

PERSPECTIVES ON TERRORISM

Volume II, Issue 3

February 2008

A JOURNAL OF THE

TRI TERRORISM RESEARCH INITIATIVE

Enhancing Security through Collaborative Research

Table of Contents:

Counter-Ideology: Unanswered Questions and the Case of Pakistan By Muhammad Amir Rana.....	3
Complex Systems Problems in the War of Ideas By Steven R. Corman.....	6
Business as Usual? Leveraging the Private Sector to Combat Terrorism By Stacy Reiter Neal.....	10

Counter-Ideology: Unanswered Questions and the Case of Pakistan

By Muhammad Amir Rana

A counter-ideological response to neutralise and defeat terrorism has become a popular theme in the anti-extremism discourse. It is widely believed that ideology is the key motivating force behind the current wave of terrorism. In fact, academics, journalists, and counter-terrorism experts take for granted that Islamic extremism has its roots in a particular extremist version of religion. Therefore, promotion of a moderate and peaceful version of religion is essential to combat terrorism at its roots.

This ideological approach has led to some interesting perspectives in the bid to find solutions to the problem of Islamic extremism. One of the more attractive ones is the “Radicals versus Sufis” perspective. According to this viewpoint, Takfiri, Salafi, and Wahhabi ideologies are radical and responsible for promoting terrorism. Opposed to these radical ideologies is Sufism, which is hailed as a moderate version of Islam capable of countering radical ideologies.

The following assumptions underpin this ideological approach to tackling terrorism:

- Al-Qaeda and its affiliated groups gain ideological inspiration from Takfiri, Salafi, and Wahhabi versions of Islam. Jihad is central to these ideologies, so they are the sources of terrorism;
- The Salafi and Wahhabi extremist movements have political agendas and want to impose their version of Islam not only in Muslim states, but also throughout the world;
- Sufism, on the other hand, stresses self-purification and has little or no political dimension. So, it is a moderate movement and cannot pose any serious security or political threat to the world;
- A Wahhabi cannot be moderate; and
- A follower of Sufism cannot be an extremist.

Given the popularity of these theories, it is important to examine and question these assumptions. First, there is a need to define the objectives of this approach (i.e. what do we intend to achieve by promoting counter-ideologies?). The biggest challenges facing policymakers across the world today are: elimination of terrorism; and neutralisation of the systems created by the extremist forces. In that context, is it necessary—and possible—to eliminate radical ideologies? And can these ideologies be countered by Sufism alone?

Secondly, there is a need to comprehend the Wahabi and Salafi interpretation of Islam. Is extremism inherent in these ideologies? If so, how and in which regions can we see its impact? Can these ideologies not be transformed into the moderate ideologies? Conversely, are all Sufi movements moderate and incapable of generating any violent movement? Are Sufi ideologies intrinsically moderate or this perception is based on its cultural expression of music, dance, festivals, etc?

The Case of Pakistan

In the case of Pakistan, the situation is more complicated than the above “Radical versus Sufis” division suggests. There are 22 organizations and parties that represent the Wahhabi/Salafi sect. Out of them, only three—the Jamat ud-Da’wah (JuD), its subsidiary group Lashkar-e-Taiba (LeT), and another small group Jamat ul-Mujahedeen (JM)—favour militant jihad. Another Salafi militant group, Tehreek ul-Mujahedeen, which is active in Kashmir, considers its movement a part of the Kashmiri freedom struggle.

Apart from these groups, every other Wahabi party considers “Jihad against the Self” (*Jihad bil-Nafs*) as the greater jihad and believes that militant jihad cannot be waged until declared by the state. These parties do not consider the jihad in Kashmir and Afghanistan obligatory. The JuD, LeT and JM are also antagonistic towards the current democratic system in Pakistan and want to enforce a *Khilafah*, or the Caliphate, whereas the other Wahabi parties not only recognise Pakistan as a legitimate, constitutional state, but also take part in electoral politics individually or in alliance with other political parties.

Similar differences of opinion on jihad and democracy are also found within the various groups of Deobandis,

which are usually put into the category of Wahhabis because of some common theological precepts. Out of 46 major Deobandi parties in Pakistan, 10 are militant in nature, with jihadist and sectarian agendas. Moreover, these militant parties do not enjoy popular support from the mainstream religious clergy. Even on the issue of support for the Taliban, there are diverse contradictory views within the major Deoband political party, Jamiat Ulema-e-Islam. A large faction of the party, led by Maulana Muhammad Khan Sherani and Khaleed Somroo, remained critical of the Taliban, even when they were in power in Afghanistan. Last year, concerning the Lal Mosque issue in Islamabad, most of the Deobandi clerics from religious-political parties and the Madressah Board had denounced the activities of the students. So, the ideological demarcation within the school(s) of thought tends to revolve around jihad.

Sufism is a complex and cross-cutting belief system in Pakistan. Even the Deobandis believe in Sufism. Naqshbandi, the major Sufi cult in Pakistan, is mainly comprised of the Deobandis. Furthermore, it is also interesting that Maulana Masood Azhar, head of the major terrorist group Jaish-e-Muhammad, is also believer of Sufism and has restricted his followers to the practices of the Naqshbandi cult.

To further complicate the intermingling of beliefs and practices, the Barelvis, who are considered to be representatives of Sufism in Pakistan, are not free from pro-militant jihadi tendencies. In the Kashmir insurgent movement during the 1990s the Barelvis were quite prominent. Some Barelvi militant groups, such al-Baraq and Tehreek-e-Jihad, are still active. Sunni Tehrik, a major Sunni sectarian group, was found to be involved in the violent activities in Karachi and Interior Sindh. The Safi'es, an important Sufi group in Afghanistan, was an ally of the Taliban in their struggle to take over the country. They even managed to obtain a few important government offices under the Taliban regime.

Pro-Sufism Barelvis dominate Pakistan's religious landscape. The reason why they did not play a major role in the Afghan jihad of the 1980s was not because of any religious or ideological bindings, but because of political factors. The Saudi influence in the Afghan jihad was another reason for their marginalization. The Saudis had supported only Wahhabi and Deobandi groups during the Afghan jihad against the Soviet Union. Moreover, the Arabs and Africans who took part of the Afghan jihad had similar sectarian orientations as the Wahhabis and felt more at ease working alongside the local Salafi and Deobandi commanders. The Afghan and Pakistani groups had also preferred to work with Arab and African mujahideen because they had the more substantial resources.

Had it not been for the Saudi and Arab factor, the Barelvis too would have been able to secure their share in the jihad effort. If that had happened, would the promotion of the Wahabi ideology be suggested as a counter-strategy today?

When one ideology is supported financially, morally and politically to counter the other, it can increase sectarian strife in a society. Pakistan faced the consequences during the Afghan jihad as sectarian strife dramatically increased in the country. Similarly, strengthening one group or sect can give rise to similar trends in other sects. So we see that many Sufi groups have also been radicalized and they are as anti-US and anti-Western as other violent groups, though they lack the training and resources received by the Deobandis and Wahabis.

Instead of targeting the entire Wahhabi/Salafi community, can terrorism and political extremism not be countered by encouraging the more moderate elements within the Salafi school of thought?

Conclusion

It cannot be denied that the Wahhabi movements have created challenges within Muslim societies. They have marginalised the elements of moderation by promoting a narrow vision of Islam. But how these movements are changing Muslim societies and what kind of political, economic, cultural and social challenges they pose is a separate issue. Their domestic and international implications demand different kinds of strategies to the one proposed by counter-ideology theorists.

It is not a surprise that campaigns to promote counter-Islamist ideologies like Sufism have had little success in Pakistan. The official moderate enlightenment and Sufism movements have failed to gain acceptance among the masses. Anti-US and anti-Western feelings are on the rise in Pakistani society and any campaign aimed to counter these sentiments is perceived as a part of the American agenda. It also remains a fact that a large majority of the educated class in Pakistan considers the spiritual rituals of the *Pirs* inappropriate and activities like

use of drugs and prostitution on the shrines immoral. The Sufi culture in Pakistan itself needs reforms. That is why the government-sponsored enlightened moderation has failed to attract common people. Instead, such efforts are increasing support for radical movements.

To develop a comprehensive counter-extremism strategy, there is a need to examine all the aspects of this problem and assess the impact of promoting so-called moderate counter-ideologies in Muslim societies.

Muhammad Amir Rana is the Director of the Pakistan Institute for Peace Studies (PIPS), Islamabad, Pakistan.

Complex Systems Problems in the War of Ideas

By Steven R. Corman

To say that terrorism is a complex problem is a truism. Usually, someone who says this normally means that the problem is hard to understand and address. But to a natural or social scientist, “complex” has a special meaning that comes from complex systems theory. There are many definitions of complex systems, but I prefer this simple one: “we have taken a ‘complex system’ to be one whose properties are not fully explained by an understanding of its component parts.”[1] This means that we cannot understand terrorism through our usual method of breaking a problem into bits and studying them because the interaction between the bits has *emergent properties* that have important effects on the functioning of the system as a whole.

For a couple of years now, my colleagues and I have been applying complex systems ideas to problems of U.S. strategic communication in the so-called “war of ideas”. This essay reviews two cuts on that issue involving assumptions about the communication process and principles for finding the right message(s). It concludes with two general recommendations for a more realistic and effective approach to strategic communication.

View of Communication

Complex systems ideas are relevant to the government’s overall conception of the communication process. They currently employ a linear view dating back to the 1950s, which assumes that communication is set of transformations that move a message from sender to receiver. It draws heavily on a model of telephone systems developed by Bell Labs engineer Claude Shannon. [2] Shannon’s model has the following components: a *source* inputs a *message* (e.g. talks) into a *transmitter* (the telephone), which encodes a *signal* that is transmitted over a *channel*. The signal, which may be affected along the way by *noise*, makes its way to the *receiver* (the other telephone) where it is decoded into a message (e.g. heard) by the receiver or *destination*.

A formal model of human-to-human communication based on Shannon’s ideas was developed in the late 1950s [3]. We call this the *message influence model* [4]. It has since become a basis for the conventional wisdom of political campaigns, business domains of public relations and marketing, and government/military domains of public diplomacy, public affairs, information operations, and international broadcasting. It assumes that communication is a one-way process consisting of transmission of a message through a modular system directly analogous to the telephone system described above. As long as *fidelity* is maintained—i.e. noise does not degrade the message and the components don’t distort it or fail—the message will reach the destination exactly as it was intended by the source. Accordingly, controlled repetition (for reliability) and optimization of the individual system components are viewed as the key to success.

It is easy to find evidence of this model in operation in the statements and language of government agencies and officials. It is common to hear high ranking officials speak or sending “signals” or “messages” to foreign governments. In 2003, the Bush Administration created the White House Office of Global Communications with a mission to “ensure consistency in messages” by “disseminat[ing] accurate and timely information”. [5] The 9/11 Commission said the government “must do more to communicate its message”. [6] Former Under Secretary of State for Public Diplomacy, Karen Hughes, was well known for her insistence on “message discipline” and instituted a regular dispatch to U.S. embassies called *The Echo Chamber* that contained talking points for use in contacts with foreign publics and media. [7]

The problem with the message influence model of communication is that it’s wrong. When we’re talking about human systems, rather than telephone systems, the transmitter and receiver are people, and the source and destination are their minds. Communication is not as simple as transferring my thoughts to your mind through my mouth and your ears. Complex processes of expression and interpretation mediate our interaction. They are affected not just by the traits and experiences of the people involved, but also by the contexts they find themselves in at the time of communication. For example, “freedom” might mean one thing to an American (freedom *to* do things), but another to a Middle Easterner (freedom *from* corrupting influences).

Much more to the point of complex systems, a critical flaw of the old message influence model is that it treats

the elements as independent bits that we can break down and optimize. Theorist Niklas Luhmann [8] rejected this idea, believing instead that communication is a property of a complex system in which participants interpret one-another's actions and make attributions about the thoughts, motivations, and intentions behind them. The complexity arises because of a *double contingency*. Given two communicators, A and B,

- The success of A's behavior depends not only on external conditions, but on what B does and thinks.
- But what B does and thinks is influenced by A's behavior as well as B's expectations, interpretations, and attributions with respect to A.

This means there are no independent transmitters and receivers transferring independent meanings back and forth, as the old model would have it. Instead communication is an emergent property of the interaction of A and B.

This thinking leads to a new perspective that we call the *pragmatic complexity model* [4]. It views communication as a process of dialog rather than message transmission, and it carries a very different set of assumptions. For instance, it assumes that success—in the sense of causing some predictable result—is not the default outcome of communication. On the contrary, it's likely that messages will be interpreted in ways that one doesn't expect and doesn't want. Communication systems also have inertia (another emergent property) that causes them to interpret messages to fit pre-existing expectations. In that case, the repetition-for-reliability principle of the old message influence model is *exactly* the wrong way to bring about change.

Finding the Right Message(s)

The second way complex systems thinking is important in strategic communication has to do with the search for the right message(s). The old model of communication carries over to a belief in a straightforward search process. We addressed this issue in another recent paper [9] that applies Stuart Kauffman's rugged landscape model. [10] Think of a landscape as an array of possible communication solutions. A solution is a combination of features like message, communicator, medium, audience, timing, etc. Each solution has a particular quality or *fitness level*, represented by the height of its point on the landscape (see Figure 1) [11]. On a simple landscape there is one peak, with a best solution at the top surrounded by solutions with diminishing levels of fitness. But on a rugged landscape there are multiple peaks of varying fitness.

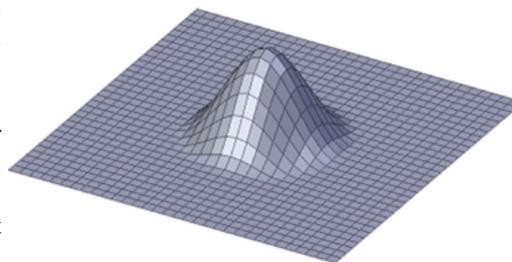
The two landscapes have radically different requirements for finding the right message. Simple landscapes are *modular* in the sense that there is limited interaction between their parts. To find the optimal solution you can optimize the parts, one at a time, making adjustments that move you in an uphill direction (i.e. improve fitness), because uphill *always* leads to the optimal solution.

Rugged landscapes, in contrast, are *integral*. Their parts are tightly coupled, meaning that you can't change one thing without affecting everything else. Here incremental improvement in performance is not enough because it might lead you to the top of a suboptimal peak. Depending on where you start, you might actually have to move downhill for a time in order to reach the optimal peak. Rather than systematic search, on a rugged landscape you need experimentation based on random variation, a more evolutionary approach.

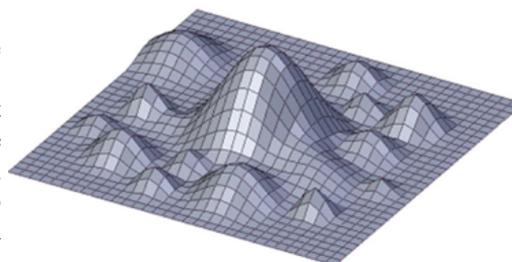
Just as the U.S. government believes in the simple message influence model of communication, it also believes the search for the right message takes place on a simple landscape. The U.S. National Strategy for Public Diplomacy and Strategic Communication (NSPDSC) [12] released last year provides a good example. It assumes

Figure 1

A. Simple Landscape, $K \leq 1$



B. Rugged Landscape, $K > 1$



the best message has already been found and sets it out in a set of broad talking points that promote American values and strategic objectives. Most of the document talks about how to optimize various aspects of delivering the message, such as coordination between agencies involved, making use of better spokespeople, and so on.

But in fact, the landscape of U.S. Strategic Communication is a rugged one because of the tight coupling of elements of the system. Multiple agencies have responsibility for strategic communication and sometimes work at cross purposes. Some spokespeople are better suited for some audiences than others. Messages intended for one audience “leak” to other audiences creating mixed messages. Audiences, even as conceived in the NSPDSC, are not independent: “Girls,” one of its target audiences, are also “youth,” another of its target audiences. These are but a few examples of interdependencies in the system that make the search landscape rugged.

What to Do

Specific recommendations associated with the pragmatic complexity model and the rugged landscape approach are outlined in our full white papers.[4], [9] But there are two underlying themes in these recommendations that I discuss here. First, both of the outdated approaches described above carry assumptions that strategic communication can best be optimized through control. In the message influence model, this is achieved by having a restricted message and hammering on it using repetition. In the simple landscape approach, control is achieved by using methodical trial and error search, making incremental improvements in the message by optimizing one variable at a time.

For the reasons discussed above, these approaches are unrealistic and actually lead to sub-optimal outcomes on our “war of ideas”. So the first order of business is for the U.S. to let go of the idea that it can control the strategic communication system. Accepting the complexity in the system, rather than fighting it, opens up new possibilities for action. For example, if they abandon the idea that they can tightly control which audiences receive which messages, they can start thinking about how they might exploit interaction between the different audiences. Just as Wall Street traders accept the complexity of the markets and profit by effectively “going with the flow”, strategic communicators can accept the complexity of the system and use it to their advantage.

Second, whereas both of the outdated approaches described above emphasize small incremental changes and assessment, the complex system view requires an approach more like evolutionary experimentation. For instance, an important implication of the pragmatic complexity view of communication is that communication systems often become “stuck” in a pattern where all messages are assimilated to a standard interpretation—much like the current situation where U.S. messages damage its credibility, if they have any effect at all. This situation requires a disruption that will kick the system out of its inertia and cause it to reorganize in a new configuration that might be more favorable to the U.S.

On a rugged landscape, controlled searches never take you far from where you start, which is most likely a spot on the floor or a minor peak. To find the optimal message(s) you need to search many different spots on the landscape by changing multiple variables at once in a random variation pattern. Such a strategy makes it much more likely that you will find the optimal peak, or at least get close to it.

To change the strategic communication game the United States should abandon control-oriented methods that were cutting-edge in the Eisenhower Administration. It should let go of the idea that it can break down communication system into bits and optimize them, embracing more modern approaches that view communication as an emergent feature of a complex system. In doing so, it can exploit the opportunities presented by complexity and use more realistic methods for changing the game and finding the best plays.

Steven R. Corman is a Professor in the Hugh Downs School of Human Communication and Director of its Consortium for Strategic Communication.

NOTES:

[1] R. Gallagher and T. Appenzeller, ‘Introduction’, *Science*, Vol. 284 No. 5711, 1999, p. 79.

- [2] Shannon, C. and Weaver, W. (1949). *The Mathematical Theory of Communication*. Urbana, IL: University of Illinois Press.
- [3] Berlo, D.K. (1960). *The Process of Communication: An Introduction to Theory and Practice*. New York: Holt, Rinehart and Winston.
- [4] Corman, S. R., Trethewey, A., & Goodall, B. (2007, April). *A 21st Century Model for Communication in the Global War of Ideas: From Simplistic Influence to Pragmatic Complexity*. Report No. 0701. Consortium for Strategic Communication, Arizona State University. Available online: http://comops.org/publications/CSC_report_0701-pragmatic_complexity.pdf.
- [5] The White House (2003, January 24). Establishing the Office of Global Communications. Executive order 13282, Office of Policy Coordination and International Relations.
- [6] Kean, T.H., et al. (2004). *The 9/11 Commission Report*, pp. 376-377.
- [7] Phil Taylor, Institute of Communication Studies, University of Leeds, UK. <http://ics.leeds.ac.uk/papers/vp01.cfm?outfit=pmt&folder=2053&paper=2438>
- [8] For the English translations see Luhmann, N. (1995). *Social Systems*. Stanford University Press, Stanford, CA. (Originally published 1984). For an easier to read introduction, see Chapter 16 of Münch, R. (1994). *Sociological theory: From the 1850s to present*. London: Burnham, Inc.
- [9] Corman, S. R. & Dooley, K.J. (2008, January). Strategic Communication on a Rugged Landscape: Principles for Finding the Right Message. Report No. 0801, Consortium for Strategic Communication, Arizona State University. Available online: <http://comops.org/article/121.pdf>
- [10] Kauffman, S. A., 1993. *Origins of Order: Self-Organization and Selection in Evolution*. Oxford: Oxford University Press.
- [11] Adapted from <http://caimrvaron.rotahall.org/2007/01/02/on-fitness-landscapes> by Koen Crolla. Used by permission.
- [12] <http://www.state.gov/documents/organization/87427.pdf>
- [2] Shannon, C. and Weaver, W. (1949). *The Mathematical Theory of Communication*. Urbana, IL: University of Illinois Press.
- [3] Berlo, D.K. (1960). *The Process of Communication: An Introduction to Theory and Practice*. New York: Holt, Rinehart and Winston.
- [4] Corman, S. R., Trethewey, A., & Goodall, B. (2007, April). *A 21st Century Model for Communication in the Global War of Ideas: From Simplistic Influence to Pragmatic Complexity*. Report No. 0701. Consortium for Strategic Communication, Arizona State University. Available online: http://comops.org/publications/CSC_report_0701-pragmatic_complexity.pdf.
- [5] The White House (2003, January 24). Establishing the Office of Global Communications. Executive order 13282, Office of Policy Coordination and International Relations.
- [6] Kean, T.H., et al. (2004). *The 9/11 Commission Report*, pp. 376-377.
- [7] Phil Taylor, Institute of Communication Studies, University of Leeds, UK. <http://ics.leeds.ac.uk/papers/vp01.cfm?outfit=pmt&folder=2053&paper=2438>
- [8] For the English translations see Luhmann, N. (1995). *Social Systems*. Stanford University Press, Stanford, CA. (Originally published 1984). For an easier to read introduction, see Chapter 16 of Münch, R. (1994). *Sociological theory: From the 1850s to present*. London: Burnham, Inc.
- [9] Corman, S. R. & Dooley, K.J. (2008, January). Strategic Communication on a Rugged Landscape: Principles for Finding the Right Message. Report No. 0801, Consortium for Strategic Communication, Arizona State University. Available online: <http://comops.org/article/121.pdf>
- [10] Kauffman, S. A., 1993. *Origins of Order: Self-Organization and Selection in Evolution*. Oxford: Oxford University Press.
- [11] Adapted from <http://caimrvaron.rotahall.org/2007/01/02/on-fitness-landscapes> by Koen Crolla. Used by permission.
- [12] <http://www.state.gov/documents/organization/87427.pdf>

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 Jebesen 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 Jebesen Center uncovered valuable video footage and chat-room 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 Jebesen 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 Jebesen 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 Riegler, 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," *Jebson Center Research Briefing Series* Vol. 3, No. 1 (January 2008), available at <<http://fletcher.tufts.edu/jebsoncenter/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., *Terroronomics* (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.

About Perspectives on Terrorism

- Perspectives on Terrorism (PT) seeks to provide a unique platform for established and emerging scholars to present their perspectives on the developing field of terrorism research and scholarship; to present original research and analysis; and to provide a forum for discourse and commentary on related issues. The journal could be characterized as 'non-traditional' in that it dispenses with traditional rigidities in order to allow its authors a high degree of flexibility in terms of content, style and length of article while at the same time maintaining professional scholarly standards.

About the Terrorism Research Initiative:

- PT is a journal of the Terrorism Research Initiative (TRI), an initiative that seeks to support the international community of terrorism researchers and scholars especially through the facilitation of collaborative and cooperative efforts. TRI was formed by scholars in order to provide the global community with centralized tools from which to better actualize the full potential of its labours. TRI is working to build a truly inclusive international community and empower it through the provision of collaborative projects to extend the impact of participants' research activities.
- The Journal can be accessed at the following website URL:

www.terrorismanalysts.com