

STATEMENT

OF

FRANK J. CILLUFFO

BEFORE

THE AMERICAN BAR ASSOCIATION STANDING COMMITTEE ON LAW &
NATIONAL SECURITY

“THE ROLE OF INTELLIGENCE IN IDENTIFYING, PREVENTING AND
RESPONDING TO TRANSNATIONAL TERRORISM: A FRAMEWORK FOR U.S.
NATIONAL SECURITY PLANNERS”

DECEMBER 10, 1996

Assumptions About the Current Terrorism Threat

For decades, the potential for two possible types of attacks have haunted terrorism experts within the US national security community — the likelihood of a major terrorist incident occurring within the continental United States and the possible use of weapons of mass destruction by terrorists. Both have now come to pass. Moreover, recent reporting indicates the possibility that the perpetrators of the 1993 World Trade Center bombing seeded their bomb with potassium cyanide. If so, the threat was only neutralized because the terrorists were not aware that the heat and shock generated in the explosion would destroy the poison.

Two critical thresholds have now been crossed, forcing policy makers to plan for terrorism that may well be within our home territory, involving weapons more dangerous than ever before. This sea change in terrorism demands a vigorous and flexible response policy to counter the threat of terrorism — in both its novel and familiar forms.

Before discussing US response options, I'd like to quickly touch on some assumptions regarding the changing face of terrorism.

First, terrorism always has, and always will remain the weapon of the weak. It is a low cost, high leverage method and tactic, enabling small nations, sub-national groups and even individuals to circumvent the conventional projections of national strength — i.e., political, economic or conventional military might. This is especially so since our swift and decisive victory in Desert Storm. Few, if any, nations would attempt to confront the US in a conventional war today — recognizing that terrorism and unconventional warfare is a more effective — and perhaps even unaccountable — means of leveraging a superpower.

Potential US adversaries are also aware that the TWA 800 tragedy received as much media exposure as Desert Storm — and probably caused more anxiety and fear among the American population.

Second, terrorism is increasingly a strategic tactic and weapon for non-state actors — increased ethnic, tribal, religious and national conflict motivate a host of adversaries with interests inimical to our own. Sub-national and non-state groups, such as the Supreme Truth, Basque separatists and militias such as the Aryan Republican Army are difficult to monitor for a variety of logistical problems and legal constraints. Even when conflict coalesces into a mass movement, terrorism tends to germinate within small cells, difficult to discern against the backdrop of the larger movement.

Third, terrorist motivations are multifaceted, and differ from group to group. Of unique concern, is the irrationality of many non-state groups. Often feeling that they answer only to a higher spiritual authority, groups such as the Aum Shinrikyo are not

bound by traditional political ideology, nor do they strive for popular support and acceptance. These motivations translate into a myriad of dangerous intentions, including a propensity for mass casualties.

Fourth, terrorists today can avail themselves of advanced technology. The use of such technology (particularly weapons of mass destruction and information warfare and infrastructure warfare techniques) truly empowers a new class of adversaries.

Terrorist groups are also utilizing advanced technologies to collect intelligence, plan attacks and conduct attacks. Terrorists can identify critical nodes and single points of failure within say the electrical system or telecommunications — the degradation of either can severely impact our national and economic security. These (and many other) critical infrastructures are vulnerable to both physical (i.e. a well-placed bomb) and electronic exploitation — via remote. The gravest scenario would be a synergistic attack, capitalizing on information warfare (or IW) strategies to multiply the effectiveness of traditional terrorist tactics e.g. disrupting emergency communications to hinder civil response during a terrorist attack.

Very quickly, what does all this mean for US national security planners?

1. Terrorism, and unconventional warfare for that matter, is increasingly becoming the strategic weapon and tactic of choice appealing to nations, sub-nationals and even individuals;
2. The US is likely to remain a primary target, both domestically and abroad;
3. Preserving our democratic principles and open society inherently leaves us vulnerable to terrorism;
4. Terrorism is increasingly transnational, with groups operating within and across borders, often with no countries to sanction or ports to blockade. And within cyberspace, where terrorists can jump from nation to nation in nano-seconds, law enforcement is constrained to borders that are not even lines on a map;
5. While the car bomb will likely remain the terrorist "weapon of choice," the increasing availability of advanced technology and knowledge relating to WMD and information and infrastructure warfare cannot be rolled back.

What options are available in light of all this? A vigorous policy of flexible response to the terrorist threat must be developed that builds on several strategies, that, in turn, are based on accurate and timely intelligence. I will spend the balance of my time spelling out these strategies.

Identification, Prevention, Response & Consequence Management

There are a number of means the US has to combat terror, including diplomatic and economic sanctions, law enforcement activities, military reprisal and covert action. Successful implementation depends on providing decision makers with concrete information on the capabilities, intentions, and modus operandi of our adversaries. Only through a robust intelligence base is it possible to provide indications and threat warning and provide the necessary information, on a case by case basis, to prevent, deter, counter and respond to the terrorist threat.

Just as terrorists frequently resort to ambiguity (by not necessarily claiming responsibility for their actions), so too must the US perpetuate ambiguity by signaling that retribution is guaranteed — yet can be achieved through a variety of responses — that keep them on edge — not knowing where, when and how the U.S. will strike.

Indications and Warnings

Because terrorist threats present a constantly moving target and are dynamic in nature, intelligence assets must be extremely flexible to provide early warning. While maintaining a robust technical intelligence capability is important, it is critical we augment our human intelligence (or HUMINT) capability. Moreover, HUMINT must be used in a highly innovative manner in order to penetrate hard targets and acquire the "right" sources within the decision loop of terrorist organizations.

Terrorists do not frequent the cocktail circuit. Recruitment, must then move to other arenas. One option is approaching the disreputable and dangerous 'line' members of the terrorist organizations. These are often individuals who may have blood on their hands, but are the only ones that have insight into the intentions, motivations and plans of terrorist organizations. As distasteful as these individuals may be, the US has no choice but to aggressively develop these sources.

The second recruitment option is equally challenging: terrorists' financial and political backers found in boardrooms and on yachts in international waters — Osama bin Laden for example. This approach, also strains the reach of the US intelligence community because of the "high cost" of a seat at these tables. These cases require considerable discretion — subtle diplomacy and clandestine means are often most effective.

Once identified, the vulnerabilities of sources must be exploited. Which terrorist groups have leadership disputes? Is there a disgruntled would-be leader who can be recruited? Which benefactors of terrorist organizations have a particular taste for Western luxuries and lifestyles? Once in place, cautious tradecraft and handling of recruits is imperative out of fears of compromising the source, or the entire operation — bringing us back to square one.

It is critical not to mirror-image Western values and mindsets onto potential recruits. Deep knowledge of regional, sub-regional and communal histories, languages and customs is essential. .

In sum, HUMINT is vital to providing indications and warnings of terrorist threats. Innovative methods must be developed to effectively recruit these sources. We need to recognize that good citizens do not have information about terrorist organizations or their plans. Hence it is necessary to cultivate these sources, as actual penetration with US assets raise many other tough ethical dilemmas, including whether or not we are willing to get our own hands bloody — the price of admission to the inner circle.

Prevention

With well-developed HUMINT sources within terrorist organizations, decision makers may have the opportunity to undertake operations against terrorist actions before they occur.

Prevention assumes both a tactical and strategic approach. In each case, intelligence is vital for identifying vulnerabilities that can be leveraged for prevention. Tactical prevention involves operations to defer and disrupt immediate terrorist threats. In such cases, support for law enforcement and the military is crucial.

Unless state sponsored, the main tools of tactical prevention are covert action and law enforcement activities. As the origin of some forms of terrorism is a "gray area" — a gap between conventional military response and traditional law enforcement activities, covert action — in support of larger national policy objectives — may reap great rewards.

Intelligence is also crucial in support of law enforcement. Terrorism, on top of whatever else it may be — is criminal. It is law enforcement who must investigate, identify, arrest and ultimately prosecute those directly responsible for the criminal act. This can range from extradition with friendly nations, to the use of hostage rescue teams to extract perpetrators from less-than-friendly nations. Acknowledging the difficulties pertaining to sources and methods, intelligence in support of law enforcement investigations or operations must be improved. I recognize that many in this room are working on improving this process.

Intelligence also needs to illuminate the shadowy networks of terrorist procurement and logistics and to effectively track finances. As terrorist organizations come under more sophisticated surveillance, the complexity of the supply "chain" for money, munitions and other material increases. Thus more links to be exploited — intelligence must discover the weakest links in hopes of accessing the entire chain. Tactically it may include freezing or zapping bank accounts — strategically it may

include applying economic sanctions against state sponsors of terrorism, but we must remember that these measures are diplomatically and politically problematic at best.

These individuals can also be reached by employing psychological operations. PSYOPS is an underutilized but effective tactic intended for influencing the behavior of the targeted audience. It could be used, for example, to erode popular support to isolate the military and operational planners from the larger organization, organizations from each other and from the larger "movement," and ultimately the movement from society at-large.

These preventative measures depend on interagency and multi-disciplined cooperation, as well as reliable international liaison. Each measure depends on intelligence to identify the key area of vulnerability that can be leveraged — militarily, through law enforcement, or through clandestine means — to prevent terrorist strikes before they occur. Innovation and vigor are essential to implement these strategies.

Response Options and Consequence Management

No matter how robust, intelligence will never provide a 100% picture or provide early warning of all terrorist incidents. As such, developing strategic and tactical response options and consequence management and remedial planning are top priorities. Like preventative measures, it is important to ensure that response options are tailored to the specific case, what worked effectively in one case, may not lead to the desired outcome in another.

Strategic response may include full-scale military intervention and reprisal. Again, it is essential that clear indications of state sponsorship must be found in near real-time — within the "window of popular support." In the case of the La Belle Disco bombing in Germany, sufficient evidence of state sponsorship was found in order to retaliate militarily against Libya. Among the few other scenarios that lend themselves to the use of the military instrument are cases in which safe havens are used to provide sanctuary for terrorists. The use or threatened use of the military instrument can provide strong leverage on a state to acquiesce to the rule of law or to discontinue support in behalf of terrorists. Intelligence is critical for tracking the movements of terrorists and identifying training camps, Op Centers and safe havens.

Beyond these measures, the US must signal to the leaders of non-state hostile actors that they will be held personally accountable not only for their own actions, but for those of their subordinates as well. The full weight of US military and law enforcement will be brought to bear, with the intent to reciprocate. Put simply, we will find out what a given terrorist organization values and demonstrate our ability and willingness to "take it away" in order to deter an incident before it occurs.

National security planners must also prioritize plans for civil emergency preparedness and coping with the consequences of a terrorist attack, particularly those involving WMD or a crippling infrastructure attack. Thinking back to Oklahoma City, the powerful image of the fireman cradling a baby in his arms, will stick with me as long as I live. It is a reminder that the devastation of terrorism is local. Suppose it had been a radiological, chemical or biological — the first tier responders would be like the canaries in a coalmine. Lacking the proper decontamination gear, medical vaccines and antidotes or even sensors to detect if in fact a WMD was used could be devastating — in fact they may even inadvertently exacerbate the problem — spreading the deadly effects. It is essential to ensure that civil emergency responders have the tools, resources and training they need.

Conclusion

As terrorism extends the battlefield to incorporate all of society, I am concerned with the recent emphasis placed on physical security and hardening of targets. As one example, the successful hardening of airlines and airports urges terrorists to alter their modus operandi — ie resort to using shoulder-launched missiles, or to simply select from the endless number of soft targets such as subways and train stations. In short, the number of targets is too vast to ever ensure full physical security — if we ever did harden all targets, the terrorists win, because our way of life would be lost. The inadequacies of physical security highlight the importance of indications and warnings, prevention, response and consequence management. In each of these, intelligence must play a vital role.

The changing face of terrorism requires a vigorous and flexible response by US national security policy makers. It is not simply a matter of throwing more money at HUMINT or CT programs. Rather, national security leaders must foster a culture of institutional innovation to better prevent, respond, prepare for and contain the impact of a terrorist attack. Fostering such a culture is essential for developing and honing responses to the terrorist threat — whether it be improving interagency and intra-agency cooperation, intensified PSYOPS, improving our understanding of the culture and mind-set of our terrorist adversaries, or more resourceful collection methods including recruiting the "right" sources and identifying key vulnerabilities that can be exploited and leveraged. Granted, developing such measures is easier said than done — declining morale within the clandestine service of the CIA, concerns about civil liberties and budgetary limitations are all legitimate concerns. In the end, however, strong leadership can surmount these obstacles and position the national security community to forge a flexible and vigorous approach to diminishing the terrorist threat.