Business as Usual? Leveraging the Private Sector to Combat Terrorism

By Stacy Reiter Neal

"Big business" and today's transnational terrorist movements such as al-Qaeda are, at first glance, drastically different entities with radically different aims. While one embodies Western capitalism and secular values, the other rails against the established world order, envisioning a society in which religious values are paramount. Despite their near-diametric opposition in principle, however, the trajectories of multinational corporations and transnational terrorist organizations have become increasingly similar since the terrorist attacks of September 11, 2001.

Groups employing terrorist tactics—once largely secular and with local or regional aims—have transformed from entities seeking to affect change within a single government or society to movements that retired Brigadier General Russell D. Howard calls "the new terrorism."[1] This "new terrorism" is global in nature; its goals transcend the secular realm and, in the case of al-Qaeda, take on a "transcendental" quality. [2] Rather than operating at the national level (either through state sponsorship or as an insurgent force against the state), today's al-Qaeda and its affiliates constitute truly a transnational movement. Al-Qaeda functions through its worldwide cells, relying on a supranational ideology for the movement's cohesion; small groups adopt the al-Qaeda "brand" as an identifier for their independent operations.[3] And, these new-generation terrorist movements are also well-financed and organized—often relying on legitimate businesses as fronts for financial and material support.

At the same time, while Western companies that operate branches, administrative offices, or factories in conflict-prone regions have long been aware of the risks of terrorism, their concerns have been historically oriented toward executive kidnappings and anti-capitalist demonstrations—incidents within the means of groups with limited aims and goals connected to the regions in which the multinational company operated. Now, in a globalized world, corporate satellites in foreign countries often house crucial operations rather than support or production functions that rely on direct orders from and feedback to headquarters in Western nations. As multinational corporations grow, they often become more decentralized, with separate, sometimes autonomous divisions operating globally, unified by a common brand identity. In addition to growth and international expansion, multinational corporations also operate in a world where terrorist threats have impact on a global scale rather than at just a regional level. Due to their increased international presence and wealth, these corporations have become high-value terrorist targets.

In today's environment, the strong international presence and impact of both business and terrorism leads to a reciprocal relationship. Terrorist groups learn best practices from business, and gain legitimate cash flows as well as big payoffs through publicized attacks. Meanwhile, corporations have felt the impact of terrorism both negatively (as targets) and positively (as terrorism creates new business opportunities for some companies—and therefore new revenue streams). In 2001, businesses were the targets in an overwhelming 90 percent of terrorist attacks against U.S. interests [4]; at the same time, security goods and services produced by the private sector (and which were often formerly provided by the public sector) account for hundreds of billions of dollars in private sector revenue each year.

The intertwined fates of business and terrorism prompt the question: given their similar transnational interests, similarly evolving structures, and interest in similar economic factors, how can business be best leveraged to fight terrorism? Writ large, the private sector's engagement in counter-terrorism can be classified in two ways:

- As a resource for public-sector counter-terrorism initiatives, including information-sharing and critical infrastructure protection; and
- As a catalyst for innovation in research and counter-terrorism tactics.

These two main roles will be explored broadly in this paper. While many private sector firms already act as security resources and innovators, some aspects of these roles—information-sharing in particular—are challenges that must be addressed if future public-private counter-terrorism partnerships are to succeed.

Private Sector as a Resource

The first, and perhaps most obvious, role for the private sector to play in counter-terrorism is as a resource for—and a partner to—government efforts. Given that the "private sector owns and operates an estimated 85 percent of the country's critical infrastructure,"[5] critical infrastructure protection is a logical first step in public-private counter-terrorism efforts. Indeed, programs initiated by the Clinton administration in 1996 and updated by the Bush administration in 2001 and 2003 appointed led federal agencies to consult with private sector entities in developing preparedness plans. [6] Critical infrastructure protection initiatives have been established within financial, telecommunications, energy, transportation, and other sectors; the information and cooperation from the private sector have been absolutely essential to the U.S. Federal Government's ability to secure these crucial facilities.

However, only one percent of the U.S. private sector owns the entire 85 percent of privately held critical infrastructure. While corporations within this one percent are no doubt highly engaged in partnership efforts on state and federal levels, the question is, how can government better engage the remaining 99 percent of companies—many of which, through their usual course of business, have the opportunity; the public interaction; and the means to provide potentially valuable street-level information to government, particularly intelligence agencies? [7]

Two cases clearly illustrate how successful engagement of non-critical infrastructure private sector firms can provide valuable intelligence resources to government. In 2001, a Minnesota-based flight school independently reported a suspicious student—a man who turned out to be Zacarias Moussaoui, a convicted 9/11 co-conspirator who was absent in the attacks because he was already in custody, thanks in part to the flight school information. [8] Similarly, an employee in a New Jersey Circuit City store was instrumental in thwarting a plot to attack Fort Dix in January 2006 when he notified authorities that a customer requested suspicious terrorist training footage to be transferred from VHS to DVD. [9] In each of these situations, private sector employees realized they had come across potentially valuable intelligence and took the initiative to locate the appropriate channels to report behavior observed in the course of their job-related duties. While it is not viable or desirable to implement an enforced reporting system within the private sector, a more streamlined public-private information sharing process could yield similar information that can be used to intercept would-be terrorists at the planning stage.

However, many challenges remain to building effective public-private information-sharing systems. The main obstacles to effective intelligence partnership programs include: information security and privacy concerns; the lack of an effective organizational structure to facilitate knowledge exchange; difficulty in measuring the success of intelligence-sharing in preventing terrorist attacks—and therefore of providing "proof" that investment in sharing efforts is worthwhile; and fears about the implications of increased government regulation over the private sector. Regardless of the potential benefits of cross-sector intelligence cooperation, these challenges are fundamental issues that will not—and should not—be overlooked. [10]

Private Sector as a Catalyst

In addition to partnering and cooperating with government efforts, the private sector can and is taking a lead role—both inadvertently and intentionally—in counter-terrorism. The private sector has long been home to innovation that is later adopted by the public sector. The same pattern of innovation is holding true for terrorist organizations, which adopt private sector best practices and fulfill business-school organizational behavior theories through their actions.

By leveraging business knowledge and best practices, terrorist organizations have successfully evolved into functional, nodal networks with strong messaging and mobilization capabilities. Taking a page from the multinational corporation's playbook, al-Qaeda has poured energy and resources into establishing a strong public relations committee as well as a dedicated media arm, al-Sahab, which has produced well-made propaganda videos and online content—even going as far as to hold online "press conferences" with senior al-Qaeda strategist Ayman al Zawahiri. [11]

Beyond effective media outreach techniques pioneered by private-sector businesses, terrorist organizations like al-Qaeda have also taken cues from "headless," decentralized, networked business models such as Craigslist,

maximizing the power of the Internet to communicate with broad constituencies and to create an organization that draws its strength from its cellular structure. [12] Furthermore, terrorist organizations adopt and disseminate best practices and technologies—such as improvised explosive devices (IEDs), suicide attacks, and other weapons and tactics—among their cells in much the same way that high-technology firms roll out new technologies for their consumers. [13] Organizational theory insights and knowledge transfer from the business world are therefore key resources in understanding and combating the new networked terrorist structures. In fact, by leveraging this business knowledge, counter-terrorists would be better prepared to face the modern terrorist organization than ever before.

However, beyond providing best practices and theoretical insights, the private sector has been innovative in pursuing research, development, and profit-making activities that can actively feed counter-terrorism efforts. One private-sector innovation that may be best suited for counter-terrorism campaigns is the well-established field of risk management. Due to their global presence, multinational corporations have long managed "a variety of risk factors," perfecting risk management techniques and strategies for profit that could also be "beneficial and effective for states around the world" in the campaign against terrorism. [14]

Post-9/11, the specter of international terrorism has opened new business opportunities to many firms. Terrorism insurance, security consulting, safety products, and other markets have been opened to private sector firms that have adapted to the modern security environment. These business opportunities have prompted many firms to lead cutting-edge research and development efforts that, in turn, drive the current field of terrorism knowledge. By pursuing their own goals, corporations can actually generate vital information, introducing new insights and information to the public sector.

The private sector's need for targeted research on terrorism-related issues is indeed an incentive for original and valuable research. Private sector firms have initiated projects exploring unknown factors that have ultimately yielded information beneficial both to the business and to the field of terrorism research. One company, a producer of safety products for consumer fuel tanks, approached the Tufts University-based Jebsen Center for Counter-Terrorism Studies to find out how terrorists instruct followers to manipulate fuel tanks as explosive devices. Through this directed research project, the Jebsen Center uncovered valuable video footage and chatroom transcripts that provide insight into evolving terrorist tactics. This information can be used both by the company—to improve its products and understand the threats its clients may face—as well as by the intelligence and counter-terrorism community in assessing the evolution of terrorist tactics—a dual function that academic research institutes like the Jebsen Center are well equipped to perform.

Additionally, the increased responsibility of the private sector in helping to combat terrorism will undoubtedly produce new risk assessment methods, policy models, and other technologies that can be applied by public sector decision makers in the future. Establishing formal cross-sector communication channels that facilitate exchange and partnership will be a key step in any successful public-private intelligence or counter-terrorism relationship.

The private sector's value as both a resource partner to and an innovator in the public sector in the fight against terrorism has yet to be fully realized. The theories and methods used by and originating within the private sector are practical tools that can and should be utilized by counter-terrorism professionals. By working together with private sector leaders, the U.S. government can maximize the potential of the private sector to provide alternate forms of information and spur creative thinking and research in counter-terrorism. Bridge-building organizations in academia or the non-profit world can further facilitate this cooperation by acting as a synthesis point for both private-sector needs and ideas and public-sector policy development.

Stacy Reiter Neal is Associate Director of External Affairs at the Jebsen Center for Counter-Terrorism Studies, The Fletcher School of Law and Diplomacy, Tufts University.

NOTES:

[1] Russell D. Howard, "Understanding Al Qaeda's Application of the New Terrorism—The Key to Victory in the Current Campaign," in Russell D. Howard and Reid L. Sawyer, eds., *Terrorism and Counterterrorism: Understanding the New Security Environment*, Second Edition (Dubuque, IA: McGraw-Hill, 2006), 91.
[2] Ibid. Howard here credits Ralph Peters, a military strategist and author, with the term.

[3] Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (New York: Portfolio/The Penguin Group, 2006), 140.
[4] Philip E. Auerswald, et. al., "Where Private Efficiency Meets Public Vulnerability: The Critical Infrastructure Challenge," from Auerswald et. al., eds., *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability* (Cambridge, UK: Cambridge University Press, 2006), 7.
[5] Under Secretary for Democracy and Global Affairs, U.S. Department of State, "Chapter 6: Critical Infrastructure Protection," from *North American Plan for Avian and Pandemic Influenza*. Available at <http://www.state.gov/documents/organization/91311.pdf>.
[6] See Daniel B. Prieto, III, "Information Sharing with the Private Sector: History, Challenges, Innovation, and Prospects," in Auerswald et. al., eds., *Seeds of Disaster, Roots of Response*.
[7] Telephone conversation with Robert Riegle, Director, Office of Intelligence & Analysis, U.S. Department of Homeland Security, October 23, 2007.
[8] Dean C. Alexander, *Business Confronts Terrorism: Risks and Responses* (Madison: University of Wisconsin Press, 2004), 13.
[9] Matt Katz, "Store Clerk's Tip was Key to Foiling Fort Dix Terror Plot," *USA Today*, May 9, 2007.
[10] For further discussion of public-private intelligence partnerships, see Stacy Reiter Neal, "Cross-Sector Intelligence Partnerships: Is Public-Private Information Sharing a Neglected Counterterrorism Tool?" in Russell D. Howard, Reid L. Sawyer, and Natasha E. Bajema, eds., *Terrorism and Counterterrorism: Understanding the New Security Environment*, Third Edition (Dubuque, IA: McGraw-Hill, 2008).
[11] Associated Press, "Al-Qaida invites journalists questions for al-Zawahri," December 20, 2007. Also see Rohan Gunaratna, "Strategic Counter-Terrorism: Part III, Mass Media Response to Terrorism," *Jebsen Center Research Briefing Series* Vol. 3, No. 1 (January 2008), available at <http://fletcher.tufts.edu/jebsencenter/publications.shtml>.
[12] See Brafman and Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*.
[13] For more detail, see Rockford Weitz and Stacy Reiter Neal, "Preventing Terrorist Best Practices from Going Mass Market A Case Study of Suicide Attacks 'Crossing the Chasm'," in Sean S. Costigan and David Gold, eds., *Terrornomics* (Hampshire, England: Ashgate Press, 2007).
[14] Jocelyne Kokaz-Muslu, "Preventing International Terrorism: Can Multinational Corporations Offer a Fresh New Perspective?" *Berkeley Electronic Press Legal Series*, Paper 1016 (2006), 5-6.