PUSHING THE LIMITS

Michael D. Carrington*

We presently find ourselves pushing legal, technical, and human limits to prevent terrorist attacks from occurring again in America. After September 11, 2001, Americans finally began listening to terrorist experts. These experts advised the United States government to tighten security measures;[1] strengthen existing laws;[2] enact emergency legislation;[3] and utilize the elite military forces for retaliation, preemption, and/or prevention.[4]

The tactics, equipment, and processes to accomplish this formidable task are currently evaluated, changed, and created in an environment of urgency, if not crisis. I will present a practical security/law enforcement perspective regarding these efforts, their current framework, and their future development. The central issue is the relationship between sustaining order in a post 9/11 America and maintaining our constitutional freedom.

I. THREAT ASSESSMENT AND MANAGEMENT

Threat management depends on the assessment results. The assessment depends on having reliable information and making informed judgments. The justification for new and revised procedures will depend on the credibility and acceptance of the assessment. When assessing possible threats, the first and most elementary step is to identify the threat. Possible threats may be crime, natural disaster, technology failure, or terrorism. In the case of terrorism, the terrorist actor must be identified. Analyzing a threat that China may pose, for example, is much simpler than the analyzing the threat from loosely defined terrorist groups. "Intelligence on the military programs of nation-states is

[*] Appointed by President Clinton, Mr. Carrington served as U.S. Marshal from 1994 until March, 2002 and was a member of the Northern District of Indiana's anti-terrorism task force. Prior to becoming a U.S. Marshal, he was an Adjunct Associate Professor teaching Criminal Justice at Indiana University South Bend. He has been involved in numerous security projects, including the 1984 Olympic Torch Relay and the 1987 Pan American Games. Mr. Carrington has attended and participated in numerous seminars and conferences on security and criminal justice topics. The author would like to thank Bryan Reed for his thoughtful comments and help.

[1] *See, e.g.*, Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. No. 107-173, 116 Stat 543 (2002) (codified at 8 U.S.C. §§ 1701-1775).

[2] *See, e.g.*, Uniting And Strengthening America by Providing Appropriate Tools Required To Intercept And Obstruct Terrorism Act (USA Patriot Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[3] *See, e.g.*, Emergency Supplemental Appropriations – Response to Terrorist Attacks On September 11, 2001, Pub. L. No. 107-38, 115 Stat. 220 (2001).

[4] *See, e.g.*, Authorization For Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001)(codified at 50 U.S.C. § 1541).

comparatively more static and large enough to be covered by a variety of intelligence means."[5] The threat posed by terrorists is "fluid and elusive" and much harder to keep under continuous scrutiny.[6]

A. *Identifying the threats and vulnerabilities*

After identifying the outside threat, the threatened entity, nation-state, or large company must conduct a self-evaluation, identifying its own weaknesses and vulnerabilities. Unfortunately, the United States' vulnerability has been evidenced many times prior to September 11, 2001, for example: On February 26, 1993, Ramzi Yousef and co-conspirators detonated a bomb in a parking garage below the World Trade Center in New York City killing six people and injuring 1000; on April 19, 1995, Timothy McVeigh detonated a rented truck full of explosives in front of the Murrah Federal Building in Oklahoma City, Oklahoma killing 168 people; on July 27, 1996, an unknown person(s) detonated pipe bombs in Atlanta, Georgia at the Summer Olympics killing two people and injuring 112; and on October 12, 2000, a terrorist group steered a tug alongside the USS Cole while in the Yemeni port to refuel and detonated a bomb killing seventeen U.S. sailors and injuring thirty-nine others. The United States is no stranger to terrorism, both on its own soil and abroad. Furthermore, the American vulnerabilities have been exposed on numerous occasions, and are in fact published in an annual report by the Counterterrorism Threat Assessment and Warning Unit National Security Division of the Federal Bureau of Investigation.[7] The United States at large, however, did not truly understand its own true vulnerability until September 11, 2001, when 2998 Americans were tragically killed by terrorists, who crashed commercial airliners into the World Trade Center. This attack demonstrated the unpredictability and fluidity of terrorists. "An open society such as ours cannot eliminate completely danger from all aspects of life."[8]

After determining the threat and the threatened entity's vulnerabilities, assessment of the probability of the actual attacks and events must take place. The probability of actual attacks is now a part of our everyday lives. On February 7, 2003, the United States Presidential Office of the Press Secretary released Homeland Security Presidential Directive – 3, which created a

[5] John V. Parachini, Statement Before the House Subcommittee on National Security, Veterans Affairs, and International Relations Combating Terrorism: Assessing Threats, Risk Management, and Establishing Priorities (July 26, 2000), *available at* http://www.cns.miis.edu/pubs/reports/paraterr.htm (last visited Mar. 7, 2003).

[6] *See id.*

[7] *See generally* Federal Bureau of Investigations, FBI Publications – Terrorism in the United States, *available at* http://www.fbi.gov/publications/terror/terroris.htm (last visited Mar. 8, 2003).

[8] Parachini, *supra* note 5.

national security advisory system.[9] This advisory system instituted five threat levels with associated colors ranging from green, low risk of terrorist attacks to red, severe risk of terrorist attacks. This system is similar to tactical alerts utilized by the U.S. military, in which various threat conditions are posted and various security measures are enacted to coincide with each respective threat level.[10] In determining the threat level, the U.S. government makes a decision on the following conditions:

> [a] decision on which Threat Condition to assign shall integrate a variety of considerations. This integration will rely on qualitative assessment, not quantitative calculation. Higher Threat Conditions indicate greater risk of a terrorist act, with risk including both probability and gravity. Despite best efforts, there can be no guarantee that, at any given Threat Condition, a terrorist attack will not occur. An initial and important factor is the quality of the threat information itself. The evaluation of this threat information shall include, but not be limited to, the following factors:
> To what degree is the threat information credible?
> To what degree is the threat information corroborated?
> To what degree is the threat specific and/or imminent?
> How grave are the potential consequences of the threat?[11]

However, Gavin de Becker, a national security expert, states that the Homeland Security Alert System is strictly political, and "[i]t is viewed by virtually all serious professionals in the field of security and threat assessment with disdain."[12] Furthermore, according to de Becker, the system's primary flaw is analogous to a doctor advising a patient of the severity of the illness but not the cure. The Bush administration has provided a public alert system,

[9] Homeland Security Presidential Directive-3, (Mar. 12, 2002), *available at* http://www.whitehouse.gov/news/releases/2002/03/20020312-5.html (last visited Mar. 8, 2003) [hereinafter Directive – 3].

[10] One scale is called Defense Condition (DEFCON), which alerts military personnel on the possible threat of war and the Terrorists Force Protection Condition (FPCON)(formally called the Terrorist Threat Condition (THREATCON)). Each of these systems has a threat level assigned to varying degrees of possible attack. The FPCON scale ranges from normal, no threat to FPCON DELTA, which indicates that a terrorist attack has occurred and intelligence suggests that an attack is imminent. DELTA is generally a local condition, because the threat is intended for that specific installation. Most military bases find themselves in a FPCON CHARLIE versus DELTA during times of heightened terrorist threat awareness. *See also* Secretary of Air Force, Air Force Anti-Terrorism Standards, Attach. 4 at 59 (2002), *available at* http://wwwsam.brooks.af.mil/web/af/courses/amp/cluebag/afi10-245%20Anti-terrorism.pdf (last visited Mar. 8, 2003).

[11] Directive – 3, *supra* note 9.

[12] Jennifer Barrett, *High Alert*, NEWSWEEK WEB EXCLUSIVE, Feb. 13, 2003, *available at* http://www.msnbc.com/news/872585.asp (last visited Mar. 8, 2003).

but has failed to inform the American public of the meaning of this threat information.[13] Parachini stated, "[w]hile some hedge against the unpredictability of the future is commendable, we must not confuse prudent measures with efforts to avoid political blame for failure to take necessary precautions. . . . However, a balance must be struck between responsible preparedness and mere political hedging."[14]

After assessing the likelihood of an attack it must be determined if the attack is certain, highly probable, moderately probable, improbable, or probability unknown. Once this determination is made, the possible damage that may be inflicted by the attack should be assessed. This analysis must be made critically with possible losses kept in mind. In security language the final result should be a plan to manage the risks. Accomplishing this in companies can be difficult, much less in the context of our "Homeland!" Thus, the question arises are we betting lives on predictions made in the most complex of environments?

II. WHO'S RUNNING THE SHOW

Organizing law enforcement and security activities to prevent terrorist activities has proven difficult for the United States government. The fragmentation and decentralization of American law enforcement and security agencies are significant factors. Consider, for example, "turfs." During the development of the Homeland Security Department, it was recognized that many federal, state, and local agencies would have to share information. Until September 11th, many agencies did not share information, and many believe that if there was broader communication between the agencies – maybe the lives lost on September 11th could have been prevented.[15] However, "[f]ederal agencies are making progress in overcoming 'cultural' barriers and turf wars that once prevented them from sharing key information or data related to homeland security . . . ."[16]

The discussion of the details is underway and is very "devilish." There is great pressure for results and the present limits on procedures are for some being stretched beyond "reasonableness." The private security model has always been more oriented to preventing and mitigating "bad things." Most public law enforcement resources have traditionally been dedicated to responding to requests for service and crimes already committed. The incredible technology available to law enforcement and security efforts brings with it many issues, including its "proper use."

[13] *See id.*

[14] Parachini, *supra* note 5.

[15] *See* Maureen Sirhal, *Agencies are Overcoming Data-Sharing Barriers, Officials Say*, *available at* http://www.govexec.com/dailyfed/0303/030403td1.htm (last visited Mar. 8, 2003).

[16] *Id.*

III. BASIC SECURITY

Tightening security usually begins with some basic security principles revolving around first, defining who should be allowed "in" and second, determining the activities in which they should be allowed to engage. In the context of the United States this discussion is very interesting and complex. We are pushing our equipment, and the people on all sides are trying very hard suddenly to tighten security at everything from borders to Super Bowls. This results in false positives and negatives. Information monitoring and gathering procedures change with the elevated threat level. The technology is here. How will it be used? Big brother and lots of other people are watching and listening. Electronic databases are immense and growing daily, and include all of us. The private sector is very involved in gathering and storing this information as well.

Economics and politics are obviously critical to these issues and their outcomes. It is a guns and butter type discussion with danger and threat levels driving the priorities. The security perspective is fairly straightforward when you accept the view that there is great danger. This gives weight to the other side of the equation and the priorities and procedures should facilitate the prevention of bad things. Billions of dollars, millions of security workers, hi tech equipment refinement, and utilization to include substantial monitoring and recording of most public activities and some private and personal activities too. My message: Get used to it, it is here to stay.

IV. FINDING THE GROOVE

The framework for all these activities are our political and legal systems which apportion and limit government and private power in ways reflecting our "peoples" wishes. The current limits are being pushed and are hardly recognizable for some. Citizens have supported these "pushes" because they want to be made safe or at least feel safer. Emergency situations requiring special restrictions and procedures are provided for and are more easily agreed upon and understood by those affected. New rules and limits reflecting the new threat level and technology are needed. If America is to fight a war against terrorism, it probably needs proper anti-terrorism laws. Finding and agreeing on the "groove" will not be easy. The discussion has hardly begun. Which raises the question, give me liberty or . . . ?