The Last Days of Summer

James J. Wirtz

Thinking about the recent history and future course of homeland security will be forever tied to a series of events that transpired on a beautiful Tuesday morning in September 2001. The attacks on the United States that day had a profound effect on everyone – witness the outpouring of emotion on the part of the "9/11 generation" following the good news from Abbottabad. But those who grew up in the shadow of 9/11 will never really know what changed that day. Events might suggest to them that people were complacent or careless during the last days of that summer. They also might be forgiven for thinking that people will again become complacent. After all, al-Qaeda is on the ropes and Osama Bin Laden has gone to a watery grave. Why should we continue to care about homeland security? But this would be an incorrect perception of what transpired during the last days of that fateful summer; it is also wrong to use that perception as a guide to the future of homeland security. So what about America and Americans changed on 9/11 and what do these changes hold for the future?

A Growing Sense of Unease

Looking back on the months leading up to 9/11, it is clear that the intelligence and law enforcement systems were indeed "blinking red." Al-Qaeda was on the move and the United States was failing to take effective action to derail the terrorist network. Scholars have documented that a general feeling of unease had spread across Washington that summer as various government agencies struggled to assess and respond to the emerging threat of transnational terrorism undertaken by non-state actors.[1] The US government was attempting to head off al-Qaeda before the network could act on their nefarious intentions. Ultimately, the government would lose that race.

The academic community also was aware of the emerging threat posed by transnational terrorist networks populated by non-state actors. Although I never considered myself an expert on terrorism, by 9/11 my own work covered several topics that were eerily prescient. I had edited a volume in which one of the authors described the strategic significance and fundamental techniques behind the tradecraft used in 1993 by the terrorists who bombed the World Trade Center.[2] The operatives involved in the September 11 attacks also used the same tradecraft by "hiding in plain sight" to prevent detection by intelligence and law enforcement officials. In the summer of 2001, the US Air Force Institute of National Security Studies also published an edited volume in which I suggested that as the US military bolstered personnel and base security in the Middle East, terrorists might seek "softer" domestic targets within the United States.[3] Neither of these articles came close to predicting actual events, but they do demonstrate that scholars were turning their attention to the threat posed by transnational terrorism.

Two personal experiences in the summer of 2001 also stand out in my mind. The first was a dinner conversation I had with two US Customs officers. The officials had just identified and detained a gentleman from Central Europe who had attempted to use a badly forged Italian passport to enter the United States. The motivations behind the forgery were not particularly threatening, but I do remember expounding at length with the officials about how border security was becoming the front line of American defense. I recognized that it was imperative to stop terrorists from entering the country before they could disappear into various ethnic communities or the anonymity of one of our great cities. The customs officers did not disagree with my position, but they also gave me the impression they thought I was exaggerating the significance of what was to them a rather mundane action.

The second incident was a debate that emerged during a conference sponsored by

the Defense Threat Reduction Agency in Norfolk, Virginia. The debate concerned the likelihood that the United States would suffer a mass casualty terrorist attack. One of the speakers suggested that such an event was unlikely because terrorists lacked the organizational and technical skills needed to orchestrate the use of chemical or biological devices to obtain maximum lethality. The 1996 Aum Shinrikyo Sarin attacks on the Tokyo subway were used to illustrate this point. Despite the fact that the Aum cult possessed significant resources and much technical expertise, their effort to disperse Sarin was rudimentary at best. The other speaker did not dispute this assessment of Aum's prowess when it came to weaponizing Sarin, but instead made a point well known to social scientists: just because something has not yet occurred does not guarantee that it will not happen in the future. Within a few days, this argument would be settled, but not in a way that the conferees had anticipated.

During the final days of that summer, scholars and officials alike were concerned about transnational terrorism undertaken by shadowy groups. "Non-state actor" was a fashionable way to describe non-governmental organizations that were bent on launching destructive or disruptive activities. Officials and scholars also knew that by breaking down barriers to transportation and communication, globalization and the information revolution were making international borders highly porous. For the most part, the availability of these new conveniences was viewed as a positive development. For instance, I remember a trip I made to London in July 2001. I had purchased the plane tickets and made the hotel reservations entirely online. I also abandoned travelers checks for the airport automated-teller machine, which, I was reassured, would allow me to deduct British pounds directly from my American bank account. It was hard to perceive the dark side of this new freedom as one experienced it for the first time. In hindsight, it is easy to see how al-Qaeda was able to "ride the rails" of the information superhighway, but this mixed metaphor itself conveys how difficult it was to envision how terrorists could harness new technologies to create mayhem.

Although some of them were quite novel, all of the pieces of the puzzle were available. There was a growing recognition that globalization and the information revolution were transforming the security landscape. We just lacked a framework to make sense of it all.

THE NEW AGE

As I watched the World Trade Center collapse, I was struck by the audacity of the terrorists and what I can best describe as hubris, our hubris. We had underestimated our opponents and they had succeeded in striking us in a significant way. Theoretical concepts such as asymmetric attack, porous borders, and "hiding in plain sight" took on a harsh reality as it became clear that we had lacked a sense of urgency during the summer of 2001. We were living on borrowed time and time had run out. It was almost as if Americans were banking on the fact that our opponents would not have the nerve to attack our homeland. Al-Qaeda had plenty of nerve.

It also was immediately clear that our thinking about emerging terrorism was biased towards either well-understood threats (bombing, shooting, hostage taking) or more exotic activities (chemical and biological weapons), not the real problem at hand. Our reality was worse than our imaginations. Al-Qaeda was willing to use locally available materials to create death and destruction. They had identified the high-energy systems that served as the infrastructure of modern society as means to attack the United States. Instead of chemical weapons, for instance, chemical plants now appeared to be a likely terrorist target because they provided access to highly toxic compounds within urban areas. Instead of using time and resources to develop their own weapons, Al-Qaeda recognized that it could weaponize our industrial and transportation infrastructure to attack us. The fact that this infrastructure was not entirely designed to resist unauthorized or unintended uses created a critical problem for the US. Vulnerabilities had to be identified and countermeasures had to be adopted before these weaknesses could be exploited in another devastating attack.

I realized from my previous work on the topic of intelligence failure that it quickly would become apparent that scores of "signals" – accurate and timely pieces of information concerning what was about to unfold – were contained within the files and systems the intelligence and law enforcement communities maintained. Needless to say, officials and analysts had failed to exploit fully the materials that were contained within this "intelligence pipeline." As would become apparent in the following weeks, however, the intelligence problem posed by transnational terrorism was daunting because it crossed scores of organizational and jurisdictional boundaries. Information uncovered by the Central Intelligence Agency, for instance, might have to find its way to a local law enforcement agency to be put to good use, but there was no existing method to move this data in an operationally relevant timeframe. And if the information was highly classified, there was no real way to move the information at all. Local law enforcement officials lacked the required security clearances or facilities to receive or store classified reports. Additionally, local law enforcement agencies were now on the front lines. Information collected during a traffic stop, for example, might be critical to an ongoing analysis by the Federal Bureau of Investigation or Customs officials. But there was no way for local officials to communicate information in an operationally relevant timeframe to federal agencies that focused on international threats. Al-Qaeda was hiding within the operational and jurisdictional seams that existed between the US military, the intelligence community, and law enforcement agencies. The fact that our opponents were exploiting these seams created a critical vulnerability that had to be quickly eliminated.

9/11 did not "change everything," but it demonstrated that the threat posed by transnational terrorism was real and immediate. Our opponents had chosen to attack us; they had chosen war. The idea that we could respond in a leisurely way to the emerging threat, that we were somehow ahead of the terrorists, was gone forever. We could not count on controlling the pace of events. It also quickly became evident that al-Qaeda had chosen to exploit vulnerabilities embedded in the very infrastructure of modern life. Potential threats were intermingled within our cities because scores of high energy or potentially toxic systems permeated our infrastructure. Weapons suitable for mass destruction or mass effect were already in place within the United States. What the terrorists needed was an innovative or cunning plan to gain access to them. Our defenses were poorly configured because they reflected a sharp distinction between foreign threats, which were primarily the responsibility of the military and intelligence community, and domestic threats, which were the purview of law enforcement agencies. There was a distinction between the "front lines" and "the rear" when it came to our thinking about threats. That distinction no longer seemed appropriate, but just about every resource, organization, and concept we possessed reflected distinctions between foreign and domestic security as well as military or intelligence activity and law enforcement. Overcoming these weaknesses, which were exploited by al-Qaeda on 9/11, animated our activities during the first homeland security decade.

THE FUTURE OF HOMELAND SECURITY

There have been several important developments since that fateful summer. We now recognize the importance of intra-governmental relations in defeating the terrorism threat and the need to share information, resources, and best practices across federal, state, local and tribal jurisdictions and agencies. We now understand the importance of collaboration and cooperation among law enforcement, fire, emergency medical services, public health, and intelligence officials to generate the situational awareness and capabilities needed to combat the terrorism threat. We also recognize that we have to work to bridge the boundaries between jurisdictions and agencies to prevent our opponents from operating within the seams of our defenses.

Today, homeland security programs and policies are less animated by a crisis atmosphere and instead reflect the notion that emerging best practices have to be

embedded within a wider range of intelligence, law enforcement, and other public service programs. In a domestic setting, the activities of most public officials and agencies are directed at meeting myriad demands for support and services that have little to do with transnational terrorism. Programs that are intended to respond to the ongoing threat of terrorism have to help bolster capabilities when it comes to the "all-source threat" focus of the vast majority of law enforcement, fire, public health, and emergency medical service agencies across the country. Instead of remaining an "extraordinary" activity, homeland security in the United States is becoming part of everyday life because it is slowly but surely improving the ability of federal, state, local and tribal agencies to prevent and respond more quickly and effectively to all sorts of threats and incidents.

For theoretical, practical, and operational reasons, incorporating an "all-threat" approach to homeland security is a positive development. From a theoretical perspective, it is difficult to anticipate the exact nature and best response to future threats. It is better to foster broad situational awareness across a variety of jurisdictions and disciplines (e.g., border patrol, public health, or the chemical industry), to look for unanticipated developments or new patterns of potentially disruptive activity. From a practical perspective, it is simply not politically possible to devote large portions of scarce public funds to respond to a mercifully rare type of event (i.e., a mass casualty terrorism attack), while communities suffer from a long list of mundane problems. Homeland security initiatives that help communities respond to local problems will enjoy greater political support than activities that seem to deal with rarified issues of little immediate significance. From an operational perspective, an "all threat" approach can help improve communication across disciplines, agencies, and levels of government because it fosters better interaction in dealing with everyday events. By making data fusion and operational cooperation a matter of routine, "all-threat" collaboration can serve as the basis for prompt detection and defense against a potential terrorist incident.

There is also evidence that our overall situational awareness and response protocols continue to improve. The quick and effective action taken by local bystanders and patrol officers during the 2010 Time Square bombing incident suggests that average Americans feel empowered to respond to suspicious situations and that police and fire departments possess appropriate procedures once suspicious activity is reported. The car bomb in Times Square failed to detonate, but if it had, quick action by the New York City police and fire departments would have helped to limit casualties from a bomb blast.

Because the attitudes of Americans have changed, efforts to improve homeland security are now embedded in a general way in public policy and our attitude towards national security. Ten years after 9/11, the crisis atmosphere has faded, but organizations and agencies everywhere recognize the imperative to strengthen homeland security and to include homeland security "best practices" across a range of public service activities and agencies. The emergence of homeland security as a "process" is a phenomena that will gain strength in the years ahead. This process has already stopped several significant terrorist plots before they could unfold. It also has made the United States a far less hospitable place for clandestine terrorist networks.

CONCLUSION

Before 9/11 it *might* have been possible to write this essay, but I doubt that it would have been published. The threats described would have appeared implausible. Reviewers might have granted me the fact that launching a mass casualty terrorist attack using materials at hand was possible, but such an act would have appeared to lack strategic justification. I also doubt that manuscript reviewers would have been willing to grant that our opponents possessed the motivation or operational skill to pull off this type of operation, or could easily slip through our security measures. In other words, one could have posited a perfect storm attack, (e.g., terrorists armed only with box cutters succeed in destroying the World Trade Center in a few hours), but it would

have been dismissed as either alarmist or foolhardy.

The fact that we now believe that we could (again) be the victim of a mass casualty terrorist attack and that it is a mistake to underestimate the ingenuity and determination of our opponents marks the most important way Americans have changed in the aftermath of the September 11 attacks. This is the greatest lesson we learned on that last day of that summer. We no longer are living on borrowed time, we are working to recognize and overcome our weaknesses.

ABOUT THE AUTHOR

James J. Wirtz *is dean of the School of International Graduate Studies, Naval Postgraduate School and director of the Global Center for Security Cooperation, Defense Security Cooperation Agency.*

---

[1] Stephen Marrin, "The 9/11 Terrorist Attacks: A Failure of Policy Not Strategic Analysis," *Intelligence and National Security* 26, nos. 2-3 (April-June 2011): 185.

[2] J. Bowyer Bell, "Conditions Making for Success and Failure of Denial and Deception: Nonstate and Illicit Actors," in *Strategic Denial and Deception: The Twenty-First Century Challenge,* Roy Godson and James J. Wirtz, eds. (New Brunswick: Transaction Publishers, 2002), 129-162,

[3] James J. Wirtz, "Antiterrorism via Counterproliferation," in *The Terrorism Threat and US Government Response: Operational and Organizational Factors,* James Smith and William C. Smith, eds. (USAF Institute of National Security Studies, 2001).