies harden US military units and installations to terrorist attack, counterproliferation also might channel terrorists toward civilian targets. Third, US counterproliferation efforts address key allied vulnerabilities to terrorism involving weapons of mass destruction, further bounding the terrorist threat. Fourth, potential policy and budgetary tradeoffs are looming between counterproliferation and a major component of antiterrorism policy, consequence management (the protection of civilian populations from weapons effects following a successful terrorist attack). The chapter explores each of these claims and then concludes by offering some observations about the relationship between counterproliferation and antiterrorism.

Counterproliferation and the Limits of State-Sponsored Terrorism

Current US counterproliferation policy reflects the guidance laid out in the May 1997 Quadrennial Defense Review (QDR), which estimated that chemical or biological weapons were likely to be used in future conflicts. The 1997 QDR called upon the Defense Department to undertake two initiatives in response to this threat estimate. First, the Defense Department was to institutionalize counterproliferation by using the concept as an organizing principle in every facet of military activity. US forces were to prepare to operate in a WMD environment. Second, Defense was instructed to "internationalize" counterproliferation to encourage allies and potential coalition partners to train, equip, and prepare their forces to operate alongside US units in a nuclear, chemical, or biological warfare environment. Counterproliferation is a multifaceted enterprise that embodies DoD efforts to reduce and counter the threat posed by weapons of mass destruction.

Counterproliferation addresses the "supply-side" of the WMD issue by reducing the availability of nuclear, chemical, and biological weapons that might find their way into the hands of terrorists. Arms control and nonproliferation efforts are an important part of counterproliferation because they can be used to constrain, roll back, or even prevent states from acquiring unconventional weapons. The Cooperative Threat Reduction program reduces the latent threat posed by Soviet "legacy" systems. By properly disposing of weapons that are no longer needed, counterproliferation helps keep obsolete munitions and materials from falling into hostile hands. Similarly, US export controls help to reduce the possibility that irresponsible or aggressive groups or states will acquire weapons of mass destruction and associated technologies. International norms against trafficking in dangerous materials or weapons help prevent dual-use technologies from reaching black markets and terrorists.

Counterproliferation also embodies Defense Department efforts to counter existing WMD capabilities by: (1) deterring the use of WMD against US interests by denying adversaries their political or military objectives; (2) defending US and allied forces and populations from missile attack; (3) sustaining offensive and defensive military operations in a WMD environment; and (4) preparing for chemical, biological, or nuclear use against US and allied civilians. By making military forces a less vulnerable target and by guaranteeing that any use or prospective use of WMD will be preempted or met with prompt retaliation, US counterproliferation policy reduces the threat of state-sponsored WMD terrorism. In other words, because counterproliferation helps to insure that US forces can retaliate after military units or civilian targets suffer WMD attack, American policymakers can make credible deterrent threats that discourage state-sponsored terrorism.

Counterproliferation efforts "bound" the terrorist threat by reducing the incentives for state-sponsored WMD terrorism and by limiting the opportunities for states to transfer materials and technologies to non-state actors to construct and use nuclear, chemical, or biological weapons. Counterproliferation is an ex ante and costly indicator (witness the financial and psychological costs of anthrax vaccination alone) of US resolve that bolsters general deterrence. The assumption that US deterrent threats are credible is a

cornerstone of the Gilmore report, which dismisses the prospect of state-sponsored nuclear, chemical, or biological terrorism as extremely unlikely. According to Gilmore, the threat of US conventional preemption—here the 1998 cruise missile attack on the al-Shifa pharmaceutical plant in Khartoum, Sudan comes to mind—or nuclear retaliation in the aftermath of a mass casualty terrorist incident creates enormous disincentives for states to become involved in terrorism. These disincentives apparently are clear even to so-called "rogue states": despite accesses to nuclear, chemical, or biological weapons, no state has put its unconventional arsenal at the disposal of terrorists. The benefits of even a successful state-sponsored terrorist attack against US forces might be short-lived. US forces are preparing to operate effectively in the wake of a WMD attack; terrorism directed against US military units should only prove to be a limited setback to American success on the battlefield. The price for this temporary setback, however, could be severe retaliation once the sponsor of a terrorist attack has been identified.

Deterrent threats strengthened by counterproliferation, however, would be less effective if they were directed at terrorists that lack state sponsors. Independent terrorists probably would expect to avoid symmetrical retaliation. They also might hope to escape discovery. If discovered, they might pose an inappropriate target for retaliation. Indeed, if terrorists embraced a millenarian philosophy or objective, they might even welcome severe retaliation. The objectives of the Heaven’s Gate cult, for example, were literally suicidal.

Terrorism as an Asymmetric Threat

To the extent that counterproliferation policies provide escalation dominance on the battlefield, they help limit conflict to the conventional level of combat, a level where US forces have repeatedly demonstrated their ability to overwhelm adversaries. This escalation dominance also enhances US deterrent threats, which reduce incentives for states to sponsor terrorist activities. But counterproliferation, combined with US dominance of the conventional battlefield, could produce an unwelcome paradox: counterproliferation might increase the likelihood of WMD terrorism by forcing adversaries to find asymmetric responses to US conventional superiority. As David Kay notes in his assessment of the terrorist challenge, "nations will seek courses of action that will allow them operational freedom from US conventional attack or, at least, the ability to inflict significant losses on the United States if it does attempt to frustrate their ambitions and military actions." Terrorism supplies an asymmetric response to US dominance of conventional battle, although likely US adversaries would never want to take credit for a successful terrorist attack.

Because counterproliferation also channels terrorist attacks away from relatively hard military targets, terrorists might find it easier to direct attacks against civilian, transportation, or industrial targets that would have an impact on the course of conventional battle. In other words, counterproliferation channels attacks away from well-prepared military units towards relatively unprepared civilian targets. US forces employ tactics and equipment that reduce their vulnerability to WMD terrorist attacks. US military personnel are equipped with personal and collective protective equipment (e.g., suits, masks and shelters). Units also are equipped with point and standoff chemical and biological agent detectors that can reduce exposure to these hazards by warning of their presence in the environment. Decontamination equipment and medical countermeasures (vaccines and antidotes) also reduce the potential damage that might be inflicted by chemical and biological agents on US forces. US military forces are more accessible to terrorist attack because they are forward deployed and often operate in chaotic environments. But, because of extensive defensive preparations, forward-deployed forces are not a particularly lucrative target for terrorists. US military units have the equipment and training needed to mitigate the impact of a WMD terrorist incident, pushing terrorists to find more lucrative (vulnerable) targets.

Another paradox produced by a successful counterproliferation policy is that concern about asymmetric warfare can heighten perceptions of a terrorist threat among the American public and policymakers alike. If US forces were expected to fare badly on some distant battlefield, then WMD terrorism would be considered "a lesser included threat," a second-order problem unlikely to make an already bad situation worse. Because changing perceptions of threat can produce significant political, strategic and military consequences, counterproliferation policies that increase the effectiveness of US military forces can actually make Americans feel less secure when it comes to WMD terrorism. Many observers probably underestimate the American response to WMD terrorism. But by influencing ex ante perceptions that terrorism is a likely asymmetric response to US conventional superiority, counterproliferation could foster an element of self-deterrence in American strategy. Because the need to develop an asymmetric response to US conventional superiority is a plausible motivation for WMD terrorism, US policymakers might become extremely reluctant to intervene in a regional crisis. In other words, we might scare ourselves silly.

Counterproliferation and Coalition Warfare

If American units find themselves in high-intensity conventional combat, they probably will be participating in an international coalition. Coalition warfare is an extraordinarily powerful weapon in the US arsenal because it demonstrates the overwhelming political commitment of the United States and the international community to stop aggression and other particularly egregious abuses of human rights. Coalitions, however, can be politically fragile. Opponents often attack an alliance by destroying its political cohesion, demonstrating to alliance members the unavoidable fact that the risks and benefits of warfare are not shared equally among the members of the coalition. Indeed, this was Saddam Hussein's intent during the Gulf War when Iraq attacked Israeli cities using SCUD missiles. Unable to stop the Gulf War coalition militarily, Saddam sought to stop it politically by attempting to turn the war into an Arab-Israeli dispute, not a battle to end Iraqi aggression.

If allied publics and militaries are vulnerable to state and non-state WMD terrorism, US-led coalitions might find themselves increasingly vulnerable to terrorist blackmail. Because counterproliferation efforts have reduced the impact that WMD terrorism might have on forward-deployed US units, allied publics and militaries could be viewed as appropriate targets within easy reach of terrorist groups. By showing that allied governments are unable to protect their citizens, terrorism could undermine allied support for coalition operations by undermining popular support of allied governments themselves. The possibility that asymmetric responses might occur to US conventional superiority and the logic of coalition warfare coincide to identify allied military forces and populations as a tempting target for terrorist attack.

Counterproliferation further bounds the terrorist threat by hardening allied military and civilian targets against terrorist attack. International counterproliferation and consequence management preparations are valuable counter-terrorism instruments. The United States has launched two major regional initiatives to improve the ability of forward-deployed US forces and local allies to respond to the threat posed by chemical, biological, and nuclear terrorism. On the Korean peninsula, for instance, the Office of the Secretary of Defense and the South Korean Ministry of Defense have undertaken a series of initiatives to improve the ability of South Korean and US forces to deter and defend against weapons of mass destruction. US and South Korean officials also have opened a dialogue to facilitate counterproliferation planning. As a result, combined military exercises now include nuclear, chemical, and biological warfare scenarios. Additionally, the Koreans established a new Nuclear, Biological and Chemical Weapons Defense Command in June 1999 and have included funding for improved protective

and detection equipment in their 1999 defense budget.

The Defense Department also has launched a Southwest Asia Cooperative Defense initiative. The initiative is intended not only to improve the ability of US and coalition forces to operate in a CBW environment, but also to improve host nations' abilities to protect population and industry from chemical and biological weapons attack. Already, extensive cooperation is planned in four areas: (1) C4I and shared early warning; (2) active air and missile defense; (3) passive defense (force protection and sustainment of military operations following chemical or biological attack); and (4) consequence management.

As potential "front line" states, US friends and allies on the Korean peninsula and in Southwest Asia are particularly vulnerable to both state and non-state sponsored acts of terrorism. Although the initiatives currently underway do not completely eliminate the threat posed by WMD terrorism especially to the civilian populations of America's allies, they are a logical first step in closing off a "window of opportunity" for terrorists.

Counterproliferation vs. Consequence Management

Although US counterproliferation policy has helped reduce the threat posed by state-sponsored WMD terrorism directed against US forces, allies, and even civilians, it has done little to reduce the threat posed by non-state actors to the US population. According to the Gilmore report, this threat is real, although it has been mischaracterized. Gilmore and his colleagues believe that there is a high probability that a low-casualty event will occur in the United States involving some type of "mass casualty" device. Terrorists lacking state sponsors probably do not have the technical expertise, equipment, and materials needed to construct or use nuclear, biological, chemical, or radiological weapons to inflict casualties and destruction on a truly massive scale. Instead, Gilmore suggests that poisonings, agricultural sabotage, or product tampering seem to be plausible activities for terrorist organizations. Clearly, counterproliferation can do little if anything to address this sort of activity.

If officials really do believe that non-state actors pose a serious WMD threat to the United States and that these individuals cannot be deterred, preempted, or arrested before they strike, then significant material and personnel resources must be devoted to deal with the consequences of a WMD attack against civilians. "First-responders" need to learn how to deal with chemical or biological weapons; without training and equipment, police, firefighters and paramedics actually can spread pathogens or toxins, thereby producing more casualties. Vaccines or antidotes need to be made available to contain disease outbreaks or to save the lives of people exposed to deadly agents. Military organizations—here the National Guard comes to mind—must equip, train, and prepare to act rapidly to contain and reduce weapons effects in large urban areas. A whole new set of strategies, protocols, doctrines, and tactics needs to be developed to counter the effects of terrorist attacks.

Viewed in isolation, consequence management is no small task. Further complicating matters is the fact that counterproliferation and consequence management differ fundamentally. Counterproliferation initiatives primarily involve military forces and are directed against threats located outside of the United States. Counterproliferation is intended to deter or prevent acts of state and even non-state sponsored terrorism before they occur. In contrast, consequence management is intended to limit the impact of a failure of counterproliferation policy to prevent a WMD terrorist attack against civilians.

Counterproliferation and consequence management policies will soon present policymakers with significant tradeoffs in terms of budgets, personnel, organizational structures, and philosophies that

govern the fight against WMD terrorism. So far, these tradeoffs have not received much attention from those involved in either antiterrorism or counterproliferation. But if the terrorist threat increases, lawmakers, government officials, and military officers might confront several stark dilemmas.

First, throughout this century, US efforts to counter the effects of chemical or biological weapons have been undertaken with military units in mind. For example, troops likely to encounter biological weapons are vaccinated, but similar efforts to vaccinate entire populations would be enormously expensive and possibly counterproductive. Anti-toxins issued to soldiers are extraordinarly potent agents that could themselves create a public health hazard if issued in peacetime to American households. Military personnel are supplied with expensive equipment that requires extensive training for proper utilization. It is unrealistic to believe, however, that average citizens can be equipped and trained in peacetime to the high standards needed to operate sophisticated chemical and biological weapons detection devices or to utilize protective equipment properly. In other words, equipment and techniques used to protect military formations and personnel cannot simply be given to fire departments to help protect a local population.

Second, although counterproliferation initiatives can constrain non-state actors by drying up black markets in contraband materials and equipment or in deterring state support to terrorist groups, counterproliferation policy is primarily directed against threats that can be identified in geographic terms, if not always by national origin. Counterproliferation policy is intended to strengthen the capability of US forces to operate in a chemical, biological, or nuclear environment, a setting that implies war between recognized national entities. In this sense, counterproliferation policy reflects the state-centric bias of America’s armed forces, which prepare to fight roughly similar units in opposing military organizations. Counterproliferation policy only addresses non-state threats in a tertiary manner because it supports a US military that views non-state threats as a minor concern. Increased emphasis on consequence management thus reflects a fundamental shift in American defense priorities.

Third, to better combat WMD terrorism, consequence management and counterproliferation policies must be better coordinated. But this coordination would have to occur at the weakest point in US security: at the bureaucratic and legal nexus between foreign and domestic policy. Further complicating matters is the fact that even though counterproliferation is organized by DoD, the domestic response to terrorism is loosely organized. The Gilmore report noted, for example, that today the scope or severity of an incident involving a chemical, biological, or nuclear weapon would determine which (local, state, federal) agency would take the lead in responding to a terrorist incident. Terrorism cuts across national, bureaucratic, and jurisdictional borders, but the American effort to stop terrorism has a long way to go before it too is a seamless enterprise.

Conclusion

Counterproliferation contributes to antiterrorism in several significant ways. It bounds the terrorist threat by reducing the vulnerability of US forces, allied military units, and even allied publics to terrorist attack. It helps to deter state-sponsored terrorism by bolstering the ability of US forces to retaliate with massive conventional force or with nuclear weapons. Although leaders that possess chemical, biological, or even nuclear devices might find common cause with some terrorist group, they apparently have no desire to have their state linked to a terrorist attack involving unconventional weapons. Counterproliferation also reduces the prospects of terrorist incidents by helping to keep "surplus" materials or weapons from entering black markets. Officials or analysts rarely mention these positive contributions because counterproliferation is not intended to address the terrorist threat, although on occasion (e.g., the Gilmore report) they are factored into intelligence assessments or strategic

calculations.

Counterproliferation and antiterrorism also are linked in less desirable ways. The dominance of US conventional forces compels antagonists to seek asymmetric responses to American superiority on the battlefield. To the extent that counterproliferation bolsters this conventional superiority by providing escalation dominance, it might channel an enemy's response to available targets (e.g., terrorist attacks against civilians). Similarly, counterproliferation policies that harden US or allied forces to terrorist attack might channel terrorists toward softer (civilian) targets. Unlike the positive contributions made by counterproliferation policy, officials and analysts are highly aware of the possibility that opponents might use asymmetric attacks to respond to US conventional superiority. Concern about asymmetric attacks helps to blind observers to the ways counterproliferation bounds the terrorist threat.

The relationship between counterproliferation and antiterrorism, however, is based on more than cognitive biases—risk-averse officials and analysts could be expected to be more aware of potential losses (domestic terrorism) than existing gains (reduced threats against forward-deployed military units). If fear of domestic terrorism continues to grow, significant budgetary tradeoffs between antiterrorism and counterproliferation might be looming on the horizon. These tradeoffs cannot be avoided because many counterproliferation initiatives simply cannot be used to help in consequence management. Counterproliferation is intended to help military units in battle against relatively symmetrical state-sponsored military forces, while consequence management closely resembles disaster management. Military units can hope to defeat their opponents in battle, thereby avoiding the costs of defeat for themselves. But disaster managers cannot defeat hurricanes; they can only take steps to minimize the impact when disaster strikes. It is this difference in fundamental objective that ultimately limits the possibility of simply applying counterproliferation capabilities in an antiterrorism campaign, and that will force policymakers to make difficult organizational and budgetary choices in the years ahead.

Chapter Nine

Intelligence and Force Protection vs Terrorism

Peter S. Probst

I think most recognize that the world as we know it is in a state of flux and transition due, in large part, to the disintegration of the Soviet Union and the end of the Cold War. Economic forces, resurgent nationalism, militant Islam, linguistic and cultural differences, rampant corruption, coupled with actions of ruthless demagogues, have contributed in varying degrees to the chaotic conditions we now see in the former Soviet Union, the Balkans and, unfortunately, in too many other countries and regions of the world.

Radical Islam is a potent force in much of the Middle East, the Muslim ghettoes of Europe, and is evidenced here in the United States as well. Violent Islamic extremists with deep pockets, such as Osama bin Laden, have developed a global reach and are working relentlessly to procure weapons of mass destruction.

An emerging and significant threat is represented by improvised biological, chemical and nuclear devices that exploit technologies that once were the sole preserve of world and regional powers. The ability to decimate large population centers and wreak havoc on an unprecedented scale has devolved from nation-states to groups and now even to the individual.

The possibility of a biological Unabomber armed with pulmonary anthrax or plague is a reality as near as tomorrow’s headlines. Whether they be nations or lone individuals, proliferation enables those who are traditionally at the margins to play a major role on the world stage. Improvised weapons of mass destruction will be the great equalizers of tomorrow, providing the means for the disaffected and deranged to directly impact on the core interests of world powers.

The world as we know it is forever changed. Our strategies, tactics, and capabilities need to reflect these new realities if we are to successfully meet the terrorist challenges of the post-Cold War era and successfully navigate the treacherous waters of this "brave new world" which our children will ultimately inherit.

To be effective, intelligence and antiterrorism must be inexorably linked. They are two sides of the same coin and must engage in a continual interactive and iterative process in which existing antiterrorism standards, tactics, doctrine, and training are continually measured against the latest intelligence and anticipated developments so that our approach may be adjusted accordingly. We cannot have effective antiterrorism without effective intelligence collection and analysis.

Nor can we have effective antiterrorism if we base our security on the demonstrated capabilities of our terrorist adversaries. To do so, in effect, is to plan for yesterday’s attack; and we will be blindsided when terrorists adopt new tactics or significantly increase the lethality of their current arsenal.

Currently, many in our community are focusing on terrorist use of improvised weapons of mass destruction. There can be little doubt that such weapons could have devastating results. I fear, however, our preoccupation with the exotic is causing us to focus less on the mundane. And this has me concerned.

One tactical approach for which we are unprepared is terrorist exploitation of the Third Country Nationals (TCNs) who work at our overseas installations. They may work in food service, or as members of the charforce, or in the BX. These are the invisible people. These are the people we rarely notice, but their work gives them access to the food, water, medicine, and other consumables used by our troops.

Another example of a potential insider threat is our use of foreign contractors about whom we know too little. Our continued use of the bin Laden construction company and its affiliates on construction projects at some of our most sensitive installations in the Gulf is a case in point. The opportunities for a member of the construction crew to do serious mischief should not be underestimated and can be very difficult to detect. Moreover, implantation of devices need not take place on site if access to the materiel can be obtained during manufacture or transport. The security implications are obvious. How we will deal with them is problematic.

All this being said, the fact remains that the emphasis of such programs is "after the fact"—after an individual has been observed acting suspiciously, or after a suspicious incident has occurred. A trained terrorist operative is unlikely to attract attention. Such an individual need only act once and, most likely, his actions would appear to be within the norm.

Awareness programs, although extremely important, are largely reactive in nature. They depend on the good guys spotting someone committing a bad act—an action that is out of character and, therefore, inherently suspicious. These programs are important, but they address only one aspect of the problem.

To be truly effective security programs must be primarily proactive. Programs must be in place to prevent potential miscreants from obtaining access to vulnerable and vital DoD installations in the first place. In other words, through intelligence, we must vet those who are in positions to do us harm. If we cannot provide ourselves such assurances, then we cannot afford to employ them. The potential risk is too great. It is only common sense. This is the role of antiterrorism/force protection through intelligence. This should be the heart of our security program and, as far as I can determine, is not being adequately addressed, if addressed at all.

The arguments against such an approach generally boil down to monetary considerations. It would cost too much. It would mean either American soldiers or contract labor that can be vetted would be used, and the costs could be exorbitant.

Yes, it would cost more but how much are the lives of American soldiers worth? What is the price tag we put on our country’s security interests? The irony is that if TCNs were involved in some future Khobar Towers type attack, such policy changes would be made overnight. And regrettably, after the fact. My view is, why wait? Why risk more tragedy and trauma, and more heartbreaking ceremonies at Dover AFB.

For those concerned about the bottom line—and let’s be realistic, we all are—such costs would likely be greater because the changes would be implemented rapidly—probably by fiat and without adequate study. Other costs cannot be calculated. These are the costs of American lives and prestige. Such losses have no price tag.

In order to be truly effective I think antiterrorism must be viewed in the broadest sense. If we commit ourselves to a static defense, we will be constantly probed and tested until a weakness is found and our defenses penetrated. To put it less delicately, a bunker mentality will get you killed.

One possible fix is to extend our effective perimeter beyond the installation gate by developing ties with surrounding villages and towns. It is the traditional hearts and minds approach, and it still has validity today.

For example our engineers can build roads that enable those in villages near our bases to bring their goods to market, and link remote towns and villages to the capital. Roads are the arteries that bind remote and isolated populations together as an interdependent political and economic entity we call a nation. Roads promote a sense of nationhood and a mutuality of interests. Roads also enable the military to more rapidly reach isolated areas to assist in mitigating natural disasters and to provide requisite security.

Bringing radio and television to such areas also is extremely constructive. These media can provide health, farming, literacy, and other educational programming to better the lot of local inhabitants. Our engineers can also repair bridges, build schools, dig wells, and run pipe to provide potable water. These activities not only raise the standard of living, but create links between our troops and the local population. Gradually our perceptions of the locals change and so do theirs, as genuine friendships and loyalties develop.

Where security and custom permit, troops can also become involved in off-duty activities such as coaching kid's soccer, teaching in local schools, or assisting in orphanages and hospitals.

One of the most valuable tools is the use of mobile medical teams that minister on a regular basis to the local population. Such activities promote trust and confidence. They also can serve as a trip wire by providing a channel for local villagers to report events or developments that they fear may impact on their security or well-being.

I like to view antiterrorism as a series of concentric circles, the common denominator being intelligence. Our aim should be to extend these perimeters to the maximum.

Use of an active defense provides additional layers of security. But I would like to expand the concept. I firmly believe the best defense is an aggressive offense in which traditional counterterrorism, antiterrorism, intelligence collection, and covert action are seamless and integrated.

Even our best-guarded bases are not islands unto themselves, but very much tied to the outside world. Our bases have numerous portals of entry besides the front gate. And these other avenues of access also need to be guarded and secured.

For example, is our installation dependent on a local pipeline and pumping stations for water? Contrary to what many believe, water, when supplied in this fashion, may be successfully contaminated with several commercially available and very lethal agents. If our drinking water is delivered by tanker truck or stored in large bladders the terrorist's job may be even easier, particularly if the bladders are not adequately secured.

Local procurement or transport of food stuffs offer similar opportunities. Our veterinary officers may make random checks for conventional risks such as spoilage but, for the most part, they are neither trained nor have the means to detect poisons or other contaminants that may be purposely introduced.

In many respects, the greatest challenge we face is not the terrorist's access to technologies of mass

destruction. Nor is it his ability to employ computers and the Internet to enhance his security, develop and exploit information, and extend his operational reach. Nor is it even his increased sophistication in waging war in the political arena.

In my view, the greatest threat to our security remains problems of mindset and perception. We fail to appreciate how phenomena such as mindset and perception impact on terrorist thinking and operations. Further, we rarely consider how such phenomena constrain and distort our own views and premises on which we base our operational planning.

Failure to identify and understand our own mindset may cause us to overlook or dismiss potentially catastrophic vulnerabilities and, at the same time, constrain our ability to fully exploit those of our terrorist adversaries.

Whether an individual or a nation, the perceptions one holds molds the reality in which one operates, and the methods and means one develops to navigate in that reality. For all practical purposes, "perception is reality." Or to put it somewhat differently "reality is in the eye of the beholder." If we are to defeat our terrorist adversary, we must understand his "reality" and how he adapts to it and operates in it. This remains one of our major intelligence gaps.

We need to understand on a group-specific basis how the terrorists think, how they plan, how they collect intelligence, select targets, weigh options, and adapt to operational adversity.

From the antiterrorism standpoint, we also need to understand how the terrorists view us and our security measures. What do they see as our strengths, weaknesses, and levers to be manipulated? In other words, we need to see ourselves and our security measures, through the eyes of our terrorist adversaries. Then, when there is no hard intelligence as to the venue or timing of the next attack, we can more intelligently game out the terrorists available options and how the terrorist will most likely play his hand.

The terrorists' perceptions—right or wrong, accurate or inaccurate—will drive their strategy, tactics, and planning. An understanding of such factors is one key to developing an effective antiterrorism program. Conversely, our own perceptual lenses colored by culture, history, personal experience, and bureaucracy may further distort an already flawed or incomplete picture.

If the past is any predictor of the future, in most instances we will not obtain the intelligence necessary to pre-empt terrorist operations. And that is the rub. If it is unlikely we will be able to detect, deter, or preempt a significant number of terrorist attacks, we then need to change the rules of the game and modify the "reality" in which the terrorist operates.

What I am talking about is developing information and analysis that enables us to better predict how, when, and where the terrorists will strike because we have fed them the information on which they will likely act. In other words, we need to develop an exceedingly robust deception, disinformation, and covert action capability. What I am advocating is an orchestrated, group-specific campaign to confuse and confound the enemy, and cause him to squander resources, take unwise risks, force his hand, and entice or propel him to commit operational blunders.

Through careful analysis we can develop a better understanding of how a particular terrorist group is likely to process information, what factors are given particular weight, and the operational predilections of the terrorist leader and his planners.

Targets that are lucrative and essentially undefendable can be made to appear "hardened." Seemingly lucrative and vulnerable targets that, in reality, are traps waiting to be sprung may be created—their value and vulnerability established in the eyes of our adversaries through a variety of deception mechanisms.

Now one may legitimately ask is this antiterrorism, counterterrorism, covert action or what ever? One of our problems is we create false dichotomies and bureaucratic definitions that constrain our thinking and reduce our operational effectiveness.

Basically, I see antiterrorism and counterterrorism as a continuum—offensive measures at one pole and defensive measures at the other. Depending on circumstances, an appropriate response may lie anywhere on that continuum and will likely be a mix of defensive and offensive measures that will shift in reaction to the moves and countermoves of the various parties as the situation plays out.

We have defined counterterrorism and antiterrorism as separate and distinct. The consequence is that we have ended up with two separate and distinct areas of expertise and, in turn, have created two separate and distinct communities that do not mesh as well as they should. We have, in effect, let definitions constrain our thinking, dictate our organizational structure and, at times, drive our operational response.

I would like to suggest consideration of a different organizational approach by creating a structure that is extremely fluid, flexible and, most importantly, threat driven. It would have both offensive and defensive capabilities and special teams, but all would be under a unified rubric. In essence, it would be a task force approach in which members, drawn from the Intelligence Community, would bring to the table specific skills needed to attack a particular terrorist group or issue. Once the problem is resolved, the team would disband and its members return to their home agencies. Should a new issue arise, a new tailored team would be fielded. It is much the approach we are using against bin Laden but, rather than being the exception, it would become the institutionalized norm.

Basically, I believe in a holistic approach in which one may pick and choose from an operational tool kit of offensive and defensive measures that enables us to tailor our response to a specific threat. And through covert action, deception, and a variety of psychological operations, we alter the perceptions of our adversary so he is led down a path to ultimate destruction. In the game of terrorist vs. antiterrorist, the clarity with which we view our enemy and ourselves will, to a large extent, determine the winners, the losers and the price paid by each.

Chapter Ten

The Military's Response to Domestic WMD Terrorism

William C. Thomas

The role of the Department of Defense (DoD) in countering domestic weapons of mass destruction (WMD) terrorism is one of support, not leadership. Military forces are primarily designed to operate against threats outside the US. Many of the skills required for combat, however, are also applicable in domestic WMD emergencies and can supplement the capabilities of local, state, and federal agencies responsible for managing a crisis and its consequences.

In many cases, an event involving WMD will be of such scope as to exceed the resources of other agencies. The US military has therefore been tasked, through legislation and Presidential directives, to support civilian authorities in the preparation for, resolution of, and consequence management after a domestic WMD terrorism event. Terrorism within the United States is a criminal act, and military members are not police officers, but they can provide critical support in the form of intervention and consequence management.

This chapter explores the requirements for DoD support following a domestic WMD terrorism event. It identifies the capabilities that civilian responders anticipate the DoD will provide when civilian agencies are overwhelmed. Finally, it reviews current skills and programs and evaluates the effectiveness of the military in responding to Legislative and Executive branch taskings as well as to specific contingency plans.

The primary goal of American counterterrorism programs is deterrence. A strategy that makes the most effective use of available capabilities will allow the United States to better counter the strategies of those groups that would use weapons of mass destruction. The US military offers many important tools for use in such a strategy.

Department of Defense Responsibilities

In 1996, Congress determined that the US lacked the training and the countermeasures required to address WMD terrorism. While the Department of Energy (DoE) had response teams for nuclear emergencies, there was no comparable capability for chemical and biological emergencies. Congress went on to pass legislation mandating the development of these missing capabilities and the improvement of America's response capability. Other requirements have been dictated by Presidential directive. Many of these functions are now the responsibility of the Department of Defense.

Legislative Requirements

One of the most sweeping pieces of legislation in recent years addressing the military's role in WMD terrorism is the FY97 defense authorization act. Title XIV of the Act, referred to as the "Defense Against Weapons of Mass Destruction Act of 1996" or the "Nunn-Lugar-Domenici Act," requires the Defense Department to provide training to local and State officials who will serve as "first responders" in a WMD terrorism event. It also mandated that the DoD will have a rapid response team for detection, neutralization, containment, dismantlement, and disposal of WMD. Finally, the DoD is authorized to support the Department of Justice (DoJ) in its law enforcement function in emergencies involving chemical or biological WMD. This is an exception to the *Posse Comitatus* Act, which restricts the use of

the military for law enforcement, and it should be undertaken only in the most extreme circumstances.

The FY99 defense authorization adds a further item regarding the DoD's role. It clarifies the authority to use Reserve members in emergencies involving WMD, as members of the DoD Consequence Management Program Integration Office, or on rapid assessment element teams.

Presidential Decision Directives (PDD)

PDD 39, *US Policy on Counterterrorism*, published in June 1995, reaffirms that the US will have the ability to

- respond rapidly and decisively to terrorism;
- protect Americans;
- arrest or defeat the perpetrators;
- respond with all appropriate instruments against the sponsoring organizations and governments;
- provide recovery relief to victims, as permitted by law.

It directs the Federal Emergency Management Agency (FEMA) to ensure that the Federal Response Plan (FRP) is adequate for responding to WMD terrorism. This gives FEMA the authority to assign lead agency and supporting responsibilities within the FRP. Specific requirements for the DoD include providing transportation for the FBI's Domestic Emergency Support Teams (DEST) and ensuring DoD's counterterrorism capabilities are well managed, funded, and exercised.

The most recent directive on combatting terrorism, PDD 62, was published in May 1998 and created a new office within the National Security Council staff. The National Coordinator for Infrastructure Protection and Counterterrorism oversees preparedness and consequence management for domestic WMD terrorism, and leads the development of guidelines for crisis management. The DoD and other agencies work together under the guidance of the National Coordinator in developing training programs and response plans.

Legal Limitations on Military Support

As a general rule, federal military forces may not be used in domestic law enforcement. This restriction stems from federal law, specifically 18 USC 1385, commonly known as the *Posse Comitatus* Act. *Posse Comitatus* prohibits military members in an official capacity from participating directly

- in arrest, search and seizure, stop and frisk, or interdiction of vessels, aircraft, and vehicles;
- in surveillance or pursuit;
- as informants, undercover agents, or investigators in civilian legal cases or any other civilian law enforcement activity.

It strictly limits the use of military force against the civilian population. There are, however, a number of exceptions to *Posse Comitatus*, some historical and some based on recent legislation, which are applicable to the issue of domestic terrorism.

Under the Constitution, the military may be used to protect civilian property and functions, or to protect federal property and functions. This generally falls under the military's authority to restore order in the event of insurrection or a civil disturbance that goes beyond civil authorities' ability to control. Department of Defense Operation Plan GARDEN PLOT (DoDD 3025.12-R) outlines the use of military

capabilities in support of civil authorities during a major disturbance. The 1996 "Defense Against Weapons of Mass Destruction Act" specifically authorizes the Secretary of Defense to support the Justice Department in emergencies involving chemical or biological weapons. While the use of the military in a law enforcement role must be reserved only for extreme emergencies, and should be discontinued as soon as possible, it is nevertheless legal.

In addition, it should be noted that *Posse Comitatus* applies only to federal active duty and Reserve military forces. National Guard forces that have not been federalized (in other words, those in "state status") are not covered under this law. A governor who requires resources beyond those provided by state and local police can call upon National Guard forces to supplement them. The sight of National Guard members providing security and law enforcement in the wake of a natural disaster is a common one, and those resources could just as easily be put to use after a man-made disaster.

The legal restraints on military activities within the United States exist for good reason, but they should not limit the use of available resources that are critical in an emergency. The laws currently in place, and the mechanisms for determining when an emergency warrants an exception, ensure the proper balance is maintained in the use of military force.

Civilian Agency Expectations

A variety of agencies at the federal, state, and local levels will participate in a WMD terrorism response effort. An understanding of their requirements and expectations will enable the military to provide the most effective support.

FBI WMD Incident Contingency Plan

Because terrorist activities constitute criminal offenses, the Department of Justice serves as lead federal agency (LFA) for terrorist attacks occurring on US soil. Operating through the FBI, DoJ is responsible for crisis management, which refers to the actions taken to resolve a threat or an act of terrorism.

The FBI plan briefly discusses the support that the military offers. It highlights specific support that DoD might provide to FBI, including

- Threat assessment;
- DEST deployment;
- Technical advice;
- Operational support;
- Tactical operations, including the use of lethal or non-lethal force;
- Support for civil disturbances;
- Custody, transportation, and disposal of a WMD device.

The plan assumes there will be a liaison between FBI and DoD on a regular basis. Should an incident occur the Command Group at the FBI’s joint operations center will include the military joint task force commander. Military members are also likely to be located in the Operations Group and Support Group, and there will be a DoD component within the Consequence Management Group.

FEMA and the Federal Response Plan

FEMA, the LFA for consequence management (CoM), will conduct planning and prepositioning of equipment during the crisis management phase of an incident. At some point after an incident occurs, the focus transitions from crisis management to consequence management. As state agencies request assistance, FEMA will coordinate the federal response.

FEMA's plans for consequence management are contained in the Federal Response Plan. The plan is developed in coordination with all of the agencies that provide resources and personnel. It discusses the command and control of CoM assets and explains the broad range of capabilities that may be required. Thorough planning in advance allows FEMA and other agencies to quickly tailor the response to the needs of a particular situation. The FRP is used for natural disasters such as tornadoes and hurricanes as well as man-made disasters. While the CoM effort for a WMD terrorism event would be comparable to that in a natural disaster, there are some differences that must be considered (such as the requirement for evidence protection to aid in the investigation after the incident). As a result, FEMA added a terrorism annex in February 1997 that defines the required capabilities and the command structures for the multiagency response, both pre- and post-incident.

There are 12 Emergency Support Functions (ESF) that FEMA provides and that are outlined in the FRP. Each ESF is coordinated by a primary agency with support from a number of other organizations. Some ESFs are primarily directed toward an immediate response while others offer a more long-term solution.

- ESF-1 Transportation

- ESF-2 Communications

- ESF-3 Public Works and Engineering
- ESF-4 Firefighting
- ESF-5 Information and Planning
- ESF-6 Mass Care
- ESF-7 Resource Support

- ESF-8 Health and Medical Services

- ESF-9 Urban Search and Rescue
- ESF-10 Hazardous Materials
- ESF-11 Food
- ESF-12 Energy

The primary agencies for each ESF will develop plans for carrying out their functions. For those functions that require military support, the DoD should be involved at some point in the planning process.

State and Local Agencies

Each state has an emergency management agency (EMA) that works closely with local EMAs that are established by city, county, district, or some other municipality. The local EMAs oversee operations within their jurisdiction and will request help from the state as required. The state EMA, in turn, requests assistance from FEMA when federal help is necessary. State and local agencies develop plans for using their own assets (including National Guard), but their plans typically do not include the use of federal

military forces, as that lies within the purview of FEMA and the FRP primary agencies. The exception to this is the use of locally-based federal military forces operating under Immediate Response rules.

Military forces may be used to support local agencies in an emergency without going through normal channels. This is referred to as Immediate Response and is provided at the discretion of the installation commander or other competent authority. Immediate Response may include DoD assistance to civil agencies in meeting the following types of need:

- Rescue, evacuation, and emergency medical treatment of casualties, maintenance or restoration of emergency medical capabilities, and safeguarding the public health;
- Emergency restoration of essential public services (including fire-fighting, water, communications, transportation, power, and fuel);
- Emergency clearance of debris, rubble, and explosive ordnance from public facilities and other areas to permit rescue or movement of people and restoration of essential services;
- Recovery, identification, registration, and disposal of the dead;
- Monitoring and decontaminating radiological, chemical, and biological effects; controlling contaminated areas; and reporting through national warning and hazard control systems;
- Roadway movement control and planning;
- Safeguarding, collecting, and distributing food, essential supplies, and materiel on the basis of critical priorities;
- Damage assessment;
- Interim emergency communications;
- Facilitating the reestablishment of civil government functions.

Local and state agencies may be planning on support from local bases in the event of a terrorist event. If this is the case, they should be developing an effective relationship with the base beforehand and should include local military personnel in the planning process at some point.

The effects of WMD terrorism are likely to be so grave as to require a response from the military, supporting both the FBI's crisis management role and the consequence management efforts of FEMA and other federal, state, and local agencies. These organizations have certain expectations regarding the type of military support they will need. The DoD has a variety of resources that can be used to meet these expectations.

Current and Emerging DoD Capabilities

The Defense Department develops policies that are appropriate given its legal obligations and that guide planners and commanders as they prepare for responses to domestic terrorism. Joint and Service doctrine discuss the beliefs on the best way to employ military power in these situations. Forming the core of the federal military response will be the Chemical/Biological Rapid Response Team (C/B-RRT). The Nunn-Lugar-Domenci Act in 1996 set the stage for this team by proposing a standing DoD response force for chemical and biological terrorism that is comparable to DoE's force for nuclear emergencies. The C/B-RRT provides a graduated response ranging from prepositioning prior to high-profile events, to assisting civil authorities with hazardous materials, to responding to a WMD terrorism incident. With a commander provided by the US Army Soldier Biological and Chemical Command, the C/B-RRT's membership is drawn from existing organizations, including

- Technical Escort Unit;
- 52nd Ordnance Group (EOD);

- US Army Medical Research Institute for Infectious Diseases;
- US Army Medical Research Institute for Chemical Defense;
- US Army Material Command Treaty Lab;
- US Navy Medical Research Institute;
- US Navy Environmental and Preventive Medical Unit;
- US Naval Research Laboratory.

Each organization has its own specialty, which allows the C/B-RRT commander to tailor the deployed team to the needs of the situation and the requirements of the joint force commander. This structure enables a rapid start to the consequence management efforts that will then receive necessary follow-on support from other agencies. The units comprising the C/B-RRT, as well as other available military capabilities, are discussed later in this chapter.

Institutional Readiness

The DoD has policies for providing support during civil emergencies, including terrorism. These policies reflect the restrictions discussed above as well as the exceptions to those limitations. They provide the commander with guidance on when and how forces may be used, and with this guidance in mind, the commander can determine how best to employ forces based on the specifics of the situation.

Crisis management is primarily addressed in two documents: DoDD 3025.15, *Military Assistance to Civil Authorities (MACA)* and DoDD 3025.12, *Military Assistance for Civil Disturbances (MACDIS)*. MACA policy specifically authorizes the use of military forces in counterterrorism operations when approved by the President:

> The employment of U.S. military forces in response to acts or threats of domestic terrorism may be requested only by the President (or in accordance with Presidential Decision Directives) and must be authorized by the President. All requests for assistance in responding to acts or threats of domestic terrorism must also be approved by the Secretary of Defense.

Requests for counterterrorism support are made through the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict (ASD (SO/LIC)). The FBI, as the lead federal agency for crisis management, will typically initiate the request. There is a very good working relationship between the two organizations; in fact, there is an ASD (SO/LIC) representative in the FBI's WMD Operations Unit. The Chairman of the JCS maintains contingency plans for DoD's counterterrorism response. While supporting civilian agencies, DoD policy is that all forces involved in such support will remain under the operational control of appropriate military commanders.

Consequence management policies are covered in DoDD 3025.1, *Military Support to Civil Authorities (MSCA)*. National Guard forces under state control are the primary means of support for civil authorities, but federal military forces can be employed when the situation goes beyond the abilities of civilian agencies. Since October 1999, US Joint Forces Command's JOINT TASK FORCE - CIVIL SUPPORT has been responsible for overseeing the military's WMD terrorism CoM support.

DoD policy outlines the authorized use of military forces in crisis management and consequence management. Having determined what is authorized, it then falls to the DoD to determine what skills will be useful and how they will be employed. The military's preparation for this role is best reflected in appropriate military doctrine.

Separate from military directives, military doctrine provides the foundation for planning, training for, equipping for, and conducting operations. It presents the fundamental beliefs regarding the best means of carrying out a mission. There are two broad categories of doctrine: Joint doctrine, which considers the best methods for applying military force in general, and Service doctrine, which articulates the capabilities contributed by each Service and the best means of employing them. One indicator of the military's ability to conduct a mission is the availability of applicable doctrine, which shows how much thought, if any, has been given to the required capabilities. Military doctrine is developed at the strategic, operational, and tactical levels, and it is at these last two levels where doctrine may be found that applies to countering domestic WMD terrorism.

Joint doctrine addressing the military's role in WMD terrorism is found primarily in four volumes: Joint Publication (JP) 3-07.2, *Joint Tactics, Techniques, and Procedures for Antiterrorism*, JP 3-07.7, *Joint Tactics, Techniques, and Procedures for Domestic Support Operations*, JP 3-08, *Interagency Coordination During Joint Operations*, and JP 3-11, *Joint Doctrine for Nuclear, Biological, and Chemical Operations*. These documents discuss the context in which terrorist incidents might occur, explain how to coordinate effectively with civilian agencies at the local, state, and Federal levels, and examine the methods for operating in a WMD environment. They demonstrate that the DoD has given serious thought to the capabilities that would be important in responding to domestic WMD terrorism.

Service doctrine also addresses the requirements for this type of operation. The Army and Marine Corps have both developed doctrine for domestic support (FM 100-19/MCWP 3-33.4), military operations in urban terrain (FM 90-10/MCWP 3-35.3), and operations in an NBC environment (FM 3-series/MCWP 3-37-series). Air Force doctrine, in particular the doctrine for military operations other than war (AFDD 2-3), air mobility (AFDD 2-6 series), counter NBC operations (AFDD 2-1.8), and health services (AFDD 2-4.2), supports Air Force operations in an NBC environment and discusses the capabilities offered in response to domestic WMD terrorism.

Training for military forces is based on doctrine. It addresses the skills needed for modern missions, including those combat skills that are appropriate for combatting terrorism. There are some skills required in domestic urban operations that are not commonly required in traditional combat operations. Forces train to operate with civilian government and nongovernmental agencies, and learn about the complexities of functioning in an urban environment. Personnel who will operate within a hot zone need specialized NBC training, while those forces that will operate outside a hot zone or with decontaminated victims and responders (e.g., aeromedical evacuation crews) require only awareness training. When conducting operations, military forces must also be cognizant of the requirements for evidence collection; while saving lives is the top priority, it is also important to support investigative efforts that may prevent future incidents.

Organizations Dedicated to WMD and/or Terrorism Response

Technical Escort Unit: Part of the US Army Soldier Biological and Chemical Command, the Technical Escort Unit (TEU) was established in 1944 and is the Army's oldest chemical unit. Its missions include worldwide response for escorting, rendering safe, disposing of, sampling verification, mitigating hazards and identifying weaponized and non-weaponized chemical, biological and hazardous material. Military and civilian personnel possess a wide variety of specialized training in explosive ordnance identification and handling; radiography; military and commercial chemical handling; chemical and biological detection and monitoring equipment; medical response; Department of Transportation packaging requirements; and, Environmental Protection Agency regulations. Deployment packages include protective equipment; hazardous material transfer systems; mobile systems for

detecting, monitoring, and identifying chemical and biological agents; and communications links.

TEU would be deployed as part of the crisis management effort. Ideally, a device will be located and can be transported before it is employed. TEU provides the capability to transport an agent or render a device unusable. They are based in Aberdeen, Maryland, and require time to deploy. They often deploy in advance to high-profile events such as the 1996 Summer Olympics in Atlanta.

Chemical-Biological Incident Response Force: The Chemical-Biological Incident Response Force (CBIRF) is a relatively new Marine Corps unit. Created in the wake of 1995's sarin gas attack on Tokyo's subway system, CBIRF is designed to provide emergency support following WMD terrorist incidents.

> The concept for employment of the CBIRF details an initial, rapid response to chemical or biological incidents. When such an incident occurs, the CBIRF will deploy to the affected site. Once there, the CBIRF will provide a number of significant initial consequence management capabilities: assistance in coordinating initial relief efforts; security and isolation at the affected site (when authorized); detection, identification, and limited decontamination of personnel and equipment; expert medical advice and assistance; and service support assistance. Throughout its response, the CBIRF will be advised by civilian and government consultants in areas related to chemical or biological incidents.

As one example of its utility, CBIRF was deployed to Atlanta during the 1996 Summer Olympics. They were based downtown, mere blocks from the Centennial Park complex, in a position where they could provide an immediate tactical response should a potential chemical or biological incident occur. They were thus prepared when a bomb exploded in the park on July 27th. CBIRF representatives were on the scene within 20 minutes of the blast, and an entire 120-man team was deployed soon after that. Immediate indications were that no chemical agents had been released, and further analysis confirmed that no biological agents were present. Still, the team was prepared to fulfill its mission of "turning victims into patients" and providing a rapid start to the consequence management process, under the lead of the Atlanta Fire Department.

Rapid Assessment and Initial Detection Teams: The initial military response for consequence management after an incident will likely come from a National Guard Rapid Assessment and Initial Detection (RAID) team. The teams consist of 22 representatives from a cross-section of functional areas that can deploy and assess the situation, advise the local, state and federal response elements, define requirements, and expedite employment of state and federal military support. Their mission is to provide early assessment, initial detection, and technical advice to the incident commander during a WMD incident, and identify the requirements for DoD support.

The RAID teams can rapidly deploy to an incident site and provide initial support to the Incident Commander. The element has the ability to conduct reconnaissance, provide medical advice and assistance, perform detection, assessment, and hazard prediction, and can provide technical advice concerning WMD incidents and agents. RAID teams will also have a significant reachback capability that allows them to tap into expertise across the country.

A RAID team is organized under the peacetime control of a state's Adjutant General. Because of the rapid response requirements, the initial ten RAID teams (one per FEMA region) will typically consist of full-time Guard members. These teams will likely remain in state status, and will support responses in surrounding states without their own RAID teams through mutual assistance agreements between governors. Forty-four additional RAID teams, an idea still being considered, will likely consist of

traditional, part-time Guard members. The National Guard has reportedly faced some manning problems, trying to find personnel with the appropriate skills and rank to fill the highly specialized positions.

Organizations With WMD Terrorism Response As A Collateral Mission

Special Operations Forces: Special operations forces (SOF) offer a tactical response capability that can support law enforcement efforts when the scope of the situation goes beyond the abilities of civilian agencies. US Special Operations Command (including Army, Navy, and Air Force SOF) personnel may be called upon to aid civilian agencies in the resolution of a terrorist incident through reconnaissance, transportation, loans of equipment, or the appropriate application of lethal or nonlethal force. Such support will take place only in the most extreme emergencies, and will be conducted in accordance with all applicable laws regarding the use of military forces in support of civilian law enforcement agencies. The use of military forces will be terminated as soon as civilian agencies can effectively conduct operations.

52nd Ordnance Group (EOD): The 52nd Ordnance Group (EOD) is the only active duty Army Explosive Ordnance Disposal Group. Assigned to Forces Command, it has operational and administrative command of four subordinate EOD Battalions, each of which has 10 companies.

The 52nd ORD has units that can be employed in WMD scenarios. However, these companies are not designed solely for CONUS support, and may be deployed to overseas contingency operations. To ensure it has the ability respond to a terrorist incident, the 52nd ORD maintains two companies in the US that are dedicated to WMD terrorism response. WMD-trained elements of 52nd ORD will render safe nuclear or radiological devices. This capability complements, rather than replaces, that provided by the DoE's Nuclear Emergency Search Team. Members can also work with explosive components of chemical and biological weapons.

Though not specifically assigned a terrorism response mission, the other Services also have an EOD capability that may provide support during or following an incident. Many times this support will be provided under the Immediate Response rule. For example, Air Force EOD personnel assisted local authorities during an anthrax threat (which turned out to be a hoax) in Wichita, Kansas, in August 1998. Company commanders in the 52nd ORD have the authority to respond to requests for assistance from local officials, while EOD units in the other Services require their installation commander's approval. Units with special skills, such as EOD, are likely to find themselves assisting first responders in a terrorist event that occurs in their local area.

US Army Corps of Engineers: The DoD is responsible for the FRP's Emergency Support Function #3, "Public Works and Engineering." The US Army Corps of Engineers (USACE) has been designated as the agency that will carry out those responsibilities. Some of the functions that USACE provides for ESF #3 include

- Technical advice and evaluations;
- Engineering services;
- Construction management and inspection;
- Emergency contracting;
- Emergency repair of wastewater and solid waste facilities;
- Real estate support.

Some of the resources that can be utilized in support of the ESF #3 mission include the following:

- The Corps of Engineers' Prime Power Battalion which may be activated and rapidly deployed to a disaster area. This is a specialty unit that is trained and capable of providing emergency electrical power.
- Access to other military units - their personnel, equipment and supplies - such as Air Force Civil Engineers, Army Engineer Units, Navy Seabee Construction Units and Warehouse Managers, is also available.

The Corps of Engineers also has a support role to other agencies and departments within the Federal Response Plan.

Laboratories and Research Agencies: Certain military laboratories are designed to study WMD and their effects. The US Army Medical Research Institute for Infectious Diseases, for instance, would work closely with CDC in the event of a biological terrorism event. Other labs focus on chemical and nuclear weapons. In some cases, emergency responders work closely with labs on a regular basis, providing a critical synergy of theoretical knowledge and operational expertise. Other research agencies can provide essential information for a terrorism response. The Air Force Technical Applications Center, for example, can collect and analyze samples to determine the effects of nuclear weapons, while the Defense Threat Reduction Agency has experience in chemical-biological defense and nuclear weapons effects.

Additional Military Resources

Each of the Services has certain capabilities designed for combat that, while not specifically designated for use in a domestic terrorism role, may be especially useful nonetheless.

Security: Every Service has security personnel who can aid local authorities in providing security and law enforcement following an incident. Such support must be consistent with previously discussed legal requirements and policies. Also, it is likely that security will be upgraded at local military installations following an incident, which might preclude the provision of assistance to civil authorities. Security forces may deploy to protect military assets that are part of an incident response effort. Their NBC training makes them an excellent security asset when operating in or near a hot zone.

Medical: The Department of Health and Human Services is responsible for accomplishing ESF #6, "Health and Medical Services," which supports local and state health systems that are likely to be overwhelmed following a major terrorist event. The National Disaster Medical System is a partnership between Federal and non-Federal health providers (including the DoD and the Department of Veterans Affairs) that aids in the triage, treatment, and evacuation of patients.

Military medical personnel are, in many cases, trained to operate in an NBC environment and care for the victims of such weapons. They are also prepared for the types of traumatic injuries that are likely to be sustained during a bombing or other violent attack. This allows them to provide critical support to victims following a WMD terrorist incident. Some examples of suitable military assets include

- Air Force Medical Patient Decontamination Teams;
- Air Force Air Transportable Hospitals;
- Army Chemical Companies (NBC medical elements);
- Triage Teams;

- Preventive Medicine Teams;

- Air Force Aeromedical Evacuation aircraft and personnel (93% of this capability is in the Air National Guard and Air Force Reserve Command).
- Air Ambulances (rotary- and fixed-wing)

Local medical systems are likely to be overwhelmed following an attack, requiring the use of federal (including military) resources. First responders and military response personnel will also require specialized medical care to minimize their risk.

Support Services: Military forces have trained to deploy rapidly to austere locations and establish a basic infrastructure for conducting operations. Much of this support comes from support services personnel who ensure that shelter and meals are provided for military personnel. This capability can also be used to support civilian agency personnel, providing a "tent city" that offers basic living support to emergency and relief workers. Such facilities can also be used to house decontaminated victims and other evacuees. Mortuary affairs functions are typically found within services units, and will be essential to limiting the spread of disease following a mass-casualty incident.

Transportation: The rapid movement of emergency personnel, relief equipment, and medical supplies, is essential to minimizing the consequences of a WMD terrorist event. Many of the units and organizations discussed above will require air mobility to deploy to the site of the incident. The destruction caused by a WMD may render nearby airfields unusable, thus mandating the use of surface transportation from distant airports to staging areas near the hot zone. Airlift assets will need to be diverted from other missions, which may have an impact on US military operations around the world. Mobility aircrews are trained to operate in a NBC environment, as are air mobility support forces that can operate an aerial port for the delivery of supplies and personnel. Surface transportation, provided primarily by NBC-trained Army forces, will be required in some cases to move equipment near or into a disaster area.

Urban Search and Rescue (US&R): Upon arrival of the FEMA civilian US&R teams in the disaster area, the DoD provides each team a military radio support team and liaison officers capable of continuous twenty-four hour operations. The DoD provides transportation for the FEMA US&R teams from the time of arrival in the Mobilization Center, Staging Area or in the disaster area through team redeployment to their home city and/or state. FEMA US&R teams are self sufficient for up to 72 hours. The DoD assumes responsibility after this initial period to provide service support and resupply to include replacement medicines, tools and supplies. The DoD is responsible for providing military units to conduct basic and light US&R, trained structural engineers from the US Army Corps of Engineers to advise US&R units, and equipment for civilian teams to conduct medium and heavy US&R operations. The Air Force’s auxiliary, the Civil Air Patrol, can also be called upon to perform search and rescue missions.

Communications: ESF #2, Communications, is the responsibility of the National Communications System (NCS). The NCS is an interdepartmental organization composed of 23 federal departments and agencies, including the Department of Defense, National Security Agency, and the Joint Staff. Its function is to ensure the effective flow of communications in a disaster or other emergency. DoD’s emergency telecommunications assets include the following systems and capabilities:

- Advanced Research Projects Agency Network;
- Defense Data Network;

- Defense Switched Network;
- Defense Message System;
- Defense Satellite Communications System;
- Future Secure Voice System;
- Joint Chiefs of Staff Alerting Network;
- National Military Command System;
- Washington Area Wideband System;
- Worldwide Military Command and Control System.

Both the National Security Agency and Defense Information Systems Agency actively support the NCS.

In addition to working with the NCS, the military can directly support the lead Federal agency and state and local agencies. Tactical communications assets can be used to improve the capabilities of responders. In a situation covering a large area, or where there is no power or other infrastructure available to establish a FEMA Disaster Field Office, the Chairman of the JCS may make available a National Airborne Operations Center. This E-4B aircraft can carry a staff of approximately 40 personnel and provide them with communications, meeting areas, and living quarters, both in the air and upon landing, for 48 hours.

The Figure that follows outlines the Emergency Support Functions contained in the Federal Response Plan, and the military capabilities that can be used to directly support those ESFs.

Conclusion

Since the 1995 bombing in Oklahoma City, America has realized it is not immune from terrorism at home. The Tokyo subway attack raised fears about the use of WMD. There is increasing concern that some fundamentalist religious groups may seek to encourage the plagues or the apocalypse their teachings predict. In light of these heightened threats, it is important that governments at all levels are seriously considering the threat of domestic WMD terrorism. The military's training for the NBC battlefield and its experience in consequence management following natural disasters will in many cases provide critical support to civilian agencies before, during, and after a WMD event. Presidential directives, Congressional legislation, and civilian agency expectations have provided guidance for the development of the tools required to counter the emerging threat. Hopefully, the mere fact that such capabilities exist will effectively deter terrorists so that these skills will never be required.

FRP EMERGENCY SUPPORT		DoD SUPPORT
ESF-1	Transportation	Airlift (fixed wing and rotary wing) Surface transportation
ESF-2	Communications	National Airborne Operations Center (NAOC) Civil Air Patrol Tactical communications assets National Communication System
ESF-3	Public Works and	US Army Corps of Engineers

	Engineering *DoD is the Primary Agency; USACE is the designated Operating Agent*	Civil Engineers/Combat Engineers EOD Airlift
ESF-4	Firefighting	Airlift Air National Guard firefighting aircraft Firefighting personnel
ESF-5	Information and Planning	RAID teams Civil Air Patrol
ESF-6	Mass Care	Services personnel Airlift Decontamination teams
ESF-7	Resource Support	Airlift
ESF-8	Health and Medical Services	Aeromedical Evacuation Medical personnel Decontamination teams
ESF-9	Urban Search and Rescue	Airlift Aerial Reconnaissance Civil Air Patrol
ESF-10	Hazardous Materials	Airlift TEU CBIRF 52 ORD Decontamination teams
ESF-11	Food	Airlift
ESF-12	Energy	Airlift

Federal Response Plan Emergency Support Functions and DoD Support

Chapter Eleven

International Incident Response

Operations Directorate, Office of the Coordinator for

Counterterrorism, US Department of State*

Introduction

> "Terrorism is at the top of the American agenda, and it should be at the top of the world's agenda." President Clinton, address to the UN General Assembly, September 1998.

As President Clinton made clear in 1998, terrorism is very much a global problem, and one of paramount concern to the government of the United States. The US Government and American citizens abroad are often targets, but terrorism threatens everyone. Like drug abuse, poverty, or disease, terrorism is a pervasive transnational problem. Because of the worldwide menace terrorism represents to national and international security, it demands a well-conceived, thorough, and robust international incident response.

Terrorist attempts to influence American policy have been among the most vexing problems for the United States. Today, the growing capability of terrorist groups to inflict mass casualties and capture public attention complicates an already acute policy dilemma, especially in an era of rapid globalization. The speed and reliability of both transportation and communication are factors driving the dispersion of terrorist networks. Terrorist organizations are subsequently more linear, more loosely defined, and harder to track. While these realities certainly work to the advantage of terrorists, globalization also presents opportunities to those tasked with responding to the terrorist threat. It is critical that we adapt our countermeasures to meet the changing dimensions of international terrorism.

The problems and imperatives inherent in organizing responses to international terrorist incidents today are the subject of this chapter. Against the backdrop of certain watershed terrorist incidents in American history, we will briefly review some of the ways in which the terrorist threat has changed and discuss how US policy principles have developed. We will then look at the ways government responses to terrorism are improving, and discuss whether these strategies adequately address the types of threats seen today. Finally, we will identify some important factors that can be expected to shape international responses in the coming decade.

Although we will focus on international terrorism, it is worth noting that the lines between international and domestic terrorism are blurred and cut across many functional areas, making interagency coordination a critical component of any comprehensive US strategy to combat terrorism in the 21st century.

Learning the Lessons of International Response

No Concessions

Current US counterterrorism policy is the result of many often painfully learned lessons. America's experience with international terrorism is as old as the United States itself, and many of our presidents

have faced difficult choices in crafting appropriate responses. The Barbary pirates were a famous early example. During the late 1700s and early 1800s, seaborne bandits from Tripoli, Tunis, and Algiers frequently raided American ships off the Mediterranean's Barbary Coast. It had become routine US practice to negotiate with these pirates and to pay the huge ransoms they demanded. By 1801 the United States had paid over $2 million in this manner, or over one-fifth of the US annual revenue at the time. President Thomas Jefferson finally put a stop to this with an early version of our current no-concessions policy, by refusing ransom demands of the Barbary pirates. He observed: "This is cruelty to the individuals in captivity, but kindness to the hundreds that soon would be so, were we to make it worth the while of those pirates to go out of the straits in quest of us."

Jefferson famously followed up his no-concessions policy with military action; in 1801 he dispatched a squadron of US Navy and Marines to protect American shipping in the Mediterranean. When in 1803 pirates acting under the order of the Pasha of Tripoli seized the *USS. Philadelphia*, took the ship's crew hostage and demanded $3 million in ransom, the stage was set for one of the first ever uses of US military force abroad. In response to the seizure, US Navy Lieutenant Stephen Decatur's forces blockaded Tripoli, set fire to the *Philadelphia*, and bombarded the city. The operation was a success, and the pirates released the hostages.

The United States later directed similar action against the Algerian navy in 1815 in response to its sponsorship of piracy. Decatur, by then a commodore, defeated a number of Algerian vessels and killed the commander of the Algerian navy. This compelled Algeria to release all of its American hostages, to sign new agreements insuring the safety of American ships, and even to pay a $10 thousand indemnity for its sponsorship of piracy.

Notwithstanding such historic policy victories, the US Government continues to face a terrorist threat nearly 185 years later. The face of most modern terrorism may only dimly recall the days of Barbary pirates, but the fact remains that the United States and many other states continue to face pernicious threats from criminal groups seeking to influence policy and gain concessions through violence. The United States has learned (and occasionally has had to re-learn) important lessons in how to counter the threat.

Our greatest successes against international terrorism have come when we have adhered to the sound policy tenets that Jefferson employed to resolve problems on the Barbary Coast; i.e., when we refuse to make concessions to terrorists, when we isolate and put pressure on states that sponsor terrorism, and when we apply the rule of law to terrorists.

Beginning in the 1960's and continuing today, increasing threats to security forced the United States to strengthen our legal and political tools of counterterrorism. In 1960, a rash of airplane hijackings to Cuba prompted President Kennedy to order tighter security aboard aircraft, including plainclothes law enforcement agents. The US Congress made hijacking, the carrying of concealed weapons aboard aircraft, and the use of weapons to assault, intimidate, or threaten aircrew members federal crimes. Penalties became severe—up to life imprisonment or death; hijacking hoaxes were punishable by 5 years imprisonment.

The United States and other countries have not always played hardball with terrorists, and have not always employed clear counterterrorist policies. Kidnappers released US Ambassador Burke Elbrick when the Brazilian government acceded to the terrorists' demands for a release of prisoners and publication of their manifesto. In April 1970 the US Department of State announced that it was considering payment of ransom as a legitimate policy option in kidnapping incidents. Within a year,

however, the United States announced a "no ransom" policy regarding terrorist demands following successful resolution of a March 1971 kidnapping of US servicemen in Turkey. When the Government of Turkey refused to grant concessions, the kidnappers abandoned the hostages. The terrorists were hunted down, arrested, tried, and convicted. Three were hanged, one imprisoned, and a fifth died in a gunfight with the Turkish police.

The consequences of playing hardball have sometimes proven to be just as deadly for American victims as for terrorists. In 1973, the Palestinian terrorist group Black September seized ten hostages, including US Ambassador Cleo Noel and his Deputy Chief of Mission George Moore in Khartoum, Sudan. The terrorists had a long list of demands: the release of 60 prisoners in Jordan and all Arab women detained in Israel; the release of Sirhan Sirhan (Robert Kennedy’s assassin); and the release of jailed members of Germany’s Baader-Meinhof gang and several other terrorists. The United States and its allies refused to comply, and Black September promptly murdered the two American diplomats. President Richard Nixon later remarked on the tragedy:

> All of us would have liked to have saved the lives of these two very brave men, but they knew and we know that in the event we had paid international blackmail in this way, it would have saved their lives, but it would have endangered the lives of hundreds of others all over the world.

Putting Pressure on State Sponsors

Jefferson’s challenges in North Africa were very early examples of "state" sponsored terrorism. As the power of the United States increased, the frustration of marginal regimes with agendas inimical to those of the United States led to an increased use of terrorism to try to influence US policy, gain concessions, and exact revenge. This phenomenon became particularly disturbing during the Cold War. Absent a major global war between superpowers, some states found terrorism to be a cheap and deadly weapon capable of making America and its allies suffer. They used it to try to force changes in policy and to weaken our resolve on larger issues such as the Middle East peace process. Terrorism is fundamentally undemocratic.

The seizure of the US embassy in Tehran is one of the most blatant examples of a state's use of terrorism to date. It became a watershed event in the history of American counterterrorism, as the United States scrambled ineffectually to coordinate an international response to the hostage dilemma. Almost every evening, television news programs kept count of the number of days they had been held. President Jimmy Carter swore not to leave Washington until the hostages were released, virtually imprisoning himself and reassuring the regime in Tehran that it was influencing US policy. America itself became hostage.

The failed American rescue attempt in 1980 resulted in the tragic deaths of many US servicemen, and the hostages were freed only when the government of Iran saw fit, on the inauguration day of President Ronald Reagan. The US Government had endured a rude wake-up call that it was not well prepared to deal with terrorists or their sponsors, despite its superior economic, diplomatic, political, and military might. Changes were needed.

Military Responses, and Enforcing the Rule of Law

The 1980’s were a bloody decade in terrorism, and were a period of increased state sponsorship. In December 1979, the US Department of State began designating state sponsors of terrorism, designations

that carry harsh penalties in trade and international relations with the United States. Libyan sponsorship of terror, in particular, was pronounced, and Libyan leader Colonel Muammar al-Qaddafi earned the dubious distinction of becoming a lightning rod for American counterterrorism efforts. Notable attacks against the United States and its interests included the bombing of the La Belle Discotheque in West Berlin, a known favorite among US servicemen. The attack was sponsored by Libya. President Reagan ordered American warplanes to attack Libya with surgical strikes in retaliation. The US military had returned "to the shores of Tripoli," and for similar reasons.

New bilateral and multilateral treaties on counterterrorism were negotiated between the United States and a number of nations, notably the United Kingdom, in which references to terrorist crimes as "political offenses" were removed. This reflected awareness in the US counterterrorism community and the Reagan administration that enforcing the rule of law was crucial in countering the terrorist threat. In a speech to the American Bar Association on this subject, Reagan recalled that the Latin characterization of "pirates" was *hotes humani generis*, enemies of the human race. He stated: "We must act together, or unilaterally if necessary, to ensure that terrorists have no sanctuary anywhere."

The Pan Am flight 103 bombing, which killed 259 people on the plane and 11 people on the ground, over Lockerbie, Scotland, was another example of Libyan sponsorship, and one of the deadliest terrorist attacks on an airliner. The aftermath of the bombing, however, provides some hopeful guidelines for cooperation in bringing terrorists to justice. A massive criminal investigation by US and British law enforcement authorities yielded a mountain of evidence that implicated Libya and led to criminal indictments against two Libyan suspects. Years of patience and multinational support from the United Nations and other organizations led to the isolation of Libya and the imposition of harsh sanctions. The two suspects were tried in an independent Scottish court in The Hague.

Other accomplishments in the area of counterterrorism law included the Omnibus Diplomatic Security and Antiterrorism Act of 1986 which, among other provisions, empowered US law enforcement agencies to pursue and apprehend criminals abroad who are wanted for crimes against US citizens. The idea—the so-called "long arm statute"—is simple but critically important: to deny terrorists the sanctuary provided by foreign jurisdictions. In short, they can run, but they can’t hide.

The "full court press" against terrorism that began under Reagan included the creation of a special interagency task force on counterterrorism, headed by then-Vice President George Bush. The Vice Presidential Task Force on Terrorism produced a report in late 1985 that was to have a crucial importance in coordinating more efficient and potent responses to the "new" forms of international terrorism that plague the United States today. With better coordination among US agencies, greater cooperation between the United States and other countries, stronger legislation, and innovative efforts like the Rewards Program, the number of terrorist attacks and terrorist groups began to fall.

The Current Threat

Geography

US citizens and facilities around the world remain targets of choice for terrorists. The economic and international prominence of the United States is often a pretext for resentment and retaliation, perpetrated by non-state groups against non-combatant targets. These groups often turn to violence, wishing to influence public opinion, create havoc, confound US policy, or exact revenge on the superpower they hold responsible for real or perceived injustices. American businesses, property, officials, and citizens are widely dispersed, and are vulnerable to attack by such groups.

Terrorists operate transnationally in the seams of society. For example, while the Japanese terrorist cult Aum Shinrikyo is best known for its attack on the Tokyo subway, it operates worldwide and has a global, not just regional, agenda. Many organizations have cells on different continents; Hizballah and al-Qa'ida are two prominent examples. Western countries, in particular, are attractive to terrorists in a few respects. The civil liberties that are so important in protecting citizens against government intrusion provide freedoms that can insulate groups or individuals wishing harm on our citizens from government scrutiny. These groups frequently establish "legitimate" businesses to fund their terrorist activities. Indeed, terrorists today frequently take advantage of these circumstances to organize, raise money, establish safe houses, and garner sympathy for their cause. Over time, many groups acquire an above ground presence that is then used to build resources for illicit purposes. The United States has enacted legislation that makes fundraising by these groups illegal by prohibiting any financial transactions with them. We are urging our allies to adopt similar measures.

Ideology and Sponsorship

The collapse of the Soviet Union left many of the communist terror cells that plagued the United States during the Cold War without the ideological and financial sponsorship, training, and other support they had enjoyed for many years. Over much of the Cold War, the ideologies of most groups threatening the United States were variations on the same geopolitical doctrine. Today the situation is less monolithic.

For much of the last 40 years, most of the terrorist threat to America came from groups that were enemies of capitalism, Arab nationalists, or Islamic extremists whose leftist inclinations were largely a concession for sponsorship. Although some groups crossed religious, cultural, or political boundaries, each was usually aligned with one of the two great superpowers.

Today, however, we see groups and individuals that are more independent and less accountable, with many having ties to other networks, namely organized crime and narco-trafficking. Motivations are still political, but increasingly incorporate religious or apocalyptic motives as well. Loyalties are often bought with social services or extensive propaganda outreach campaigns. Responses to acts of terrorism today must take into account these motivations and capabilities.

Communist organizations like Germany’s Red Army Faction and Italy’s Red Brigades have declined steadily following the dissolution of the USS.R. and a series of counterterrorist successes. On the other hand, communist terror is by no means dead: Greece’s 17 November group remains one of most active and most elusive terrorist groups in Europe, with not a single member prosecuted since its first attacks in 1974.

Responses to terrorist attacks often focus on blocking sponsorship of the perpetrators, and efforts in this area today are directed at a wider variety of sources than in the past. Many terrorists find sponsorship, or at least tolerance, in sympathetic regimes whose agendas or ideologies are inimical to those of the United States. The US Department of State maintains a list of state sponsors of terrorism that is reviewed continuously. Designation as a state sponsor of terrorism carries harsh sanctions in the United States. Ambassador Michael Sheehan, the Department's Coordinator for Counterterrorism, credits the sanctions with success in pressuring sponsors such as Libya to begin reforming their policies, making life for terrorists more difficult.

Groups like HAMAS are today essentially funded by supporters in the general populace, and raise

money through mosques and social service institutions, as well as from wealthy private benefactors in Saudi Arabia and other states. The Revolutionary Armed Forces of Colombia (FARC) once was backed by the USS.R., but today needs little outside funding because of its lucrative ties to Colombian cocaine production. Terrorists in Afghanistan, Southeast Asia, and other major areas of drug trafficking also are closely linked with the illicit activity. Such links can complicate counterterrorism but also create opportunities for greater cooperation among governments, departments, and agencies in the overall counterterrorism, counterdrug, and general law enforcement efforts.

The booming offshore investment industry, where many terrorist organizations hide their financial activity, makes a diffuse target for the counterterrorism efforts of the intelligence and law enforcement authorities. Although the venerable Swiss banking system remains the place of choice to conduct secret banking, there are more than 60 nations offering a variety of untraceable financial services. Osama bin Laden brought much of his considerable personal wealth to bear in financing the activities of al-Qa'ida. Efforts at defeating him have in part focused on eliminating his access to funds and the profits from his farms and other successful businesses worldwide.

Technology, Tactics, Capabilities

Technology has made extraordinary differences in the terrorist threat and the modalities of response. Gadgets and technologies that were far more primitive or totally unheard of only twenty years ago are now commonplace in all kinds of legal and illegal business. Pagers, cellular phones, facsimiles, laptop computers, encryption equipment, electronic mail, web sites, and other tools of the terrorist trade are so commonly seen in daily life for ordinary people that their use by terrorists does not attract attention. Terrorists have become skilled at employing such equipment to their advantage. Cellular phones, in particular, are well suited to the highly mobile, covert operations of terrorists. The Internet is also being exploited by terrorists. "Cyber-Terror," or electronic attacks on government or civilian computer systems, occurs hundreds of times every day, and is often difficult to distinguish from espionage, hacking, and other threats to US information security.

The US Government, of course, can also exploit the "information superhighway" and other manifestations of the ongoing technology explosion in the fight against terrorism. Cellular phones may be mobile, but they are not immune to tracking and interception, as evidenced by the use of a cellular phone to locate and kill Colombian drug kingpin Pablo Escobar. Terrorists who think high technology guarantees their safety have forgotten the case of Yehya Ayyash, a HAMAS terrorist and master bomb maker who paid the ultimate price in 1996 for his love affair with his cell phone. It exploded in his ear.

Terrorist groups often aim for high body counts and casualties. This is probably the most menacing trend in terrorism today. It is amply evidenced in current intelligence, but more clearly by such attacks as the World Trade Center in 1993, Oklahoma City in 1995, the sarin gas attack on the Tokyo subway in 1995, and the simultaneous explosions in Nairobi and Dar Es-Salaam on August 7, 1998. While the number of international terrorist incidents has decreased in recent years, the number of casualties they inflicted was the largest in history in 1998.

Another concern is the threat of instability in the former Soviet Union and the proliferation of weapons of mass destruction (WMD) throughout the world, often in countries that sponsor terrorism and are avowed enemies of America. The Soviet demise led to the weakening, or outright loss, of legal and military control over conventional and unconventional weapons technology, expertise, and actual hardware that had been part of the Soviet bloc’s war apparatus. This raises grave concerns about terrorists' access to such deadly resources. Much of the counterterrorism community’s effort focuses on

foiling terrorist attempts to access and use chemical, biological, radiological or nuclear (CBRN) weaponry, and on preparing to respond if they succeed.

It is difficult to organize for overseas terrorist incidents and to defeat such disparate threats—but it is by no means impossible. While future terrorists are likely to continue employing reliable tactics like kidnapping, assassination, and bombing, there is widespread consensus among experts that terrorist arsenals and tactics are undergoing a disturbing metamorphosis likely to continue in the decades ahead. The counterterrorism community’s preoccupations in this regard are not mere paranoia—all of these developments have been attempted by terrorists, and most are ongoing. US response capability has been growing and must continue to grow at a pace commensurate with the threat in order to prevent attacks on US interests. We must remain flexible enough to manage and mitigate the effects of an international terrorist incident. Our counterterrorism response must be tailored to meet the challenges presented by the threat to be part of an effective policy.

United States Counterterrorism Policy and Response Capabilities

The United States is well prepared to respond to a terrorist incident overseas, but this has not always been the case. Terrorism in the 1980’s was virulent and illuminated deficiencies in America’s crisis management and response capabilities; for example, the Beirut Marine barracks bombing in 1983, the TWA 847 and Achille Lauro hijackings of 1985, and a host of other significant acts of international terrorism. They motivated President Reagan to establish the Vice President’s Task Force on Terrorism in 1985, which resulted in a recommendation about the development of an Emergency Support Team (EST) to respond to crisis situations overseas and assist the crisis management efforts of both the Chief of Mission and the host government. This recommendation was a core component of National Security Decision Directive 207, signed by President Reagan in January 1986. NSDD 207 provides the foundation for our current crisis response policy.

NSDD 207, entitled "National Program for Combating Terrorism," outlined the basic tenets of our policy for responding to international terrorism. The tenets include the principle of no concessions, applying the rule of law to bring terrorists to justice, pressuring state-sponsors of terrorism, and assisting friendly governments in their efforts to combat terrorism.

Under this framework, the Emergency Support Team (EST) was launched in 1986. The EST was kept very secret, with no unclassified discussion of the team permitted until 1995. However, with the implementation of Presidential Decision Directive 39, the decision was made to de-classify discussion of certain details of the Foreign Emergency Support Team (FEST) and the Domestic Emergency Support Team (DEST) to advertise more adequately our capability and perhaps achieve some deterrence in the process.

In permissive environments (where host governments request assistance), the current response framework is based on supporting the host government in resolving the crisis in its country under the leadership of the US Chief of Mission (COM). The FEST provides the COM and country team with a twenty-four hour crisis management capability and determines the follow-on requirements in conjunction with the host country and the US Country Team. The FEST is designed to meet the requirements of the particular threat and members are drawn from agencies across the US government. Team members advise on such issues as crisis assessment, disabling, investigation, disposal, evacuation, and medical response. In addition, responding to chemical, biological, radiological, or nuclear (CBRN) threats has been a priority for the FEST since the early 1990’s and a special response team for this purpose is in place. While the FEST is advisory only, it assists in a wide range of specialized skills not

usually available overseas. All teams are available for deployment within four hours. Within just one hour of notification, leadership consultations regarding threat assessment and the make-up of the FEST will occur.

In non-permissive environments, the response would be either a military or intelligence operation. However, support may be provided by members of the counterterrorism community, depending on the nature of the threat and the relationship with the affected country.

The State Department has the lead for crisis and consequence management for terrorist incidents overseas. The Foreign Emergency Support Team is coordinated through the Office of the Coordinator for Counterterrorism at DOS.

International crisis management exercises provide important insights in assessing and sharpening our crisis response capability. These exercises include tabletop crisis simulations to assist the leadership of both the United States and foreign governments. Some exercises involve large-scale operations. Most of these simulations and exercises are coordinated either through DOD, or by DOS through the Interagency Working Group on Counterterrorism's Subgroup on Exercises. Constant practice, review, and assessment of capabilities are notable features of the US crisis response framework.

The United States Government has implemented a rather successful interagency structure to respond to terrorist incidents internationally, as outlined in Presidential Decision Directives 39 and 62. The Counterterrorism Security Group (CSG), chaired by the National Security Council (NSC), coordinates the interagency process, under the guidance of the Principals and Deputies Committees of the NSC. The national crisis response structure has remained virtually unchanged since the Vice President's task force and it reacts quickly during a crisis to ensure a thorough US Government response.

It is worth noting that an effective crisis response requires success in many other functional areas. Research and development programs must continue to make advances in protection, detection and disablement technologies, for example. Supplies and materials, medical and non-medical, should be adequately stockpiled and located regionally, proximate to potential venues for terrorism. Training programs must increase the ability of foreign governments and US government missions to handle both crises and their consequences. Finally, in order to achieve comprehensive results, these programs must be adequately funded.

Indeed, responding to terrorist incidents in such a complex environment requires extensive interagency coordination and international cooperation. In large measure, we have been successful in that effort, but major issues and points of controversy remain.

An Examination of Our Current International Response Framework:

Assessment and Prescriptions

It is important to review our crisis management and response procedures regularly and offer critiques. It is easy to be complacent after the kind of progress the United States has made in the area of crisis management and response, but we should avoid such traps.

The FEST has been deployed approximately twelve times since its inception roughly thirteen years ago. In response to the bombings in Nairobi and Dar es Salaam, the FEST was deployed post-incident for the first time. This deployment marked a shift in the organization of the FEST, focusing on

consequence management operations. The Crowe Report of 1999 on the Embassy Bombings in Nairobi and Dar Es Salaam observed that the consequence management efforts of the FEST were ad hoc. Since April 1999, the Office of Counterterrorism at the State Department (S/CT) has been actively developing new guidelines for the FEST, configuring consequence management teams to include personnel in medical relief, search and rescue, public affairs, engineering and building safety. S/CT has also initiated a program to augment any staff at a post that is debilitated or otherwise unable to perform their regular duties.

For the past six years, the US has been fortunate to have a first-class CBRN counterterrorism capability, unmatched internationally. These capabilities are tested at least twice a year in major full field exercises, and the lessons learned during these simulations are used to constantly improve the program. However, deploying our CBRN counterterrorism resources abroad potentially leaves us vulnerable at home. In order to be insulated from domestic attack while deployed elsewhere, we should consider building some redundancy into our capability.

The threat from cyber-terrorism is increasing, and attacks are becoming more frequent. The United States has not yet determined the best way to respond internationally to support a friendly government experiencing cyber or infrastructure attacks. Perhaps a FEST team will need to be designed specifically to counter such attacks; in any case, more attention should be paid to galvanizing technical and infrastructure experts for inclusion on any FEST responding to these types of crises.

The current model of crisis response relies heavily on unilateral action and the relationship we have with the affected foreign government. However, multilateral action might add legitimacy and, in some cases, resources to the response. Coalitions help de-legitimize terrorist action and some cooperation might be valuable, especially in areas of technical assistance and the provision of equipment and supplies. However, proprietary inclinations, resource discrepancies, and the difficulty of a coordinated and rapid response all present major obstacles. Proposals like NATO's WMD Initiative should be implemented, but coordinating any international response to terrorist incidents will require much more time and negotiation. In sum, multilateral efforts at responding to terrorism should be explored, but the obstacles remain formidable.

Under the current crisis management policy the US will not use the FEST without permission from the host country. Efforts are currently under way to formalize relationships for crisis and consequence management. The more bilateral arrangements are negotiated in advance, the smoother the coordinated response in the event of terrorist attack.

One key frustration is the discrepancy between rhetoric and action as it pertains to the level of commitment to building an effective international incident response capability. For example, the FEST aircraft is thirty-seven years old. The Crowe Commission recommended that a new state-of-the-art aircraft be delivered. However, the counterterrorism community cannot agree on either funding or the type of aircraft.

US counterterrorism officials spend a significant amount of time answering congressional inquiries, assisting the GAO, developing crime and counterterrorism reports for the Department of Justice, and testifying before commissions like the Crowe Accountability Review Board, and yet we see little improvement in funding or focused action with regard to our international response mechanism. We are in the insurance business, but good insurance costs money. Right now, there appears to be a discrepancy between rhetoric and action when it comes to counterterrorism. We are making progress, and certainly commitment levels would increase after the next major attack, but our sights should be firmly set on

acquiring those response capabilities *before* the next terrorist incident.

Conclusion

The United States takes a comprehensive approach to international terrorist incident response. In general, the interagency structure has worked well. Expertise is drawn from multiple agencies at all stages of crisis management—planning, preparation, and deployment. Extensive exercise and simulation programs further refine our crisis response mechanism. Our Emergency Support Teams are easily mobilized and organized by task to meet the requirements of the current threat. America's CBRN counterterrorism capabilities are cutting-edge and continue to improve.

Many of these capabilities address changes in the nature of the terrorist threat, but as globalization drives the new transnational terrorism, more must be done. Indeed, greater access to technology, looser structures of terrorist organizations, and stronger ties to international financial and criminal networks all demand that we continue to update our crisis response capability. Bilateral and multilateral approaches to terrorism, the cyber-terrorist threat, and research and development on protective, detection, and disablement technologies all deserve more attention. We must also close the gap between rhetoric and action on international crisis response.

The United States should be proud of the progress it has made, but it is important to realize that we must maintain our readiness to counter the changing face of terrorism and to reject any notion of complacency that would leave us less than fully-equipped to fight it.

Chapter Twelve

Organizing to Combat 21st Century Terrorism

Douglas Menarchik

"Generally, management of the many is the same as management of the few. It is a matter of organization."

Sun Tzu, 400-320 B.C.

"Woe to the government, which, relying on half-hearted politics and a shackled military policy, meets a foe who, like the untamed elements, knows no law other than his own power!"

Clausewitz, *On War*

Introduction

Some scholars may argue organizational structures do not much affect the quality of combating terrorism (CT) decision and policy making. Others, however, argue organizational arrangements do matter, and that scholars should pay attention to the organizational design US Presidents have used. Leadership also plays a central role in ensuring effective policy. Both organization and leadership are critical. Good leadership can overcome poor organizational arrangements, but good organization can seldom overcome poor leadership.

Many scholars date the beginning of modern international terrorism with the multiple hijackings by Palestinian terrorists in the Middle East in 1968-69. At the close of the 20th century, terrorism appears as a ubiquitous theme in American national security documents. Six US administrations of both parties experimented with CT structures and evolved policies that built upon each other, or, at other times, replaced each other. Each administration coped with terrorism somewhat differently—by placing its individual stamp on policy and dealing with the terrorism problem as it existed at the time. Each new administration perched atop a developing terrorism bureaucracy that debated the key issues that shaped that terrorism phenomenon. They debated what priority to give terrorism, whether terrorism was a lesser or greater threat, a criminal or military threat. Some saw terrorism as a threat unto itself; others saw it as an aberrant, violent part of a larger socio-politico-diplomatic problem. Terrorism as a policy issue slowly became part of the bureaucratic landscape.

Terrorism now has become a permanent feature of US national security policy. America has a small fiefdom of subject matter experts, policy and intelligence analysts, and operators all working within discrete organizations dedicated to deal with it. The US now has had over three decades of experience in combating modern international terrorism. The US has experienced a variety of forms of terrorism, extending over a sustained time with varying intensities. This experience provides a body of data and knowledge that scholars can use to make judgments on which structures and policies are more effective and efficient than are others.

This paper will argue that America's experience shows terrorism in the 21st century will continue to warrant a relatively low priority. Despite the recent concern in the US to prepare for "consequence management" of nuclear, chemical, and biological weapons of mass destruction (NBC WMD), the US should continue to focus on dealing with high volume, low-technology terrorism that the US experienced over the past 30 years. US senior leadership should be knowledgeable about terrorism, and involved in high-level policy. All elements of the terrorism community need to be educated and trained in the nuts and bolts of combating terrorism—interagency and international coordination remains the weak link. Within the US terrorism bureaucracy, "stovepiping" (dealing with terrorism problems from the perspective of an agency's narrow viewpoint) must be overcome so that all levels of government interact, coordinate, and deal more effectively with the terrorism problem from the federal, state, and local levels. Currently, state and local interest in terrorism is negligible.

The central focus of this paper is the combating terrorism structure. The agencies must better interconnect, from the national command authority (NCA, meaning the President and the Defense Secretary, who authorize use of military force), through the cabinet and senior terrorism bureaucracy experts, down to the crisis and consequence management units that deal with terrorist incidents.

Key Issues of the Debate on Terrorism

Terrorism's Nature and Threat

Many believe terrorism is a permanent fixture in international politics, but the terrorist threat has been episodic. Levels of international terrorism ranged from less than 200 incidents per year in the 1970s to 666 incidents per year in the 1980s when major Middle Eastern terrorism campaigns rocked US interests world-wide. Terrorism proved to be a global phenomenon, affecting every region. Some regions absorbed higher levels than others (Western Europe, Middle East, South America). Terrorists appeared as individuals, in sub- and transnational groups, and some were state sponsored. The vast majority was low-technology, but the threat of "super" terrorism (terrorism involving nuclear, chemical, or biological (NBC) weapons of mass destruction (WMD)), remained a nagging concern of even the most conservative CT analysts.

Empirical data seemed to support the notion that modern terrorism would decline as a peace dividend of the Cold War's end. Many believed post-Cold War terrorism would stay in a smaller box, and not vary much from what had occurred over the preceding thirty years. Indeed, the US Department of State's data showed international terrorism declined dramatically after 1989 with the collapse of international communism, and the fall of the Soviet Union. High levels of international terrorism returned in 1991, but these incidents were linked to the Gulf War. One of the largest single-year decreases in the number of international terrorist incidents occurred in 1992, as attacks declined to 391. During 1997, there were 304 acts of international terrorism worldwide, an increase of eight from 1996. Over one-third of the attacks occurred in Colombia (90 were low-level pipeline bombings.) The 1997 attacks killed 221 persons and wounded 693 others, as compared to 314 killed and 2,912 wounded in 1996. Of these, seven US citizens were killed and 21 wounded in 1997, down from 23 killed and 510 wounded in 1996. Latin America sustained the highest numbers of incidents with 128, followed by Europe with 52, Eurasia with 42, and the Middle East with 37. The most lethal region overall was the Middle East with 375 killed and 105 wounded, followed by Asia with 271 killed and 73 wounded. Businesses remained the most likely targets (about 75% of the total), and bombing the most likely attack method (175/304 events). In the past twenty years, international terrorist incidents ranged between 434 (1979) to 666 in 1987, dropped precipitously in 1989 to 375, peaked in 1991 to 565 during the Gulf War and dropped to a low of 296 in

1996.

The US was a prime target of international terrorism. The US sustained 25-40% of the blows (Israel at times sustained higher numbers of attacks). Former Secretary of State George Shultz believed America's terrorism problem was "99% overseas." Sub-national and transnational groups were home grown and supported by the Soviets or other state sponsors. Middle East terrorism proved to be especially enduring, sometimes spectacular, virulent, and anti-US. Some believed the Middle East was an engine for international terrorism, and that if the Middle East disputes were resolved, international terrorism would go away.

Are terrorists imitators or innovators, rapidly adaptable or conservative planners? Does the post-Cold War era have a "new" terrorism? Is "super" terrorism a real concern? Terrorists do what works best for them. They stay with tried and tested tactics, weapons, and targets. They have, by and large, used five types of actions (bombing, assaults, kidnappings, hijackings, assassinations, all punishable crimes). Targets in open societies are plentiful. Simple weapons they use tend to achieve their goals. Simple tactics work. Terrorists have proven themselves to be conservative planners. They have little incentive to change. Mass casualties have not been a specific goal of most terrorists. Brian Jenkins, America's first terrorism superstar scholar, often says that terrorists want a lot of people watching, not a lot of people dead. He argues against the trend toward super terrorism and terrorists' use of weapons of mass destruction. Indiscriminate terrorism occasionally resulting in a large number of casualties is not equal to mass terrorism.

In the 1990's, international terrorism declined dramatically, but it became more diverse and ambiguous. For example, progress in the Middle East peace process simply spawned a new set of terrorist players. Other new actors appeared without roots in the established disputes. The post-Cold War world introduced a new strategic environment with proliferation of technology, lucrative targets and openness of more market democracies, and weapons of mass destruction aplenty. Would the post-Cold War era also produce a "new" terrorism—"amateur" terrorists operating on their own or in small, autonomous groups who carried out unsophisticated but very deadly attacks, using home-made weapons, tactics, techniques, and weapons-making knowledge learned from the Internet? Will the 21st century see "super" terrorism (WMD) emerge?

Terrorism's Priority Compared to Other US Security Interests

Terrorism's priority has vacillated between word and deed. The US has often talked about making terrorism a high priority, but has actually failed to do so. Several Administrations had "declared" terrorism a high priority. They often made loud rhetorical statements against terrorism, but had neither the political will, resources, nor policy instruments to back up the rhetoric. Terrorism butted heads with other regional or functional priorities. The Reagan Administration wanted to do more with a proactive policy, but did not, or perhaps could not. The Middle East peace process had a higher priority than punishing terrorists in the region. The situation complicated the decisions to determine which terrorists to attack, and where and how to attack them. The Bush Administration seemed to lessen the priority of terrorism since the threat had significantly lowered in the early 1990's after the collapse of the Soviet Union and resolution of some of the Cold War's toughest, intractable disputes.

With a recent resurgence in terrorism, the Clinton Administration placed a higher priority on homeland defense and international terrorism in its written security documents. Clinton's policy, however, was not proactive nor backed up with sustained resources and action. The domestic threat has remained relatively low, but recent actions by home-grown terrorists (Oklahoma City), and some

imported terrorism (New York Twin Towers), raised questions about the future of homeland defense. The proliferation of technology and WMD, and "loose nukes," raised the interest in, and priority of, "super" terrorism.

Is Terrorism a Legal or Political Issue?

Two questions define this argument. Does terrorism have an irreducible political belief system of its members? Does terrorism affect national security? If the answer to these questions is "yes," then terrorism is defined as a military and political issue. Terrorism from individuals, sub- and transnational groups can threaten important state interests. State sponsors can use terrorist groups to carry out their foreign policy through proxy wars. Military force may be needed to prevent, deter, pre-empt, disrupt, or respond to it.

If the answer to these questions is "no," then terrorism is a legal issue. "Due process" and law enforcement are the drivers for a juridical approach to CT. A terrorist who bombs a building is an arsonist; one who takes hostages is a kidnapper; one who assassinates political leaders is a murderer. Cause or motivation does not make terrorism legitimate by this understanding.

Can a state get international agreement on what constitutes that crime? Extraterritoriality, extending the long-arm of US laws overseas into other states' jurisdiction, remains thorny. Establishing FBI liaison offices overseas is an attempt at international cooperation among police forces. The working relationship between the Departments of Justice and State, and between the US and other states, remain complex.

Law enforcement seems to have won the debate by argument and default. Many Defense Department civilians and senior officers in the US military's conventional forces did not embrace the issue. They accommodated terrorism within the framework of other higher priority security issues. The special operations community held terrorism as a tertiary responsibility.

The military, however, must remain involved in CT policy. In some special domestic cases of terrorism, and many overseas cases, a US military response may be the only response available. Americans need not be reminded that a decade after the 1988 Pan Am 103 bombing, the alleged terrorists remained free, and Libya had been punished only through an ever weakening international economic sanctions regime. Responding to overseas terrorism remains a requirement. Increasingly, the US is relying on stand-off weapons attacks with cruise missiles and precision-guided weapons air delivered. "Super" terrorism and homeland defense further muddy the water. How would law enforcement deal with these issues of strategic import, and what role does DoD play?

DoD is not a Lead Agency in terrorism, but has a primary supporting role in the national security aspects of CT. In 1986, Congress had mandated the US military become "joint." "Jointness" is solving the "stovepipe" problem by having Military Services working together for more integrated policy and operations. "Jointness" worked well for the military. The culture of the military Services began to go "purple." The Army, Navy, Marines, and Air Force worked towards a more effective and efficient joint solution to security problems rather than throwing up "stovepipe" solutions that were rigidly Service-based. The next steps "beyond jointness" are interagency and international "jointness."

Departments and Agencies that perform different functions, that have different cultures, responsibilities, and have a particular way of doing business, but that work to combat terrorism, need to take that long step into "jointness." After interagency "jointness" is international cooperation. If dealing with international terrorism requires international cooperation, then nations must find a way to work

together better.

The old saying, "one man's freedom fighter is another man's terrorist," still has resonance in some places in the world. Developing states, especially, chafe at the hint of intervention into their internal affairs. Often they see terrorists as freedom fighters who are using the only means available to fight against neo-colonialism, great power intervention, and local tyrants.

Some experts believe terrorism is a violent symptom of larger, intractable political issues. For example, some would say Palestinian terrorism resulted from the multi-faceted issues of the Israel-Palestinian dispute. Fixing the terrorism symptom meant first fixing the precipitating cause: Palestinian terrorism would cease once the Israel-Palestinian issue was resolved. Others, however, saw terrorism as a threat in itself, a form of warfare directed against US interests. Terrorism had its own dynamic, its own engine, its own nature, and required tools specifically designed to contain or kill it.

Some developing states view terrorists not as criminals but as freedom fighters, legitimate revolutionaries continuing the popular anti-colonial struggles of the 1950s. The developing world was tolerant of anti-Western violence, and applauded the anti-US, anti-Vietnam violence that racked US and Western cities. Some terrorist groups were media savvy. Western liberals and apologists stressed the terrorists' grievances. Some believed terrorism, as a phenomenon, could not be solved without first solving the "root causes" that spawned them. Western society remained confused about terrorism and its nature. Finding a consensus on a strategy to defeat it was elusive. Few Western leaders tackled the issue head on. Few knew what to do with this complex, multi-dimensional issue. These views still exist today, and hence, international consensus to defeat terrorism remains elusive.

Who's in Charge?

Terrorism touched upon many agencies, especially those involved with national security. Real power in the US government still resides in executive departments that have people, equipment, money, and a capacity to get things done. These departments also tend to do business based on their "culture" and function in government. The military has a different "ethic, mind, and profession" compared to that of a policeman, diplomat, intelligence officer, or political statesman. Getting them to work together to deal with complex, overlapping, and multidimensional issues is the rub. Many agencies scrambled to get a piece of the action and resources that came with it. Terrorism had a cachè and was a sexy subject. Key players were the State Department, DoD, CIA, NSC, Justice/FBI, Transportation/Federal Aviation Administration (FAA), and some others. How to determine who was in charge became a hotly debated topic. Six US Administrations responded with a variety of organizational answers, some more effective and efficient than others. These models included a Cabinet Committee on Terrorism, or a high level Special Situation Group. The power center tended to reside at State or the NSC. Numerous interagency structures were imbedded into and over the existing bureaucracy. Lead Agencies managed terrorist incidents. (State was responsible for overseas terrorism issues; Justice/FBI responsible for domestic terrorism issues; and Transportation/FAA responsible for domestic hijackings. Lead Agency responsibilities are determined by location of the incident.)

The issues of the debate in terrorism were heady, and indeed, caused many headaches. Few issues were resolved fully. How six Administrations played out the issues of the debate follows. My purpose is not to write history, but to use the history to support these points:

--CT should have a relatively low priority
--Senior leadership needs to be trained, educated and involved in CT

--CT structures need to be interconnected from top to bottom with DoD as a Lead Agency. These structures need to be exercised fully with games and simulations to work out the bugs and to plan to deal with NBC/WMD.
--The US should consider preparing for strategic crime by thinking about an Office of Strategic Services-type organization.

Three Decades of CT Organizational Lessons Learned

The issues of the debate played themselves out as six administrations attempted to resolve America's terrorism problem. Each Administration advanced the debate and helped develop US combating terrorism policy, deliberate planning, and crisis response decision-making structures. The policy development path was not linear. One Administration would decide to use diplomatic and economic power instruments as the first line of defense. Later, another would decide to use force to battle terrorists and their sponsors directly. Full policy justification and on-the-shelf operational tools usually lagged behind response needs. America learned how to combat terrorism one incident at a time.

Nixon-Ford: "Setting up against Sub-national and Transnational Terrorism, Over There"

The Nixon Administration became aware of international terrorism after the 1968-69 multiple hijackings in the Middle East. In 1972, terrorists upped the ante with the Munich massacre of Israeli Olympic athletes. This dramatic event showed terrorism a crime of great political importance and effect. Now, terrorists were new actors on the international stage, a hybrid of criminal thuggery, political staging, and media spectacular. These combinations drew the public eye like a magnet.

Most experts then viewed the terrorism landscape as a collage of individual and sub-national groups operating independently within a state, or transnational actions operating across borders, some with support from sponsoring states. In the beginning, few saw the "invisible hand" of states using terrorists as an instrument of their foreign policy. But terrorism almost tripled in the 70s. Sheer volume of terrorist atrocities outraged citizens. They demanded governmental action. The Nixon-Ford Administrations viewed terrorism as a crime, an overseas problem of low priority, and a manifestation of larger political problems.

By the end of the 1970s, the basic elements of an international-oriented combating terrorism policy were established, using a mix of diplomatic, economic, and military power instruments. A traditional timing sequence developed. The CT clock began ticking with the terrorist incident. The CT reaction sequence started with diplomacy and dèmarches, followed by economic sanctions and export/visa controls. US leaders considered a hostage rescue if negotiations failed, and, as a last resort, military force to retaliate.

At the organizational level, CT was a low-key, low-profile bureaucracy composed of "part-time" experts taken from other fields. Terrorism lacked priority and real interest among the top leaders. While structures were in place with high-sounding titles, the real bureaucracy operated at a Deputy Assistant Secretary level.

In general, the Nixon-Ford Administrations viewed terrorism as criminal activity conducted largely by sub-national and transnational terrorists. The US would not negotiate with criminals. America's declared policy was to not give in to terrorists' demands and to urge this policy on other states. The US believed that to give in to terrorists' demands would only further the terrorists' cause and invite further terrorism.

While the declared policy of "no concessions" weathered the strain of time, in actual practice, many governments in the 1970s negotiated the freeing of hostages on a regular basis, including the US. Later, the Nixon Administration began developing policy that called for the punishment of states that supported terrorists. The Nixon-Ford Administration emphasized the international dimension of international terrorism and used agreements and organizations to combat it, and increased protection of US facilities abroad. Diplomacy and anti-terrorism were primary tools to punish and thwart terrorists abroad.

Nixon-Ford: High-level Cabinet Structure

Nixon established an intelligence committee on terrorism in 1972, shortly after the Olympics' Munich Massacre by Black September terrorists. The committee's purpose was to work with the international community to analyze the terrorist threat and to deter it. Key agencies were the CIA, FBI, and the State Department. The Deputy Assistant Secretary of State for Near East/South Asia headed the committee. From this point on, the State Department would continue to play a central role in international terrorism.

Nixon also formed a Cabinet Committee on Terrorism (CCT) in 1972 consisting of State (Chairman), Defense, Treasury, Transportation, CIA, FBI, the Attorney General, the US UN Ambassador, the NSC Adviser, and the President's domestic affairs adviser. The Committee's purpose was to direct the fight against terrorism by having intelligence collected, providing physical protection, and evaluating CT programs in order to make recommendations.

The group had little real interest in the terrorism problem. They met only once, and had disbanded by 1977. Using the President's cabinet "buddies," political experts, and friends was helpful to direct the big picture, but the President was not square in the middle of terrorism policy leadership, a vital missing link. Despite the lofty level, terrorism did not have a high priority in the Administration. The CCT was not linked to the President, who is a necessary element for using force and setting the proper priority for terrorism. The CCT was to brief the President from "time-to-time." Since the CCT met only once, it accomplished nothing.

The concept of a President using his Cabinet to direct the fight against terrorism is reasonable only if the threat is deemed to be high enough and important enough to take the Cabinet's time. The terrorism threat did not reach that level in the 1970s until the Iran Hostage Crisis. The Cabinet-level committee certainly could have provided the political weight to government action, but individual members did not have the interest, and collectively, the group was too diverse, perhaps too large, to deal with the lower priority that terrorism had on the President's real agenda.

The CCT, however, was important in that it elevated the rhetorical or declared importance of terrorism to the penultimate level. Equally important was the bureaucratic level of a CCT Working Group chaired by a Special Assistant to the Secretary of State. He was the first national level coordinator for CT. His rank was Ambassador. This rank gave the Coordinator some bureaucratic clout within the terrorism community and a doorway to the Secretary of State. The position further established the central role for the State Department with its focus on anti-US terrorism abroad, and international terrorism as the key threat.

The Coordinator, however, had a small staff (6), no real budget, and lacked rank to impose his will upon the other departments that participated. The group functioned well, meeting over 100 times during the Nixon-Ford years. As terrorism grew as an issue and expanded into other bureaus, the size of the

working group doubled, from about ten members in the early 1970s to almost two dozen by the mid-to-late 1970s. The size of the group became too cumbersome, and therefore too difficult to focus for effective and efficient deliberate planning.

Figure 1. The Nixon-Ford High-level Cabinet Model

CCT

CCT Working Group (Intelligence Committee chaired by State)
Coordinator

Departments

Carter: "Solve the Larger Political Problem, Deal With and Contain Terrorist Incidents, and Terrorism Goes Away. Oops!"

Carter looked at the underlying causes of sub- and transnational terrorism, and saw unresolved international political issues as the cause. For example, the Palestinian problem, as a component of the Arab-Israeli dispute, had spawned numerous anti-Israel and anti-US groups. These groups were either based in Arab states, supported by them and operating from within their borders, or were transnational groups operating across international borders, some with state sponsorship.

Carter agreed economic instruments, such as sanctions and export/visa controls, stiffened diplomatic dèmarches. But Carter wanted to put military teeth into the international mix by creating a more robust hostage rescue capability, a capability that had some bite and reach, however nascent in its development. The Israelis had demonstrated such a capability in their well-executed and lucky hostage rescue at Entebbe in 1976, and German border guards were successful in their paramilitary take-down of a skyjacked airliner in Mogadishu, Somalia, in 1977. By the end of the decade, the US would have its own version of this capability.

Carter built upon and modified the Nixon-Ford combating terrorism policy legacy. He placed more emphasis on the political character and "warlike" nature of terrorism, less on its criminality. What started out for Carter as political terrorism—a smorgasbord of sub-national, transnational groups, some with state sponsorship, willing to operate against US and allied interests—ended as "microcosmic" warfare, a teapot war, that scalded the Carter Presidency in the end. Carter lurched from "soft" power instruments to "hard" military power by the end of his Administration. The operational failure of Desert One, the attempted rescue of American hostages in Iran in 1980, demonstrated the effects and consequences of terrorism on US national security interests and the personal CT politics of Presidents. The Carter Administration became consumed with international terrorism during the Iranian Hostage Crisis of 1979-1980. That crisis went a long way toward bringing down the Administration. By 1980, Carter had reversed course and was dealing with terrorism as a problem unto itself. But he played in the Iranian Hostage Crisis end game without fully developed force and policy options. He paid the ultimate political price.

Carter’s Special Coordinating Committee for Terrorism

Carter killed Nixon-Ford’s CCT concept. His Presidential Review Memorandum 30 called for a review of organization and its capabilities. He wanted to link CT to the White House and the Presidency through the NSC. This key feature would move the President closer to the decision-making process that

led to use of force. Linking the CT bureaucracy to the NSC and the White House focused attention and centralized decision-making, policy, operational management, and intelligence in one location near the center of American power. The President was the center of CT strategic decision making, with the NSC linking the terrorism experts to the operators, intelligence, and policy makers. The NSC was the primary unit for coordination of deliberate policy planning and high-level crisis management.

The positive aspect of this arrangement was that the White House was very much in control of CT and would get full credit for success. The obvious negative was that the President would get full blame for failure. It was a high-risk, White House-dominated organizational structure in a high-risk business. Carter set up a Special Coordinating Committee (SCC), chaired by the NSC Adviser. The Committee consisted of secretaries from State, Defense, the DCI, and the Chairman, JCS. The SCC resolved jurisdictional disputes, assured coordination, and dealt with high-level terrorism crises. The title of the group is important. The term "coordinating" clearly implies "hands-on" management and leadership involvement. Nixon’s CCT, on the other hand, implied a more removed oversight function. Nixon’s structure may have had too little senior leadership involvement. Carter’s structure may have had too much.

In addition, the SCC supervised a Senior Interagency Executive Committee (EC) that handled the routine day-to-day terrorism affairs and dealt with "high-level" CT crisis management. The EC consisted of Assistant Secretaries from State (Chairman), Justice (vice chairman), DoD, Energy, Transportation, Treasury, and representatives from CIA, FBI, the Joint Staff, and the NSC. By 1977, the EC’s huge size proved cumbersome. The Assistant Secretary-level was sufficiently high to push difficult issues into the SCC for adjudication. In theory, the combination of the SCC and EC was adequate to deal with most CT issues. Sustaining the power and punch of the committee, however, proved too difficult. This group only tangentially connected to CT operations in the crisis response management structure. This made CT operations twice removed from senior leadership. Senior leadership was somewhat disconnected from operations.

Positioned under the EC was an interagency Terrorism Working Group (TWG) that plugged into the working bureaucracies. It was an all-inclusive sounding board, touching all elements within the terrorism community. As a debating society of deputy assistant secretaries, colonels, and GS-15s, it could sharpen its terrorism policy. The TWG became too large to be effective.

In 1978, the TWG organized into six standing committees: A Research and Development Committee focused on anti-terrorism research; a Domestic Security Policy Committee looked at maintaining the US border and monitored US domestic vulnerability; a Foreign Security Policy Committee focused on overseas issues; a Contingency Planning and Crisis Management Committee made plans for incident management training; a Public Information Committee; and an International Initiatives Committee that developed multilateral aspects of CT. This reorganization allowed the TWG to focus its deliberate planning on discrete issues.

Lead agencies were responsible for crisis management. Where the incident occurred resolved theoretically the "who’s in charge" question. State dealt with terrorism abroad, Justice/FBI with domestic terrorism, and Transportation/FAA with domestic hijackings. State, Justice, and Transportation were Departments headed by Secretaries who had clout by being the President’s designated executives. These departments also possessed human and material resources to get things done. Under the Carter CT organization, the Lead Agencies and the SCC managed crises and were supported by the EC and TWG. The DoD was a supporting organization, but it needed NCA authority for action. The President and/or the Defense Secretary were the only authorized persons who could deploy US military forces, not the

State and Justice Secretaries. How to get the military into all aspects of coordination, deliberate planning, and crisis response management proved difficult.

The operational planning often came from covert/clandestine military and intelligence operational organizations that were "stovepiped" due to their secrecy and compartmented origins and natures. The "stovepipes" did not interact easily with other elements of CT policy and intelligence. Without the full vetting, head-to-head negotiating necessary to prepare and select options, the US made mistakes. Military operational failure was separate from policy failure. Goldwater-Nichols would come a decade later, and from Congress, to help fix "joint" operational planning and execution. But stovepipes between special operations forces and conventional forces would remain, even after Goldwater-Nichols. Cultures within cultures, secrecy, "bad blood," and operational entanglements precluded proper operational and policy coordination. Political disaster resulted.

Figure 2. Carter's Special Coordinating Committee Model

SCC (NSC Adviser as Chair + State, DoD, DCI, CJCS--cabinet secretary-level)

EC (Asst. Secretary-level, State Chairs)

Terrorism Working Group (Coordination + Deliberate Planning)

Lead Agencies (Crisis Management)

All three Administrations in the 1970s had experienced a sharp increase in terrorist activity directed against US interests overseas, and focused on how to deal with state-sponsored terrorism. The reason for the increase was that states that sponsored terrorism were providing funding, weaponry, intelligence, sanctuary, international protection and diplomatic cover, and training for proxy terrorist groups, including their own intelligence agents. The US supported democracies that were attempting to deal with terrorists as criminals. Some states sponsored terrorism, and other states had neither the capability nor capacity to deal with groups operating within their borders (Lebanon for example). To deal with this reality, Carter added a military dimension and used force to rescue hostages in Iran. This embryonic military capability came into being in 1977, and by 1980, the State Department's Director for Combating Terrorism had designed a counter-terrorism strategy that used the military for tactical responses and rescues. The FBI also developed a domestic force response capability if negotiations failed.

Despite the clear advances made during the Carter years, many in the terrorism bureaucracy believed major problems persisted in the overall program. From the policy side, different agencies had different responsibilities and viewed the terrorism problem only from their agency's perspective. The Justice Department viewed terrorism as an international criminal activity. The State Department viewed the problem as one of either state-sponsorship, or saw terrorism as a collage of political thugs, some of whom had state sponsors, all as part of a larger diplomatic dispute. State therefore pushed for additional diplomatic resources to resolve the problems. The DoD was reluctant to engage the terrorism issue since it diverted resources from the Soviet conventional and nuclear military threat.

Terrorism continued to have a lesser priority than other regional and functional issues, such as the Middle East peace process, arms control, maintaining alliances, and managing the global Soviet threat. On the operational side, policy makers and military forces involved in combating terrorism were often drawn from other related operational areas. They had neither the experience, nor the necessary training to gain the confidence of their more conventionally minded leadership. Combating terrorism was not a

career for most, but an additional duty, a stopping post on the way to more main-stream career jobs.

Counterterrorist operations were always risky. Despite great successes at Entebbe and Mogadishu, other failures had tremendous political down-sides, such as the Egyptian commando failure in Larnaca, Cyprus in 1978, and the US failure at Desert One in 1980. Few of the key operators and policy leaders personally exercised the policy options in a terrorism war game.

While deliberate policy planning continued, crisis response management systems did not function adequately. Few of the top leaders were ever brought into the complex decision-making structures until a live crisis forced their hand. Deputy Assistant-level players were usually the highest-ranking participants in CT war games, simulations, and exercises. A competent, capable, and exercised second-level management structure did not yet exist in the late 1970s. The CT policy makers "ad hoc-ed" responses during a crisis. These policy makers were not trained in their field. Intelligence remained diversified among the CIA, State, and Defense, and within the bowels of the FBI and Justice Department for domestic terrorism. The right hand still did not talk adequately to the left.

By May 1980, the Carter Administration had developed a full-blown combating terrorism program with elements that addressed the increased international terrorism threat. The program called for adherence to international agreements on terrorism, support for the no concessions policy, security for US facilities abroad, increased response capability for weapons of mass destruction, and improved intelligence and interagency coordination.

Carter saw the terrorism problem tied to other international issues, and not as a threat only to the US. The Middle East problems, the core of which was the Arab-Israel dispute, spawned numerous and unrelenting terrorism campaigns against Israel, the US and the West in general. Rather than focus on terrorism as a discrete issue, the Carter Administration focused on solving the Arab-Israel dispute. He believed solving that chronic sickness would solve the terrorism symptom. Carter proved only partially correct.

The Iran Hostage Crisis and Desert One

In 1979, another Middle East problem arose far to the East of the Levant, the Iran Hostage Crisis. This event overshadowed all else in Carter’s combating terrorism program. Carter found that although he did not want the terrorism problem, the terrorist problem wanted him. In 1976, Carter had focused on sub- and transnational terrorism in Latin/South America, Europe, and the Middle East. He had viewed terrorism as crime and a law enforcement issue.

The Iranian Hostage Crisis smashed into his Administration’s limited policy and operational options. Iran was a state that sponsored its own terrorism for its own purposes. It was a revolutionary power unto itself, operating independently, the very embodiment of the quote from Clausewitz used in the introduction of this chapter. The US needed a well-honed military option and did not have one. The failed rescue attempt was a benchmark in the evolution of US CT policy. The flow was simple: the US developed policies and organizations to deal with terrorism. State sponsors took on the US and did not flinch at diplomatic or economic pressures. A military rescue attempt failed while the world watched. The military operational failure helped topple a sitting US President.

The Desert One benchmark showed that state sponsors were real. At the end of the 70s, state-sponsored terrorism became an unambiguous threat to US interests, consumed Carter, and helped bring his Administration down. A role had been created that needed a hero. That hero would be Ronald

Reagan.

Reagan: "In your Face CT"

Reagan replaced Carter in dramatic political fashion and dramatically raised the rhetorical level of US CT policy. Reagan saw communists behind each terrorist, and increasingly saw state-sponsorship as the heart of the problem. The declared policy jumped ahead of actual capability. Reagan took on the terrorists early, dealt with the sub- and transnational groups, and increasingly went after state-sponsors. He elevated the priority of terrorism, surrounded himself with like-minded senior leaders and experts, and established an aggressive proactive CT program that included a military power projection capability.

Reagan willingly accepted the CT tools Carter bequeathed him: economic sanctions as a means to punish state sponsors and the hostage rescue capability. But Reagan upped the ante. He said the US would use all appropriate means at its disposal to respond to terrorism abroad. This unambiguous policy placed the military on the front lines, and threatened military actions to respond to terrorist incidents.

While the terrorism rhetoric-levels were high for the incoming President, the deliberate planning system in the government bureaucracy and within the terrorism community lagged behind. The praxis of actual policy limped behind the fire-breathing rhetoric of the declared policy.

With Reagan's terrorism interests and political clout, his Administration's views reshaped US policy. Terrorism became warfare. Diplomacy, economic sanctions, and military force were the traditional tools of coercion and would be used to cut out terrorism.

By the 1980s, the US and the Western allies had mustered the political will to act forcefully against terrorists. In addition to a "no concessions" policy, the West added two pillars that essentially remain in force today. First, no state that practiced or supported terrorism would do so without consequences. Second, Western states would take action to identify and track terrorists, and bring them to justice.

Getting good intelligence complicated policy implementation. No intelligence is more difficult to collect than CT intelligence. Technical and strategic intelligence collection is important, but individual terrorists do not show up on satellite imagery. "Inside" intelligence gathering is a dangerous, tedious business, perhaps the most difficult in HUMINT operations. In the 1980s, the US and Western countries shared intelligence and began to concentrate on developing special committees devoted to CT and international cooperation. Focusing on the practical aspects of CT, such as border, visa, and travel control, paid off. Several European terrorist groups, such as the Italian Red Brigades, the German Red Army Fraction, the French Direct Action, were defeated and ceased to exist.

Conventional military forces were primary options, but special operations within the military and intelligence "black" world would be used to disrupt, pre-empt, prevent, deter, and respond to terrorist campaigns. Special operations, however, seemed too risky. Reagan picked his targets carefully, choosing Qaddafi and Libya, not Syria and Iran, using conventional forces as primary tools during the Libyan air strikes in 1986 and the Egyptian airliner take-down, and interagency police-military-intelligence forces for the capture of Fawaz Unis.

Reagan set the tone for his Administration's overall response to the increased terrorism campaigns against the US with his campaign promise for swift and effective retribution to punish states that sponsored terrorism. Reagan took on a high combating terrorism profile by using sharp, at times screeching, rhetoric. The tough talk played well with the American public. Reagan used such barbed

quips like "terrorists can run but they can't hide." Whereas Carter learned overtime and through experience to place a high emphasis on state-sponsored terrorism, Reagan came to office ready to act. He saw terrorism as a threat unto itself, sponsored by the Soviets and others who would do the US harm. Reagan would not compromise with them. He placed a high emphasis on state-sponsorship, using the State Department to push the diplomatic buttons to keep terrorists at an arm's length from our borders, and emphasized crisis response management.

By April 1984, Reagan codified his new combating terrorism policy instructions by authorizing direct action missions and pre-emption. Important players in the security decision-making arena agreed terrorism was political violence and state-sponsored terrorism was warfare. Secretary of State George Shultz, NSC Adviser Robert MacFarlane, and CIA Director William Casey shared these basic views with Reagan. They had a convergence of opinion within their respective security organizations. The policy makers agreed on a proactive course of action, but they needed the bureaucracies' forces, operators, and intelligence support to implement it.

Their attention was indeed focused, because the mid-1980s saw the highest levels of international terrorism activity directed at US interests abroad. The terrorism campaigns in 1985-87 exhibited volume, quality, as well as numerous "spectaculars." The gap between declared (rhetorical) priorities and actual priorities embarrassed Reagan several times in the early-mid 1980s. For example, the US appeared helpless when terrorists hijacked TWA 847 and murdered an American sailor.

Reagan had enough. In January 1986, George Bush's Task Force on Combating Terrorism published its findings and set up a comprehensive combating terrorism policy. The recommendations were incorporated into America's national security documents that directed strategic action. The Task Force codified existing policies and structures, and established a small interagency group to oversee non-crisis operations and activities. The small group brought together the key combating terrorism players from policy, intelligence, and operations in order to exchange information, think through policy and crisis responses, and to prepare their principals for key decisions falling into the terrorism arena. The Task Force also authorized the use of military force and set up a combating terrorism intelligence fusion center at CIA and a National Intelligence Officer on Terrorism. Good ideas that had languished in the terrorism bureaucracy surfaced, were vetted, and if found worthy, incorporated into the deliberate planning and crisis response management structures.

U.S combating terrorism programs appeared to be at the ready to deal with terrorism problems. The Task Force supported use of military force to prevent, deter, pre-empt, disrupt, and respond to terrorism. Leaders were in place, fuming, and primed to act. Terrorism had a sufficiently high priority in the government, leaders had a full assortment of hard and soft power instruments to use, and the military could be used if necessary to go after terrorists and their state-sponsors.

Action finally followed rhetoric and policy planning. US air forces struck Libyan targets in April 1986 following the killing by Libyan intelligence agents of Americans in Germany. The US forced down an Egyptian airliner carrying Abu al-Abbas, the head of a Palestinian terrorist group responsible for the commandeering of the *Achille Lauro* cruise liner and murder of an American citizen. And a CIA-FBI-military sting operation "snatched" the Palestinian terrorist, Fawaz Uniz, in international waters.

Suddenly, the high water mark of US CT proactive policy ended abruptly—Iran-Contra stopped the heady proactive policy in its tracks. But the unintended effects and consequences of Iran-Contra improved US CT capabilities in the long run.

Iran-Contra and Its Effects on US CT Policy and Organizational Structures

Desert One ended the rising tide of U.S CT policy in the 1970s. The Iran-Contra Affair, likewise, stopped Reagan's aggressive proactive measures in their tracks, turned them over to the bureaucracy, and reversed direction. With the senior executives occupied with the politics of the scandal, second-level executives worked a low-key, in the weeds, police work approach that had very positive, unintended consequences, not expected by the hard liners, and surprising to the moderates in the terrorism bureaucracy.

Iran-Contra placed the CT bureaucracy in a high political profile under the lights of the media. State Department officials and the NSC Legal Counsel began attending terrorism interagency working group meetings as "watchdogs." Many believed Iran-Contra had been run out of the White House. Post Iran-Contra politics diminished the NSC's role in CT. The "cowboys" in the White House were considered "loose cannons" that needed monitoring and to be taken to the wood shed.

Interagency and international coordination became more difficult consequently. Dealing with other countries on issues of international terrorism became more difficult. Other states did not trust US CT policy since the US appeared to violate its own hard line "no concessions" policies, and appeared to trade weapons for hostages. One CT Coordinator believed that when the US strayed from its "no concessions" policy by trading arms for hostages in Iran, terrorists kidnapped more Americans. When the US reaffirmed its long-standing, but often-discarded policy, terrorists eventually freed US hostages.

As a result of Iran-Contra, the US terrorism bureaucracy shifted its emphasis to judicial responses. George Shultz and the State Department took charge. Shultz re-oriented the proactive approach. He placed a trusted manager to run the NSC CT office. Ambassador Robert McNamara replaced the fired Lt. Colonel Oliver North. Shultz's trusted Terrorism Coordinator Jerry Bremer, using State as a power base, refocused the interagency working group on terrorism towards a diplomatic, judicial/legal program. The US retained its no concessions policy, apologized internationally for having deviated from it, and focused on an extraterritorial judicial approach to identify, track, apprehend, and prosecute terrorists wherever found.

Since the terrorism-as-warfare approach had been stopped in its tracks by Iran-Contra, the judicial approach became the front line by default, at least for a while. This raised many issues for the law enforcement community. They had not yet prepared the policy and operational ground work. The Justice Department and FBI were not yet ready to become international policemen. Nor was the international community ready for this action. Unresolved issues surfaced. How could the US enforce its laws overseas? It could not. Extraterritoriality became a hot issue again. How would the State Department deal with FBI "attachès" overseas, and where did State's Regional Security Officers responsibilities end and the FBI agents begin? How would the CIA deal with gathering overseas intelligence and gathering evidence? Intelligence is not equal to evidence in a court of law. As a result of Iran-Contra, the Reagan Administration contributed a non-military approach to combating terrorism, the opposite of what it had intended.

Reagan's Special Situation Group Model

Reagan created, early in his first term, a Special Situation Group (SSG). The Vice President was the chairman of the group, while State, Defense, Director of Central Intelligence, NSC Adviser, Chairman of the JCS, and the President's Counselor were its members. In many ways, the SSG looked and functioned

like Carter's SCC, except the Vice President chaired it, and the President's Counselor attended. Despite these changes, the SSG's early experiences were negative.

The kidnapping in Italy of US Brigadier General Dozier by Red Brigade terrorists showed the SSG to be a poor coordinator and integrator of US policy and operations. The "who's in charge?" issue quickly manifested itself. Dozier was a military officer. DoD and the military had a vested emotional interest in an effective resolution of the kidnapping. The Lead Agency concept placed State at the top perch and diplomacy as the primary tool. But State was not part of the national command authorities (President and Defense Secretary) that were needed to authorize the use of military force. The "NCA" problem had to be dealt with in order to use force overseas. The State Department, as a lead agency and centerpiece for overseas terrorism, had to be connected to the NCA when force options were prepared. The State/DoD squabbling tangled the chain of command.

In 1982, Reagan provided new CT instructions that codified the Lead Agency Concept. Reagan did away with the Executive Committee. He set up an interagency terrorism management organization under the SSG. The Terrorism Standing Group (TSG) was chaired by the NSC, and it included DoD, State, CIA, FBI, and FEMA. The Terrorism Standing Group provided the SSG operational support and interagency coordination during a terrorism incident. The Lead Agencies managed the incident, as in the Carter Administration. This arrangement gave the NCA command and control of military forces.

Beneath the TSG stood the Interdepartmental Group on Terrorism (IG/T). State chaired the IG/T. The IG/T brought together the agencies for deliberate planning and policy development. Lead Agencies still managed the details of terrorism incidents. This overall structure provided operational and policy support to the highest interagency committee, the SSG, that had ultimate responsibility to respond to the terrorism incident. This structure put the White House in the middle of CT, and plugged the President in as much as he wanted to be plugged into CT. This structure solved the NCA problem of using force overseas. Reagan and the Secretary of Defense now had a military response capability and a crisis response management system to manage terrorist incidents.

By April 1984, Reagan's new policy orientation had developed pre-emption as an option. The US would not necessarily stand by to take the terrorist's first blow. Reagan was surrounded by friends who thought like he did. Secretary of State Shultz also saw terrorism as political violence and state sponsored terrorism as warfare. Ambassador Robert Oakley became his Director of CT. Oakley replaced Ambassador Sayre who believed terrorism was a police matter in the main, not a military matter in general. Sayre looked for legal bases of action, not extra-legal.

In addition, Robert MacFarlane, who became Reagan's NSC Adviser near the end of Reagan's first term, also supported a proactive CT policy. CIA Director William Casey provided the intelligence arm and clandestine/covert action capability. The importance of this leadership alignment is striking. The central power authorities in CT were in alignment with the President. Their natural interests in terrorism matched that of the President. Core leadership and national priorities aligned. In addition, a series of terrorism campaigns directed against the US lent urgency for US action.

Bush: Low-key CT

George Bush inherited much of the Reagan Administration's apparatus. He moved quickly to put his own stamp on CT policy and organizations. He found that process easy. Bush was the most educated President on the subject of terrorism. He had lengthy high-level, first-hand experience. Bush had headed Reagan's Terrorism Task Force. He personally endorsed its recommendations, shaped its findings, and

was a central figure in institutionalizing them. He did so over the heads of some of the heavy weights in the Reagan Administration that opposed parts of the package. In addition, some elements of the terrorism bureaucracy opposed some of the recommendations because they perceived losing their control and power.

The policy Bush inherited played well in the strategic environment of lessening levels of terrorism. Bush saw terrorism as criminality more than warfare. He retained the "no concessions" policy, continued emphasis on international cooperation, and maintained the extraterritoriality aspects that came to the fore in the latter days of the Reagan Administration. He championed "snatch" operations to bring terrorists and drug dealers to justice. "Snatch" operations were considered for Noreiga prior to "Just Cause," the invasion of Panama, and in Lebanon, to rescue the hostages.

He took a more low-keyed approach, as suggested by his Secretary of State, James Baker. He retained the standing interagency group on terrorism. Bush de-emphasized terrorism during his Administration. Even during the Desert Shield/Storm operations, he saw the increased threat of terrorism and the hostage taking within Iraq ("human shields") as part of the larger strategic problem of impending war with Iraq. Bush focused on the main battle, the war with Iraq, and dealt with terrorism as a side issue. Bush's NSC adviser, Brent Scowcroft, said terrorism never really came up on the White House radar screen during the Bush Administration except during the release of the hostages in Lebanon. Low-key, sustained diplomatic talks obtained the hostages' release, not military force, or arms-for-hostages swaps. In the post-Cold War era, holding hostages had become a liability for terrorists in Lebanon. Scowcroft, even less interested in terrorism as a strategic threat than Baker, kept terrorism out of the White House.

During his tenure, however, Bush significantly advanced the US government's policy and operational capabilities *if* the government had to deal with terrorism. US policy documents began to display more robust statements concerning terrorism. These documents, such as the National Security Strategy, National Military Strategy, Defense Guidance, and others, used proactive terms such as covert operations to prevent, deter, pre-empt, disrupt, and respond. The action verbs captured the full range of action that a President needed to throttle terrorists, when, and how, he wanted to. Now, operations had to catch up to policy justification. These documents provided the bureaucracy the necessary tools to create policy, operational, and intelligence programs to manage the terrorism problem.

The White House down played the importance of the hostages in Lebanon and allowed a capable terrorism bureaucracy to manage that long-fused, slow burning crisis. Whereas the hostages' families had played an important role in affecting the emotional state of Reagan in the 1980s, and to an extent, Bush, as Vice President, this did not happen again in the early 1990s. Most importantly, US diplomacy very effectively managed international relations during Desert Shield/Storm, including its responses to terrorist threats by Iraqi agents and pro-Iraqi sympathizers worldwide.

While levels of international terrorism increased during the Gulf War, they quickly returned to the much lower post-Cold War levels. Bush had showed terrorists he was not soft on them. He did so by authorizing military and police "snatch" operations. Despite some international backlash, these operations proved popular with the American people and put drug dealers and terrorists on notice they could not escape the long arm of US law. US policy and operations had caught up finally with Reagan's rhetoric that "terrorists can run but they can't hide."

Figure 3. Bush's CT Organization

Principal's Committee

Deputy's Committee

IG/T

Lead Agency

Clinton: "It's the Economy . . . . Oh My! Super- and Homeland Terrorism!

Early on, the Clinton Administration continued to experience fewer incidents of international terrorism. Clinton continued Bush's lower profile strategy. The Clinton Administration, against the advice of some terrorism experts and concerned Congressmen, downgraded the American bureaucracy set up to fight terrorism in the 1980s. Supporters say the lowered terrorism statistics did not warrant maintaining the CT vigilance and infrastructure. But without American leadership in international terrorism, and American leadership to refocus US law enforcement agencies domestically on domestic terrorism, the US would lag behind a reinvigorated terrorism campaign.

Critics of Clinton's CT program might say that he dumbed down, deemphasized, defunded, and deconstructed CT—lowered the CT rank structure, lowered the priority, diverted funds to other priorities, and combined agencies that submerged terrorism as a lesser player among other important issues, like drugs and crime. Indeed, both the State Department and NSC staffs merged terrorism into "global issue" units. The argument was that a more senior official in charge of a larger, more powerful bureaucracy would have more clout and be able to push better the CT agenda in the strategic circle where the "big boys" played, allocated resources, set priorities, and made decisions. Detractors of this move believed CT had been watered down to the point that an already weakened voice had been lost amongst the other voices in the bureau.

The face of terrorism in the 90s may be changing that reality. Prior to the World Trade Center bombing in February 1993, Justice/FBI and other law enforcement officials had been complacent about major international terrorist incidents in the US, In fact, US domestic terrorism had remained at relatively low levels in the 60s through 80s while other democratic states were used as a terrorist battleground. Both the Bush and Clinton Administrations had weakened America's first line of defense against international terrorism by cutting budgets, losing experts (lack of a viable terrorism career field forced many SMEs to return to other functional careers) and refocusing national attention (it's the economy stupid!).

These actions weakened America's international defenses against terrorism. International cooperation slackened as Western states lost patience with sanctions, and only paid lip service to CT agreements. Local and state law enforcement remained poorly trained and equipped to thwart terrorist activity in the US. The Immigration and Naturalization Service (INS) was overwhelmed, under equipped, and under trained to handle the border infiltration of terrorists, criminals, and drug traffickers. The Federal Emergency Management Agency (FEMA) had become more effective in dealing with natural disasters, but it was not yet equipped to deal with massive casualties and the aftermath of sustained terrorists attacks.

A host of strategic issues then dominated the landscape, and terrorism became a second fiddle issue. Clinton, however, used US conventional forces to retaliate against Iraq when Iraqi agents attempted to assassinate former President Bush during Bush's visit to Kuwait after the Gulf War, and against Osama bin Laden in Afghanistan and Sudan for his support for bombing U.S embassies in Africa. Cruise

missiles and air-delivered precision-guided munitions can be effective retaliation against state sponsors and transnational groups when they can be found and precisely targeted. The use of precision weapons against terrorists is becoming reasonable and practical. Clinton's use of them against Iraq, Afghanistan, and Sudan showed that terrorists can be found and hit with conventional weapons anywhere in the world. Detailed intelligence for targeting and timing are essential prerequisites, but both should improve as technology enhances precision, and international cooperation improves intelligence collection. Clinton's "tomahawk strategy" (using Tomahawk cruise missiles to attack terrorists) is technology and intelligence limited.

Post-Cold War terrorism issues began to manifest themselves and Clinton took them on as policy, operational, and intelligence issues. The "new" terrorism of the 1990s really boiled down to amateur domestic terrorists and new transnational terrorist groups such as Osama bin Laden's, and a heightened WMD threat. Indeed, the Defense Intelligence Agency's assessment placed proliferation of NBC/WMD and other key technologies as the greatest direct threat to US interests worldwide. The major transnational threats to the US were ranked by Defense Intelligence Agency as proliferation of WMD/technology, terrorism, narcotics, and other international crime, in that order. Deputy Defense Secretary Hamre said three hoax anthrax attacks occurred in the US in 1998, and about 100 in 1999. That is disturbing information, reminding one of W. H. Auden's phrase in *Gare du Midi*:

Figure 4. Clinton's CT Structure

Principal's Committee

Deputies Committee

Interdepartmental Group/Terrorism

Lead Agency

"clutching a little case, he walks out briskly to infect a city [w]hose terrible future may have just arrived."

The threat from terrorists having weapons of mass destruction was the first priority while the rise of domestic terrorism and the threat to the US homeland increasingly became a prominent issue. The terrorist profile appeared to be changing according to some terrorism specialists. The new groups appeared to be ad hoc and seemingly autonomous, not connected to established, known groups. Some groups were becoming nationalistic and religious, less political and left wing, willing to engage in higher levels of indiscriminant killing.

What Is To Be Done?

US structure and policy were adequate to combat the relatively low threats from terrorism during the 1960-1990s. Are they adequate to thwart the "new" terrorism of the early 21st century? The "new" terrorism indicates an increase in domestic terrorism that has implications for antiterrorism in the US and potentially dramatic implications for "super" terrrorism and consequence management.

How threatening will the "new" domestic terrorism be in the US and what could the US do about it anyway? The FBI seems adequately prepared to deal with slightly higher levels of domestic terrorism. How many resources to spend to protect US facilities is the larger implication. Oklahoma City

experienced a very destructive bombing of a federal building. Protecting all the federal buildings in the US would be very expensive—some say about $350,000 would be necessary to properly and reasonably protect a large complex. The bombing of the Twin Towers complex in New York City is even more problematic. Privately owned property offers an endless target list. Hence, antiterrorism becomes a very expensive proposition in the US Counterterrorism seems more cost effective. No matter how much one protects at the federal, state, local levels, terrorists can always find a "softer" target. US law enforcement can not find all the Timothy McVeigh's in America. To defend all, one defends nothing. Therefore, it is necessary for the US to focus its resources.

US CT organizations that deal with the "new" terrorism of the 21st century should not start from scratch, but build on what has worked. We also should learn from what has not worked well. New situations in the 21st century will necessitate some original thinking.

Structure: Inter-Connect the NCA-Special Cabinet-level Committee (with Terrorism Support Group), CT Bureaucracies, Lead Agencies and Crisis Response/Consequence Management

"Who's in charge?" was the key issue pertinent to this article. While CT never had a high national security priority, it frequently engaged US Presidents in pop-up crises. Presidents may not have wanted terrorism, but terrorists wanted them.

Any CT organization and program must have adequate links and connections to the NCA (for use of military force). The NCA is the head—it provides the leadership, vision, and direction. The NCA must be connected robustly to a group of Department Secretaries who adjudicate, shape, sort out the high-level key issues, oversee an effective deliberate planning process and CRM. (This group is not situation-based, but a standing group that focuses on CT as a phenomenon, not a crisis point.) The President will get full credit and blame for counter-terrorism actions. The President should be interested and involved in CT. He must lead.

The small Secretaries CT group should be connected to a small group of Assistant Secretary-level specialists that perch atop the CT bureaucracy. A Secretary or a small group of Secretaries must carry the President's torch for him, be his surrogate and impose his will on the government. The Secretary-level group must be small, interested, involved, and meet regularly enough to be effective. Its purpose is to adjudicate and sort out interdepartmental squabbles.

Who adjudicates policy battles among competing Secretaries who are theoretically of equal status is the main problem. Because Secretaries are chosen by the President—by definition strong willed people, with strong positions, strongly held—some *one* must be able to break ties, separate fights, and make decisions. Neither the Vice President nor a NSC Advisor has proven effective in this role yet. Neither the Vice President nor the NSC Adviser is suited for this role since they command no operational bureaucracy. The President must be engaged and break ties. Leaders lead. The "buck stops here" with the President. He must lead when his secretaries get entangled in the thickets of terrorism.

The Assistant Secretary-level support to the Secretaries' Group is critical. It prepares the Secretaries for important decisions. The support group is the heavy hitter in the CT bureaucracy and pushes the senior leadership's agenda. It imposes the President's and the Secretaries' will. The Assistant Secretary CT Working Group connects to the deliberate planning interagency groups and department groups in the CT bureaucracies down to the departments' CRM organization. NCA must be at the head with senior NSC staffers, department heads in State, DoD, Justice/FBI, CIA, and Transportation, who have real power with people, equipment, funding, and the will to get things done.

The structure must connect from top to bottom, the bottom being the crisis response forces. Feet of clay can topple an iron statue. Desert One was a crisis response operational failure at the low end. It torpedoed Carter's policy. Carter's organization was adequate in structure and policy tools at the high end, but it lacked training, education, equipment, and long-range CT operational experience to pull off the coup de main in Iran.

Can this CT structure deal with higher levels of domestic terrorism and "super" terrorism? I believe the existing domestic CT structures will deal effectively with higher levels of domestic terrorism. US law enforcement has been effective in dealing with the first thirty years of domestic terrorism, and it is equipped to deal with slightly increased levels. The US may be tempted to try to "antiterrorism" everything. The US is an open society and should remain that way. High profile and high value facilities need sound protection, but the country cannot afford to go overboard. A $350,000 price tag to protect adequately a single building complex from terrorist attack demonstrates the case of the endless black hole. Terrorists simply can go to the next undefended target. It is cheaper to eliminate the terrorists than to try to provide antiterrorism protection to America.

Existing CT structures also are beginning to deal with the consequence management of the aftermath of an NBC WMD attack in the US. What is obviously lacking is the executive branches connecting to the state and local police and emergency response systems. Justice and FBI are working to improve the historically strained relations between federal, state, and local police. The Defense Department must work in that direction also. The National Guard and perhaps the Reserve Component are situated best to deal with these connections. Many in the military and elsewhere will say that funds should be increased to local and state agencies to deal with these problems. In the long run, that may be true. Dealing with the consequences of a NBC WMD attack in the US does, and will continue to, outstrip state and local resources. It outstrips the current resources of the US military, but the US military has the manpower, training, organization, and equipment to begin dealing with consequence management problems on this scale.

I advocate a go slow, deliberate planning process that uses existing resources, rather than throw money and human resources at creating new structures. These type of proposals have gone a bridge too far and spend resources not justified by the existing threat. Deliberate planning? Yes. Some organizational restructuring to deal with consequence management? Yes. But "no" to new government agencies that create and supervise an elaborate federal-state-local empire of fall-out shelters and consequence management units. All of this could be done by an enhanced FEMA and state-local emergencies units, supplemented with National Guard and Reserve Component resources.

DoD as a "Lead Agency"

The DoD currently is not a Lead Agency. It supports other Lead Agencies. The DoD should be in the lead any time force is used. The problem occurs in the handoff from the Lead Agency to the DoD: the State-to-DoD handoff occurs overseas; the Justice-to-DoD handoff occurs in America under very specific circumstances now, but perhaps more expansion will occur in response to super terrorism and homeland defense; the Transportation-to-DoD handoff also occurs in very specific cases. Most of the likely cases admittedly are overseas. The DoD also should know what went on before the terrorist incident, and should be responsible for the consequences of DoD actions after the fact. By placing DoD in a supporting CT role, the US puts its preparation, selection, and execution of a force response option at a disadvantage.

If DoD were actively engaged in the deliberate planning and crisis response management from the beginning, and if DoD allocated the appropriate mix of conventional and unconventional assets from the beginning, then force use and covert/clandestine responses could be executed better. As of now, the only Lead Agency "troops" are FBI agents. Policy and intelligence needs the operators, the "soldiers," to execute force responses. Military operations, conventional and special, need to be coordinated better with CIA's covert/clandestine capabilities.

The operators (FBI, CIA, and the military) currently are removed too far from the deliberate planning phase and not properly integrated into the crisis response structures. The current task force concept addresses the deliberate planning and intelligence functions, but does not adequately combine overt/covert/clandestine operational capabilities. Dovetailing police expertise into this mix further complicates the process, but all are necessary for a seamless operation. DoD/military should be in a lead agency role to coordinate military support of diplomatic and economic sanctions, as well as force option preparation and execution. The DoD/military should consider using both conventional forces and special operations.

Terrorism Czar? Too Far!

In the 1980s, some analysts gave some thought to creating a terrorism czar, an all-powerful person who spoke for the President, consolidated power, and took action against terrorists near and afar. The US has had an Education Czar, and a Drug Czar. Why not a Terrorism Czar? Czars have proven effective in being a proponent for an issue, but Czars have no "troops." Without the dedicated funds, soldiers, police, and intelligence assets that are imbedded in the departments, a Czar cannot conduct a war on terrorism, or anything else. A Czar can be engaged only in a clanging of "symbols" as an advocate.

In the mid-1980s, the Departments mightily opposed the creation of a Terrorism Czar. They did not want to lose their power to an outside agency. Besides, use of military power had clearly defined command and control arrangements. The only legitimate authority that could order the use of military force was the National Command Authority. Likewise, the command and control of law enforcement and police forces in the US is delegated among local, state, and federal police forces. Few of them are specifically trained for domestic counter-terrorism operations. However, the vast majority of past terrorism incidents have been armed assaults, murder, bombings, arson, kidnapping, and hijackings. Police deal with these crimes.

A Terrorism Czar cannot even look good on paper. This idea was a dead letter from the start. Some believe that Lt. Col. Oliver North's position was to be an NSC Terrorism Czar that brought the reins of power into the NSC and White House. In May 1999, Clinton appointed a national coordinator for security, infrastructure protection, and counter-terrorism to "bring the full force of all our resources to bear swiftly and effectively." No harm comes by designating a Czar a White House aide, but one should not put faith in Czars. Real power, as noted earlier, resides in executive departments that have people and resources to get things done, not just talk.

Leadership: Maintain and Sustain Senior Leadership Involvement and Interest in Terrorism

As shown previously, recent US terrorism history exposes the lack of sustained senior leadership involvement, interest, and understanding of the terrorism phenomenon. George Bush was the only sitting President who came to office with first-hand experience in CT. He had headed the Vice President's Task Force on Combating Terrorism and chaired Reagan's SSG for crises. He dealt personally with several of the hostage families during the extended Lebanon CT crises in the mid-1980s. He was the exception.

The others learned CT on the job.

In most cases, Presidents gave terrorism a higher rhetorical/declaratory priority than actual national security priority. Leaders "talked the talk but did not walk the walk," calculatedly so. Presidents and cabinet members for the most part did not get involved in a terrorism incident unless it generated a national security crisis. By that time, it was usually reactive, too late except for reprisals or revenge.

Revenge is not a motive that democrats can embrace too long. Carter's Iran Hostage Crisis is the classic case. Reagan personally may have become caught up in the emotions swirling around the hostage families. But that reaction was typical human reaction, and not necessarily a criticism. During the Entebbe crisis, Israeli Prime Minister Yitzhak Rabin likewise got caught up with the emotion of the events. George Bush did also when he dealt with the wife of slain Lt. Col. Higgins over the Christmas holidays in 1986. Criticism is appropriate only when poor national security decisions stem from those meetings. Emotions that produce precipitous action can back fire.

Reagan and members of his cabinet, especially State, CIA, and his NSC adviser, became very involved and set the tone for aggressive CT policy, intelligence, and operations. Often, the policy and response options were inadequately developed and practiced to be efficient and effective. But the President's options for CT policy and operations were adequate, if not plentiful. Reagan had a full complement of options for action, backed up with policy justification that had the stamp of the CT deliberate planning process. He could do almost anything he wanted overseas operationally—deter, prevent, pre-empt, disrupt, or respond.

Reagan had national assets at his beck and call, but less than full international cooperation. Most Europeans, other than Britain's Prime Minister Margaret Thatcher, shied away from draconian, forceful measures. They believed the US were cowboys at heart, with a quick trigger finger, too much power to keep holstered.

Reagan did not have the homeland adequately covered—Shultz had convinced him the threat was overseas, not here. Homeland protection would have to wait until the major attacks on US soil in the 1990s during the Clinton years.

Interagency and International Training and Education for Senior Leaders and CT Careerists

US senior leaders just do not "get" terrorism. They do not understand that terrorism is not only criminal violence, but also a new kind of warfare. While senior leaders tend to avoid exercises, war games, and simulations like the plague, they need to be brought into exercises specifically designed to deal with a range of terrorism issues. For example, "super" terrorism-based exercises quickly would teach senior officials that terrorism is only one aspect of that particular crisis. WMD pushes the issue to the NCA whether the NCA wants to deal with it or not.

Little terrorism expertise exists above the Assistant Secretary-level. When crises occur, the understanding of the issue and the complexities of the response quickly transcend real-world experiences of senior leaders. Terrorism decision-making, therefore, is "stovepiped," and stops at the Assistant Secretary level. Education and training on the mechanics of the organizational structure, by way of exercises, would show how the system and policy works, or does not work.

Strong senior leadership and appropriate structures are critical for effective CT policy formulation and implementation. But so are the people who run the bureaucracies—these people need to be trained

and educated in what they do. Career CT specialists—what a concept!

Many in the CT bureaucracy must come together for deliberate planning. Interagency CT training and education would be helpful as a prerequisite to key CT positions. Many policy makers and operators only come together to resolve a terrorism incident during a crisis. Crisis management response training on war games, simulations, and case studies would be helpful before managing an actual event. A crisis situation is not the place to learn the nature of the terrorism business. Terrorism Task Force training exercises, similar to the joint task force training performed for policy makers and operators at the Armed Forces Staff College in Norfolk, could be developed and made mandatory for those preparing to enter the CT bureaucracy.

Terrorism education would further enhance the understanding of the broad issues of terrorism and how the terrorism phenomenon links to the larger strategic environment. Terrorism studies, and other "military operations other than war" subjects, should be part of the curriculum in government educational and training institutions. Senior professional military education now treats terrorism as an "elective." CT specialists must be educated to think strategically and to understand strategic crime, like terrorism.

Many argue the CT community is far ahead of other functional areas (such are drug trafficking and international crime) in interagency and international cooperation. Their argument is persuasive; however, much is yet to be done. Substantial progress has been made over the three decades. A terrorism career field exists, of a sort. Those who are in it enjoy it. This career path does not, however, lead to the more senior positions within the departments. Many terrorism experts still transfer in from other fields. Terrorism has been a tertiary responsibility in many, if not most, departments. Personnel are added-on when terrorism is hot, then removed when the terrorism light switch is turned off.

Functional terrorism expertise and power tend to stay within the terrorism "stovepipe" community. Terrorism often does not transfer well into other functional/regional areas. Terrorism as a field is still quite new. Terrorism experts often are not promoted outside their career fields. US leadership, at all levels, needs training and education, war games, and crisis decision exercises on terrorism.

Prepare for Strategic Crime. Think about an Alternative Organizational Structure—"Office of Strategic Services"

Strategic crime is the combined lawlessness of organized crime, drug trafficking, and terrorism of a quantity and quality that threatens a range of security interests of a state. Clear and present dangers stem from organized crime, drug trafficking, terrorism, and low-intensity conflict. These "non-traditional" security dangers will threaten the US and its allies more than the real or imagined dangers of conventional, interstate war. Russia, Colombia, and many of the states in the former Soviet Union are examples of states affected by strategic crime. These are friends and strategic partners of the US. Their well-being affects US interests.

Physical violence and intimidation against people and illegal appropriation of property undermine the political, economic, social, and psychological well-being of a state. Strategic crime attacks the state’s rule of law and legitimate power. Market democracy consists of rule of the people through their elected officials, and the citizens’ use of a free market to produce and sell goods. Strategic crime attacks market democracy by creating a perverse, parallel economy and loss of citizens’ confidence in government. If people believe the state cannot or will not provide security from strategic crime, strategic crime can undermine the foundations of market democracy. Strategic crime kills and intimidates people, takes their

property, and corrupts, perverts, and distorts democratic institutions and the free market. Strategic crime destroys the social contract between citizens and the state. Strategic crime is a threat to important interests of some of America's friends and strategic partners and some of the emerging democracies around the world. Strategic crime, therefore, is an important interest of the US.

Strategic crime is the cumulative effect of criminal violence and terrorism that can have strategic consequences. Bureaucratically, it would involve domestic and overseas agencies, criminal and national security agencies, law enforcement and military. Strategic crime occurs domestically and overseas, but it involves both law enforcement and the military. Strategic crime is departmental, interagency, and international.

Today, different US security systems deal independently with organized crime, drug trafficking, and terrorism. Combining these functions would focus attention, centralize, streamline, and provide synergy. The World War II Office of Strategic Services (OSS) model, updated to 21st century democratic standards, is a model that would work. A Terrorism OSS would be an office built upon existing departments and functions, combining law enforcement and military, CIA, DIA, State INR, FBI intelligence, and existing policy organizations in State, DOJ, NSC, DoD, DEA, etc., for policy. The organization would straddle existing units, bring necessary expertise together, draw upon the vast public domain services available, and operate to thwart strategic crime.

The idea for a Terrorism OSS, a separate, "purple" service that combines intelligence and operations and works under strict policy guidance of the NCA sounds intriguing. It solves the centralized authority problem and connects to the NCA. Focus of effort, centralization of planning, and CRM are contained in one tight organization. While the OSS worked well in World War II, trying this on for size in an America that already questions "black" operations in the CIA may be a bridge too far. America may not tolerate another narrowly focused covert organization with guns. There would be internal bureaucratic obstacles as well, not just spiritual and ethical. The military Services already view Special Operations as a Fifth Service. Another Service would seem to clutter an already cluttered table of players.

CT Priority: Keep CT Low-key

US Presidents have gotten US CT priority about right. In general, US CT has a relatively low national security priority. Thus far, terrorism has been primarily a nuisance, not a serious national threat. Terrorism priority has fluctuated. Like terrorism itself, terrorism's priority has been like a light switch. Presidents gave CT a high priority during an incident, then almost forgot about it during a lull. Reagan had the most proactive CT policy and sustained a counter-terrorism track record. Bush had arguably the most low-key, methodical approach.

The US has not set a high priority for terrorism, but has been able to sustain action against individuals, sub- and transnational groups, and especially state sponsors. State sponsors in many ways are easier for the US to target because a state has people, territory, and resources in a set boundary. Targeting sponsors may be the key. Individuals and sub- and transnational groups are more elusive, more difficult to grab hold, and more difficult to target. Does the "new" terrorism, increased domestic terrorism or "super" terrorism, dramatically affect CT's low priority?

Prepare for High-Technology NBC Terrorism Quietly and Effectively, but Focus on Low-Technology Terrorism

Super terrorism has been a threat to the US for some time. Terrorists seldom have used nuclear,

chemical, or biological weapons. There may be no "Dr. No" now, but when? The issue is not *if*, but *when* a NBC attack occurs in America. The US can sustain a terrorist attack that inflicts high casualties, but a mass casualties attack threatens strategic interests, perhaps vital interests. If conservative estimates are wrong that terrorism will not take a radical turn toward super terrorism, the consequences are too great a risk for America to take. CT organization needs to be responsive to the threat.

Super terrorism, indeed, appears to be beyond the CT bureaucracies' current capabilities. Super terrorism is a major strategic issue requiring the full attention of the NCA and agencies beyond the CT bureaucracy. That fact has been demonstrated in numerous exercises and games designed for terrorism experts to play. This training has exposed the need to quickly elevate the crisis to the NCA for action and resolution. Currently, no government agency exists to cope with the full magnitude of the repercussions of such a NBC high-tech attack, including its psychological and physical costs. Tacit agreements between Western governments and state sponsors of terrorism assume state sponsors will restrain their attacks to nuisance attacks, not strategic attacks. If terrorist attacks go strategic, such as the World Trade Center bombing could have been, then the US likely would respond strategically. Some day, a new radical state may decide to launch such an attack by using WMD however built and delivered to American soil. As noted earlier in this paper, over 100 anthrax hoaxes occurred in the US in 1999. Further, the links with international drug traffickers and organized crime provide a global network that can move money and information, fashion technology creatively, transport black market commodities, and avoid discovery by an overwhelmed police system. America can be proud of the quiet and effective ways its CT bureaucracy has planned and coordinated consequence management and disease control measures. These federal networks touch state and local emergency groups that deal with the problem at the site of the incident.

For example, the 1999 US National Security Strategy document, like several of its earlier predecessors, gives high priority to "super" terrorism and WMD in general. Terrorism experts now are suggesting the creation of a large organization to deal with "catastrophic" terrorism. They are putting organizational flesh to the nuclear arguments Dr. Robert Kupperman peddled for years. Their thesis is that a WMD attack on the US is now more likely than at any time in the past. America is prepared for "conventional" terrorism, but not super terrorism with NBC WMD attacks. They posit a focused approach on homeland defense and a massive organizational restructuring to deal with super terrorism and its potentially catastrophic consequences.

Their superstructure for super terrorism is overblown. The superstructure they envision is predicated on an imagined threat, not a demonstrated terrorist capability. They also have under-estimated greatly capabilities that already exist in FEMA, the US military, the Reserve Component and National Guard, and federal, state, and local law enforcement and emergency agencies. The homeland defense issue, with its emphasis on anti-terrorism, will deal with a major part super terrorism and consequence management.

Most terrorists use low technology. Likewise, many government responses use low technology. These methods of operations will continue. The terrorism that is predicted to occur in the emerging democracies will replicate what happened in the West in the 1960s and 1970s. Terrorists in emerging democracies likely will use the same weapons, tactics, and targets that worked against Western democracies. "Amateur" terrorism will be a nuisance to our friends just like it was a nuisance, but not a strategic threat, to the US. The picture of terrorism in the West in the 1960s and 70s will be visited upon the emerging market democracies early in the 21st century.

The West and the US should help those democracies that seek help to deal with a terrorism problem on their turf that is sure to come. Some of these countries will be open to Western help. Helping them

will help the US and the West. Training, education, police, and military assistance are necessary on a large scale. The CT bureaucracies should place the proper weight on helping others deal with their terrorism problem in the region, before that regional terrorism affects US interests. An ounce of prevention is worth a pound of cure.

A beefed up FBI should be able to handle the projected increase in domestic terrorism. America may have dozens of Tim McVeighs. The federal-state-local police cannot prevent all those who would do America ill, but they can do a credible job while maintaining America values.

Recruit More HUMINT and Language Experts

The US has fantastic SIGINT (technology) capabilities that contribute mightily to effective CT. But in the 21st century, US intelligence must broaden and deepen considerably. America's traditional national security focus on old enemies created a narrow intelligence expertise that we now must transcend. The US needs allies in the emerging democracies that were in the intelligence darkness only a few years before. Human intelligence, regional expertise, and language capabilities are essential for future CT operations. Satellites cannot track individual terrorists. Human sources are needed to penetrate terrorist organizations. Good intelligence is crucial to CT operations. The kind of tactical intelligence CT needs is derived from HUMINT. The US has many German, French, Russian speakers, etc., and regional experts. America needs to develop similar expertise in the emerging democracies, becoming knowledgeable of their politics and their languages. This infrastructure may be very costly, but is a fungible capability with interagency reach.

Think about instituting international "finger" squads. A finger squad is a group of policemen, military special operations, clandestine/covert intelligence operators whose mission is to track and identify terrorists. At the appropriate time, the finger squad turns the fugitives over to local authorities for apprehension and arrest. European police used this method during the hey-days of European terrorism. This method was effective, but politically risky. In a way, the Clinton Administration already used this approach with ad hoc specialized task forces. For example, the interagency Osama bin Laden task force collects data, monitors, and tracks his groups. This task force essentially focuses on intelligence, but could be combined with an operational component. Putting an operational point on this concept is needed.

Epilogue: A Twenty-First Century Terrorism Agenda for the United States

Jay Davis

I looked up terrorism as a useful way to begin this epilogue. I found two definitions. The first is the "systematic use of violence, fear or intimidation to achieve an end." And what's important about that is the word "systematic." Think about the varying terrorist experiences we have had recently—Osama bin Laden, Aum Shinrikyo, and others. You could characterize them as systematic, not single events, so it is useful to look at that definition. The second definition is equally interesting. It is "an atmosphere of threat or violence," not threat or violence itself, but an atmosphere of threat or violence, which implies a terrorist, after an initial event, might be very successful at propagating terrorism by more subtle means. So I thought that this is a good place to start. It is important in both of these definitions to understand that achieving the ends is not necessarily the same as the means to a terrorist. Sometimes we focus on the means, sometimes it is useful to step back and focus on the ends.

The things I would like to discuss include:

- My perception on why this particular subject comes to us now;
- What the US government is doing in general;
- What the Defense Threat Reduction Agency (DTRA) is doing, in specific; and
- What has been recommended recently; and then
- Can we derive a 21st Century Agenda for terrorism by examining a couple of "cases."

When I talk to my own agency, or when I talk outside, I say that I think of terrorism like I do law and business. There are general theories, but there are also case studies. And you are only as good as the number of case studies you have done. In fact, when you go out in the field, your ability to achieve your goal is drawn on all the theories, but also all the lessons you learn from the scenarios; there are the operators who have worked with the case studies that have the advantage. So, I have a fairly strong affiliation for the law and business approach to understanding things.

How did this come to us, this concern about terrorists now? There are two interesting, slightly different answers to that. The first is our dominant military might, both nuclear and conventional, particularly with the high-tech capabilities. Our intelligence and command and communication capabilities basically deter any classical confrontation. No one is going to be brainless enough to come up against us one-on-one, straight on. And that, in fact, invites an asymmetric response—coming at the United States on its terms is perhaps one of the dumbest things you can possibly do. Therefore, the terrorist option (playing the game by other rules) is very attractive to adversaries. That is one function driving our current concern.

The second driver is that our societal and economic success, perhaps overbearing success, is both to some extent ending, which is a driver for bad behavior and a negative reaction to our role and presence in other parts of the world. It is easy to forget that because we like ourselves so much, we forget that the rest of the world does not necessarily like us. A particular problem couples both of these to some extent since we have become the last resort for other world leaders. Depending on how you interpret this, it is sometimes good and sometimes insane. We have become the last resort for other world leaders in reaction to ethnic violence and political aggrandizement. In general, the reaction to these problems leaves us with an unsatisfactory peace. We need only to look at Iraq, Bosnia, Kosovo, and other places to

see examples of how unsatisfactory the peace is, which makes us enemies and invites reprisals against us based on frustration. So, in fact, our success at being world cop has led to the problem. It is particularly important to realize that in some of these places, after all, we have gone in on fairly high ethical grounds whereas most of the people there just wanted to get on with the business of killing each other. So our interruption was not welcome by either side. Terrorism comes to us partly because we have a lot of functions, capabilities, and roles—more than anyone else.

What are we doing in response? We are doing the typical American response. It is one of the things we are good at it—we are proceeding in parallel with many different things at once and not necessarily bringing them together. We have a great many programs that address the military and civilian sectors (some flawed). We are seeking technological solutions in all the categories we possibly can. And, we are fighting for the control of purses. Since I am an operator, I tend to notice that we tend to fight for that control without operationalizing the whole solution. But in retrospect, as a student of this and an operator, what is good is that unlike in other times in our past, we do not seem to be deluding ourselves by looking for a "silver bullet." That is the good news. In fact, we are admitting that this is pretty difficult, multi-component, multi-spectral problem. So, no one is hawking a single solution to the problem. If go back and look at our fifty-year past and the Cold War, that is our usual approach. Whatever difficulties may have started this problem, they will not necessarily cure it. We may not be looking for one solution because no one wants the assignment for it, which is also a universal problem. If you walk the halls of the Pentagon, the problem of how to counter terrorism or how to do consequence management or how to gather intelligence to keep from having to do the other two is not "number one" on anybody's list. That is not a bad thing; it is a realistic thing. Everyone has lots of other assignments. Thus, the fact that no one is searching for a "silver bullet" solution may be because no one wants to get out front on this issue.

What is my agency (DTRA) doing, it is fair to ask. We are full-spectrum partners in this; we do both non-proliferation and counterproliferation; we play offense and defense. We execute the inspections, the arms control processes for every treaty that the US is a partner to, in a very classical sense. We execute the Cooperative Threat Reduction Program, which dismantles systems in the former Soviet Union to try to prevent the migration of hardware and intellectual capabilities to other states, although we do not have a human dimension. We are not paying people, scientists, and engineers to keep from migrating, but we do work to keep hardware from disappearing. We run the export controls business for the Department of Defense and the study of the more difficult problem of patterns of commercial transactions that might tell you if someone is acquiring the capabilities to produce weapons of destruction. Those are the pieces of my agency that deal with non-proliferation, keeping weapons of mass destruction out of the hands of bad actors.

On the counterproliferation side, it tends more towards the sharp end of the stick. We shape the chemical and biological program for our warfighters. We are very, very busily working for the battle CINCs, providing exercises to test this notion of how the CINCs work in the warfighting environment and how we help a CINC respond to civilian needs—not a simple problem. Again, we come back to my emphasis on exercises. We run a lot of exercises that shape our doctrine and try to suggest operational changes. In that area, we are coordinating actions well in advance of some the organizations in both the Department and Defense Advanced Research Projects Agency to try to handle the full spectrum of research and development in the national security area to deal with this threat. We have a major role in nuclear deterrence. And we provide important derivative training in consequence management. It is useful to remember that for fifty years we have not quite practiced how to do consequence management, and we need to determine what from the nuclear era is applicable to the biological or chemical environment. Finally, in the counterproliferation business, we run full spectrum—from sensors to define

what a facility is doing, to suggesting what the attack modality might be, to modeling and simulation, to deliberate planning, to emergency response, and so on. Floating over the top of all of this organization is a set of system studies to define new programs, required roles, capabilities, and responsibilities.

I think a very fundamental point I want to make is this notion of what has been recommended or what to put on a counterterrorist agenda. Some of you are obviously going to ask me questions about the recommendations of the Commission regarding how the government should be organized to handle counterterrorism. That Commission has recommended we should have a czar, a senior person on the National Security Council, more coordination across agencies, perhaps more committees, and others ways of coordinating the counterterrorist efforts and other inevitable recommendations. There is a recommendation for an Assistant Secretary and related organizational changes. I do not want to minimize that effort. But what I would like to do in response to the topic I was given for this epilogue is to suggest a somewhat different agenda for responding to this problem.

I said I believe in case studies or working problems. I will give you two that are very much worth our time in thinking through counterterrorism. The first of these, familiar to all in the military, is the Goldwater-Nichols Act. The Goldwater-Nichols Act drew a very, very fundamental watershed distinction. It said that the Services would organize, train, and equip and that the CINCs would do joint planning, exercises, and execution. The difficulty we have with counterterrorism is there is a food-fight going on within the Pentagon and in town, that is primarily focused on the issues of organization, training, and equipment. That seems to be where the money is, that seems to be where the publicity is; it is a procurement activity; these are pretty much 8-5 jobs. I am an operator; I am not used to making money my job. My concern, my function—having been an emergency response manager in my past—is what I call the "Organizational Chart When We Go to War." The "Organization Chart for War" is different than the "8-5 Organizational Chart." My concern in the counterterrorist area is how we focus on what in the Goldwater Nichols Act were the planning, exercising, and execution responsibilities of the CINCs. In general, "The Organizational Chart When We Go to War" is different; it is leaner and certainly a lot more practiced. The Marines have a useful expression—"muscle memory." If we are going to do one of these things for real, we need to have "muscle memory."

How do we concentrate on joint planning and execution? How do we see the difference; how do we find the gaps and fill them? It is important to realize that counterterrorism is not going to war. The CINCs go to war when their plans are complete; that is their job. They make a plan and then they push off. The difficulty is that in terrorism, war is thrust on you; it comes to you. So the CINCs get the plans top-down and in fact, in counterterrorism and consequence management, you are going to have to plan bottom-up. You are going to have to react to the event given to you. The planning—the calls for help—flow *up* the chain, not down—or up *then* down the chain. It is going to be driven by resource needs of the real event, not by planning in advance.

We do not have a good model for this. We need to derive one. We certainly have to practice, but it differs from the organization, training, and equipment role quite clearly. We have figured out how to organize, train, and equip, but we have not yet figured out how to work out models, how we let, in a remarkable way, the civilian world drive the military. We talk a lot about military assistance to civilian first responders, but I think we have problems with that. We need to work on educating the civilian world in advance of an event and the Service counterparts on how this would work. So my interest, and our (DTRA'S) interest to some extent, is in scenario development that lets us practice, practice, practice. That is why, as I said earlier, DTRA is working with Special Operations Command on exercises today; we are working with Joint Forces Command tomorrow on an exercise in their area; and in the European Command responding to terrorist activity. Again, the intent is to find out how we drive this thing from

the bottom-up. It is useful to remember that we have a headstart here. We have been doing this for fifty years. But there, the military owned the problem; in this case the military does not own the problem; the civilian sector is a strong player.

There is another concern. The difference between acting versus reacting, or the counterterrorism versus consequence management pieces. The harder part of this will be moving to the anticipatory step and understanding the intelligence taskings and means that will give us advance warning of these events so we are not just in the reactive mode. If we are driven to be reactive, we can be the best reactors in the world and still not necessarily be successful, if we are forced to play a passive role. That is the first case, the Goldwater-Nichols Act, which I think needs careful examination to see how it does or does not help with the situation.

The second one is more technical and operational, and kind of interesting. We have, in fact, solved a terrorist problem in the last twenty-five years. We have solved it so successfully that we have forgotten about it; and that is a treat. The problem was aircraft highjacking and bombing. We solved that problem; it has more or less gone away. It had an operational and industrial solution. What is interesting is that we have forgotten the technical, capital, and operational costs of the integrated system of metal and explosive detectors that sit in all the airports of this nation, that have, by and large, been successful in preventing airplane bombings and highjackings, which looked to be endemic just thirty years ago. The system is not perfect, but it is good enough. Since 1986, there have been four aircraft bombings, each of which caused over 100 deaths. Interestingly enough, none of those flights originated in the United States. Thus, we have pretty much nailed this thing, on a scale of other problems.

Pressing ahead—in the chemical and biological world—we need to move to some sensor systems, to integrated logic that can detect in time to protect and warn for counterterrorism, not just for effective treatment for most of these cases. After the fact identification is nice, but we would like to do better. In the nuclear area, I will not kid you about how hard this problem is. We still have quite a lot of work to do to control special nuclear materials and the places they might leak, to detect transit across transnational boundaries. This is an exceedingly hard problem.

What is interesting is that having worked this case with the aircraft industry, we know the costs; we can use those as economic targets. An interesting question is "what would we pay for the equivalent of installing metal detectors in airports; is that price equivalent to what we would pay for installing sensors in public buildings?" What can we do for that price? We can begin to work the problem backwards that way. I have watched evolution of detector development. I do not think we have ever put economic modeling of the problem and the market out in front; so the other thing I hold out to you is that we need to commercialize this sector. We pay that price without knowing it, therefore it cannot be too high. Are we willing to pay twice that, three times that to detect biological weapons? I leave that assignment to the reader…. I didn’t say I was going to give you all the answers.

It is fair to talk about a couple of my fears. I have one lingering fear. This may seem funny. My lingering fear is the development or arrival of a terrorist with a sense of humor; it is a scary thing. Remember the definition: "the use of intimidation or the creation of an atmosphere of threat." A terrorist with a sense of humor can probably achieve the end of destabilizing or discrediting a government without killing many or even any people, if he/she is very, very clever. I can create the appearance of terrorism or the impact of terrorism without very many deaths. If you want a good reference for this, go back and read the thirty-year old book called *The Monkey Wrench Gang* by Edward Abbey. It is a book about eco-terrorism in the American West, about three men and a woman who were angry with developers. It is a terrorist with a sense of humor. The book was very unpopular with some people at the

time, but it is worth a re-read.

There is a famous San Francisco story I love to tell. About ten years ago, San Francisco, being an old labor town, was one of the last places where there were social activists. A campaign started to buy the power plants and run them by the city. The semi-socialists lobbied that surely the power would be cheaper if the plants were run by the people. And you can see in California, the slow work-up to this campaign, about six weeks to effectively "nationalize" the power plants. A beloved humor columnist in San Francisco ended the entire campaign one Sunday morning by writing one line in his Sunday column. He wrote, "You mean they are going to run the powerplants with people who can't remember to close the windows when they are washing buses." On Monday morning he went to work, and the entire political campaign was over; it had died; and it was never mentioned again. You should not underestimate the attitude of the civilian population if you can successfully create a matter of trust with the federal government. So one of the things I worry about is a terrorist with a sense of humor who knows how to play the game who destroys that trust.

Let me say, in conclusion, I think these steps, the careful analyses of past cases and problems and previous work could give us an adequate agenda of the 21st Century. I think neither the threat nor its solution, quite surprisingly, require drastic social steps or impossible technical breakthroughs. They do require, however, a very serious and focused effort and shared vision of the Executive and Congress, which is pretty hard to get. What is important to recognize is the shared vision has to be held for a very long time.

About the Contributors

Robert M. Blitzer: Mr. Blitzer retired at the end of November 1998 as Chief of the Domestic Terrorism/Counterterrorism Planning Section, National Security Division, FBI Headquarters. On December 1, Mr. Blitzer joined SAIC as the Associate Director of the Center for Counterterrorism Technology and Analysis. From 1986 to 1995, he served in the FBI's International Terrorism Operations Section, where he assisted in the management of several high profile terrorism matters, including the bombing of Pan Am Flight 103 in 1988, the World Trade Center Bombing in 1993, the plot to bomb several locations in greater New York City in 1993, and the bombing of the Alfred E. Murrah Building in Oklahoma City in 1995. Mr. Blitzer has received both the Attorney General's Distinguished Service Award and the Director of Central Intelligence's National Intelligence Medal of Achievement. In 1996, Mr. Blitzer was named Chief of the Domestic Terrorism/Counterterrorism Planning Section where he was responsible for the coordination of several national counterterrorism programs. Mr Blitzer graduated from St. John Fischer College in Pittsford, NY, in 1968. He joined the FBI in April 1972 as a Special Agent.

Jay C. Davis: Dr. Jay C. Davis has served as the director of the Defense Threat Agency (DTRA), Washington, D.C. since October 1, 1998. Dr Davis has been a scientific advisor to the United Nations Secretariat and several U.S. agencies. He participated in two United Nations inspections of Iraq as an expert on mass spectrometer and construction techniques. Dr. Davis was appointed Lawrence Livermore National Laboratory's Associate Director for Environmental Programs in June 1994. He is a nuclear physicist, has worked as a research scientist and an engineering manager, leading the design and construction techniques of several unique accelerator facilities used for basic and applies research. Dr. Davis holds a Bachelor of Arts degree and Master of Arts degree, both in Physics, from the University of Texas, and a Ph.D. in Physics from the University of Wisconsin. He is a Fellow of the American Physical Society.

T**homas M. Hastings:** Mr. Hastings is the Deputy for Operations, State Department's Office of the Coordinator for Counterterrorism. He is responsible for overseeing the development of crisis response plans, for implementing these plans, and for conducting Foreign Emergency Support Team (FEST) real-world deployment and readiness training. Mr. Hastings retired from the Marine Corps in 1993 where he was a faculty advisor and Special Operations instructor at the Marine Corps Amphibious Warfare School. He also served as first Marine Corps detailee to the State Department Counterterrorism Office. Mr. Hastings has two Masters degrees, one in National Security and Strategic Studies from the Naval War College and one in Personnel Management, Central Michigan University.

Bruce Hoffman: Dr. Bruce Hoffman is Director of the RAND Corporation Washington DC office and a member of the RAND Senior Research staff. He was formerly Reader in International Relations and Chairman of the Department of International Relations, St. Andrews University, Scotland. In addition, he served as director of the University's Centre for the Study of Terrorism and Political Violence. Dr. Hoffman has long been associated with RAND where he served in both the Strategy and Doctrine Program in RAND's Army Research Division and the International Security and Defense Strategy Program in RAND's National Security Research Division. He holds degrees in Government, History, and International Relations, and holds his doctorate from Oxford University. He is Editor-in-Chief of *Studies in Conflict and Terrorism*, and is a member of the Advisory Board of *Terrorism and Political Violence*. He also serves on the DoD Counter-Terrorism Advisory Board. His many publications include the recent book *Inside Terrorism*.

David A. Kay: Dr. David Kay is currently the Vice President of Science Applications International

Corporation (SAIC) and Director of the Center for Counterterrorism Technology and Analysis. Dr. Kay served as the UN's Chief Nuclear Weapons Inspector, leading numerous inspections into Iraq following the end of the Gulf War. He led teams that found and identified the scope and extent of Iraqi uranium enrichment activities, located the major Iraqi center for assembly of nuclear weapons, and seized large amounts of documents on the Iraqi nuclear weapons programs. He has fifteen years of international management experience with international organizations and trade associations, including the International Atomic Energy Agency. Dr. Kay holds a Bachelor of Arts degree from the University of Texas at Austin and a Masters in International Affairs and Ph.D. degrees from Columbia University. He is the recipient of the IAEA's Distinguished Service Award and the U.S. Secretary of State's Commendation.

Douglas Menarchik: Dr. Douglas Menarchik (Colonel, USAF, Retired), at the time of the writing of this chapter, was the Director, Center for the Defense Leadership and Management Program (CDLAMP) at the National Defense University. Prior to becoming CDLAMP Director, Dr. Menarchik was a Professor of Democratic Defense Management at the George C. Marshall European Center for Strategic Studies and Defense Economics in Garmish, Germany. He has served as Military Adviser to the Vice President , where his portfolio included terrorism and low-intensity conflict, and as Assistant for Terrorism Policy at the Pentagon. Dr. Menarchik also worked on the Air Staff at the Pentagon in the Middle East/African Policy Division, and in USAF Special Operations dealing with combating terrorism, foreign internal defense, and crisis response management. Dr. Menarchik has a Bachelor of Science degree from the U.S. Air Force Academy. He received both his Master of Arts and Ph.D. from George Washington University. He also has a Master of Religion degree from the Liberty Baptist Theological Seminary. Additionally, Dr. Menarchik served as a Senior International Fellow at Harvard University's Center for International Affairs and taught at the Air Force Academy. He published a 1993 book, *Powerlift: Getting to Desert Storm.* He also has written extensively on combating terrorism, low intensity conflict, and international crime. Dr. Menarchik was recently named to head the George Bush Presidential Library at College Station, Texas.

Peter S. Probst: Mr. Peter Probst currently serves in the Office of the Secretary of Defense where he is primarily concerned with issues relating to international terrorism, political violence and infrastructure vulnerability. He represents the Office of the Secretary on such issues at meetings with senior U.S. and foreign government officials, and also has co-authored a major study entitles, *Terror-2000: The Future Face of Terrorism.* At present, Mr. Probst's primary focus is on the future terrorist threat and the development of strategies, tactics and policy initiatives to more effectively counter it. Prior to joining the Department of Defense, Mr. Probst served some 20 years with the Central Intelligence Agency working in both the Directorate of Operations and the Directorate of Intelligence. There, his primary responsibilities concerned terrorism, insurgency and international narcotics trafficking. Mr. Probst also serves on the Standing Committee on Global Terrorism, Political Instability and International Crime of the American Society for Industrial Security. He is a member of the Terrorism Task Force and the Information Technology Security Task Force of the Center for Strategic and International Studies, and is a member of the Advisory Board for the Investigative Project on Religious Extremism sponsored by the Middle East Forum. Mr. Probst is a graduate of Columbia College and Columbia University where he received a B.A. in history and an M.A. in anthropology/archaeology. Mr. Probst also served in the U.S. Air Force Intelligence Service which he retired with a reserve rank of Lieutenant Colonel.

Gregory J. Rattray: Dr. Greg Rattray (Lieutenant Colonel, USAF) was, at the time this chapter was written, Deputy Chief of the Defensive Information Warfare Division at Headquarters, Air Force. He has served as an intelligence officer at Headquaters, Strategic Air Command and the 18 Tactical Fighter Wing at Kadena AB, Japan. He was also assigned to the Air Force Academy as an Assistant Professor of

Political Science and Deputy Director of the USAF Institute for National Security Studies (INSS). He has published on proliferation, arms control and information warfare. His dissertation, "Strategic Information Warfare: Challenges for the U.S.," will be published by MIT Press in summer 2000. Dr. Rattray is a graduate of the U.S. Air Force Academy, the Kennedy School of Government at Harvard University, and recently received his Ph.D. from the Fletcher School of Law and Diplomacy at Tufts University in May 1998. Lt Col Rattray is currently serving as Commander, 23rd Information Operations Squadron, San Antonio, Texas.

Stephen Sloan: Dr. Sloan is a Professor of Political Science at The University of Oklahoma. He has lectured at The National War College and The Army War College. He has conducted over sixteen simulations of terrorist incidents with concerned personnel and units in the United States and overseas. He has also conducted crisis management workshops for multinational corporations and the Indonesian Foreign Ministry. He is a member of The International Institute for Strategic Studies and The American Society for Industrial Security (Standing Committee on Global Terrorism and Political Stability). He has authored *Simulating Terrorism* and *Low-Intensity Conflict: Old Threats in a New World*. He co-edited with Richard H. Schultz, Jr. *Responding to the Terrorist Threat: Security and Crisis Management.* Dr. Sloan's latest book, co-edited with Sean Anderson is *Historical Dictionary of Terrorism*. Dr. Sloan received both his Master of Arts degree and Ph.D. from New York University.

James M. Smith: Dr Smith is Director of the USAF Institute for National Security Studies (INSS), located at the US Air Force Academy (USAFA), where he is also on the faculty. Dr Smith, while on active duty, was a member of the initial cadre that established the Dynamics of International Terrorism and the Crisis Response Management courses at the USAF Special Operations School. He also worked in the late 1970s effort to establish a viable US military terrorism response capability. He recently returned to the topic with his publication, with William C. Thomas, of an article "The Real Threat from Oklahoma City: Tactical and Strategic Responses to Terrorism," in the Spring 1998 *Journal of Conflict Studies*. Dr Smith is a graduate of the US Air Force Academy. He holds a Master of Science Degree from the University of Southern California and a Doctorate in Public Administration (Public Policy) from the University of Alabama. In addition to faculty positions at the USAF Special Operations School and the US Air Force Academy, he has taught national security related courses at the Air Command and Staff College and at the United States Military Academy, where he was also Associate Dean for Academic Research.

William C. Thomas: Major Thomas (USAF) at the time his chapters were written was Chief, Military Operations Other Than War, at the USAF Doctrine Center at Maxwell AFB, AL. Formerly a faculty member at the USAF Academy where he edited the journal *Soldier-Scholar* (now *Airman-Scholar*), he was selected to return to graduate school under USAFA sponsorship for a PhD with a follow-on assignment back to the USAFA faculty. His study is focused on peace operations in the graduate international relations program at George Mason University, where he enrolled beginning in the fall 1999 term. He has published, in addition to the *Journal of Conflict Studies* article co-authored with Dr. Smith cited above, an article "Understanding the Objectives of Terrorism: A Key Analytical Tool," in the *American Intelligence Journal* in Spring 1996. He has just completed a study "The Role of the Department of Defense in Countering Domestic WMD Terrorism" under INSS sponsorship. Maj Thomas is a graduate of the University of Virginia, and he holds a Master of Business Administration degree from Regis University. Before entering active duty with the Air Force, he was an intelligence analyst for ANSER in Washington where he supported US Special Operations Command's strategic planning offices.

David Tucker: Dr. Tucker is a Visiting Professor in the Special Operations Academic Group at the

Naval Postgraduate School. Before coming to the Postgraduate School, he served in the Office of the Secretary of Defense for Special Operations and Low-Intensity Conflict and as a Foreign Service Officer in Africa and Europe. His publications include *Skirmishes at the Edge of Empire: The United States and International Terrorism* (Preager 1997), "Fighting Barbarians," *Parameters* (Summer 1998), and "Responding to Terrorism," *Washington Quarterly* (Winter 1998). Dr Tucker holds his PhD from the Claremont Graduate School.

James J. Wirtz: Dr. Wirtz is currently a Professor and Chairman, Department of National Security Affairs at the Naval Postgraduate School where he teaches courses on nuclear strategy, international relations theory and intelligence. He was a John M. Olin Fellow at the Center of International Affairs, Harvard University and also taught at Franklin and Marshall College. He is the author of *The Tet Offensive: Intelligence Failure in War* and co-editor with T.V. Paul and Richard Harknett of *The Absolute Weapon Revisited: Nuclear Arms and the Emerging International Order*. Dr. Wirtz received his Bachelor or Arts degree and Master of Arts from the University of Delaware. He earned his MPhil and Ph.D. in Political Science from Columbia University.