Chapter 6

Terrorist Innovation: Homegrown Terrorism and the Internet

Peter K. Forster [1]

> We face threats from homegrown terrorists – those who live in the communities they intend to attack and who are self-radicalizing, self-training, and self-executing.
>
> *Robert Mueller III, Director FBI, January 20, 2010*

Between September 11, 2001 and October 2009, the United States faced 32 "domestic" incidents of terrorism with thirteen of them occurring in 2009.[2] At this point, it remains unclear whether 2009 represents an increasing trend or merely a spike in domestic incident. It is, however, clear that the threat of domestic terrorism is real. While these incidents share similarities, it is their differences that indicate multiple threats are emerging from multiple sources. Thus, it is important for the counter-terrorist professional to examine both the successful and failed attacks and understand the similarities and differences displayed by the adversary in each case. This can be a laborious process involving many variables. This paper seeks to launch the debate by narrowing the broader subject to one focusing on how terrorist groups innovate and more specifically, assessing how Internet-based communication is influencing the innovation process. The paper concludes that terrorist use of the Internet can be characterized as serving informational, operational, and knowledge transfer needs and that the competition for the communication battle space will continue. Furthermore, it identifies some approaches to combating this effort.

Terrorist use of the Internet is well developed in three relevant areas – recruitment, radicalization, and exploitation of events which includes not only the media coverage but the more subtle process of "peer review" that either encourage or dissuade others from using the tactic. If information transfer represents the first generation use of Internet, the second generation is knowledge transfer which encompasses the enhanced ease and value of the Internet's

[1] Dr. Forster is a professor at the Center for Network Centric Cognition and Information Fusion (NC2IF), College of Information Science & Technology (IST), Penn State University.

[2] Bobby Ghosh, "Domestic-Terrorism Incidents Hit a Peak in 2009," *Time online*, 23 December 2009; www.time.com/time/nation/article/0,8599,1949329,00.html.

growing interactivity that facilitates tactical, operational, and strategic situational awareness. The November 2008 Mumbai attacks epitomized the tactical use of interactive Internet-based technologies. The terrorists' efficiency and effectiveness was enhanced through the gathering, fusion, and sharing of information gathered from a variety of sources. Although in its infancy, knowledge transfer or learning via the Internet, as discreet from information transfer, is a strategic concern for those concerned with counter-terrorism.

To approach this subject, it is important to understand the global context in which the integration of technology is occurring, to identify the role technology plays for terrorist groups and in the terrorism processes, and finally what this says about terrorism in the 21st century and how might it be combated. This study will limit its scope by using information from a variety of cases, primarily but not exclusively US domestic ones, to develop some assertions and possible counter-strategies. As a result of this methodology, it is not meant to be a comprehensive study but one that offers some lessons learned and thus contributes to a broader understanding of a complex and dynamic issue. The study's greatest contribution is to emphasize that terrorism is a dynamic issue and as a result counter-terrorism also must be.

Terrorists or terrorist groups continue to innovate, adapt, and redesign themselves in order to promulgate their objectives. As a result, innovation and learning evolving from what others have done, what has been successful, and what has been the response and reaction is critical. "Copy catting" in the terrorist world is an understood phenomenon and concern. At a more sophisticated level, innovation and learning by and among terrorist groups is neither new nor should it be ignored. Between 1997–2001, the IRA reportedly generated between $ 20 – $ 30 million by providing training to the FARC, the PLO, and the ETA.[3] The Iranian Revolutionary Guard Corps supplied new IED technology and training to Iraqi Shiites as recently as 2007.[4] Today, a growing number of British and American Muslims are travelling to Afghanistan, Pakistan, and Yemen to receive training from the bomb-makers, operational directions from planners, and practical field experience by participating in in-theater attacks. The increasing use of communication technologies has only served to increase inter-organizational and individual adaptation of successful methods and innovation and promises to continue to be a key part of the terrorists' strategy into the future.

Global terrorism in 2010 is characterized by a convergence of need, interest, and means. These are being met by Internet communications that increase accessibility and offer greater interactivity. Virtual communications have become the center of gravity for terrorism in the 21st century. The ultimate control and

[3] Andy R. Oppenheimer, "IRA and Technology Transfer," Presentation to RTI International, Washington D.C., 13 March 2009.

[4] Clay Wilson, *Improvised Explosive Devices (IEDs) in Iraq and Afghanistan: Effects and Countermeasures*, Report for Congress RS22330 (United States: Congressional Research Service, 28 August 2007).

manipulation of this battle space is essential to implementing an effective counter-terrorism strategy. In order to develop and implement such a strategy it is important to understand how the Internet is being used by the jihadist, where are its weaknesses and strengths, and how might it be exploited as an instrument of change.

Communication is the adhesive between the individual and the group and in increasingly geographically disbursed terrorist groups is critically important.[5] US successes at disrupting the activities of "al Qaeda central" in the wake of 9/11 has resulted in an increased need for engaging or permitting "affiliated groups" to extend the battle space. Al Qaeda has made good use of virtual communications to promulgate its Salafist ideology and incite individuals and organized affiliated groups to action. Certainly the message has resonated with some closely linked al Qaeda allies such as the Pakistani Taliban who reportedly provided training to Faisal Shahzad. A more geographically disbursed indication of increased affiliate activity is a May 2010 recording by Abu Basir Al-Wahishi, a reported leader of al Qaeda in the Arabian Peninsula, in which he talks about AQAP's commitment to attacking the US and Western interests.[6] While affiliates seek to act, previously unconnected individuals and groups are coalescing to either perform specific tasks such as David Headley and Tahawur Hussain Rana conspiracy to attack a Danish newspaper or pursue mutual interests such as the reported connections between Hezbollah and South American drug cartels. Third, the Internet has been successfully used to recruit and further radicalize the disenfranchised. Finally, it has enhanced the exploitation of events increasing the reputation of those who move to "violent radicalization" and enhancing the conviction of the self-radicalized, such as Nidal Hasan, to take violent action.

Use of the Internet as a recruitment and radicalization venue is well documented. Using well designed strategies to reach target markets including multilingual websites and blogs, terrorist groups continue to use the Internet to disseminate their message and seek new adherents. Young Muslims who feel disenfranchised from the Western society in which they live explore the Internet for information on extremism, find like-minded individuals, and build virtual groups of radicalized individuals.[7] What has increased is the recruitment of westerners or those sufficiently familiar with western culture to reduce the scrutiny by local law enforcement. However, the vast majority of radicalized individuals do not convert their words to action. Those who do, such as Najibullah Zazi and Shahzad, have sought additional connections beyond those

[5] John Horgan, *Walking Away from Terrorism: Accounts of Disengagement from Radical and Extremist Movements (Political Violence)* (New York: Routledge, June 2009).

[6] Targeted Actionable Monitoring Center (TAMC), Institute of Terrorism Research and Response, 17 May 2010.

[7] Mitchell D. Silber and Arvin Bhatt, *Radicalization in the West: The Homegrown Threat* (New York, NY: The New York City Police Department, Intelligence Division, 2007), p.8, www.nypdshield.org/public/SiteFiles/documents/NYPD_Report-Radicalization_in_the_West.pdf.

offered by the Internet. The predominance of "violent radicalization" processes combines the Internet with some kind of face-to-face interaction and "training" usually outside of the target country. Additionally, a review of cases indicates an increasingly important role for a "spiritual adviser" who continues to act as a mentor to the terrorist once he or she has returned to the country of the attack. Anwar al-Awlaki, killed by a US drone, is well known for providing such a service to Hasan and Shahzad, but Zazi received similar support from the Imam in his Queen's mosque. Apparently, this combination is sufficient to push many towards actions although the level of success remains surprisingly and fortunately minimal.

The third part of the information sharing paradigm is the exploitation of events. Renown and recognition resulting from a terrorist act are often cited as key characteristics or objectives. The live video of the United Flight 175 striking the South Tower on 9/11 encapsulates the impact of disseminating an event. Exploitation has flourished in the video era. The dissemination of Internet-based video to exploit the effectiveness of IED attacks has become a key part of the planning and execution process and has contributed to their expanded use and resulted in the video man, who records the material, becoming an essential element of attack group.

The use of commercial networks has created a global presence for terrorists and has eliminated many barriers to recruitment, radicalization, and exploitation. Notwithstanding, the globalized network is a venue for planning, attack coordination, and learning as well. Hence, the potential for greater terrorists' operationalization of the Internet is significant concern. Like the information sharing paradigm, the knowledge sharing use of the Internet has tactical, operational, and strategic dimensions.

At the tactical level, Internet-based technologies may be used to enhance target refinement and situational awareness while shortening training and implementation times. Irhabi 007 used the Internet as a propaganda vehicle. However, his understanding of the web's tactical value was evident when he connected with US-based terrorists plotting to blow up US sites and proceeded to review photographs of potential targets.[8] A more disturbing example is the previously mentioned Lashkar-e-Taiba coordinated attack on Mumbai. The effective use cell phones, blackberries, and GPS devices, as well as the terrorists' monitoring of social networking sites displaying information from people on the streets and the news media provided enhanced situational awareness for the attackers and their external handler. In this circumstance, the use of technology tactically altered the incident by providing unprecedented command and control and operational flexibility. The terrorists' maneuverability confused security forces and acted as force multiplier. Direct connections between the terrorists and their external handler permitted real-time situational awareness which allowed the attackers to avoid security forces until their

[8] Nic Oatridge, "A world wide web of terror, July 14th," *The Economist*, 23 July 2007, p.28.

choosing, to make decisions on whether and when to exchange or execute hostage, to provide suggestions on the type of weapons to be used, to motivate the terrorist teams when their conviction appeared to wane, and ultimately to order them to commit suicide.

Secretary of Homeland Security, Janet Napolitano, characterized the reality of the networked world as "tools for creating violence and chaos are as easy to find as the tools for buying music online..."[9] The Internet also remains a means of direct communication. Terrorists prefer simplicity and effectiveness. At the operational level, Internet interactivity provides a vehicle by which communications among perpetrators may be maintained and effective approaches may be disseminated. Zazi e-mailed his facilitator in Pakistan about bomb making ingredients as he was preparing for his New York City attack.[10] A simple search of websites yields a plethora of homemade videos of IED attacks and information on construction. As a result their use has proliferated and migrated in Iraq, Afghanistan, and Chechnya. According to the Congressional Research Service (CRS), the extent to which information is being disseminated to IED users has reduced the half-life of new countermeasures against IEDs to a few months.[11] While the privatization of violence has decentralized terrorism, a brief review of failed attacks, as previously noted, still indicates that the on-line learning function appears not to be fully developed.

Strategically, the enhanced Internet interactivity may be used as learning platform in which inspired groups with limited or no connection to a more formal training apparatus of sophisticated groups will increasingly turn to virtual community to learn the "tools of the trade." To date, the results from engaging in the virtual learning environment have failed to meet expectations. While the Internet offers a high level of proliferation, its anonymity makes it hard to confirm the quality of information. Bilal Abdallah and Kafeel Ahmed failed to detonate an improvised explosive vehicle device in London in July 2007, the day before resorting to a suicide mission at the Glasgow Airport. Their case proves the difficulty of constructing a workable explosive device using the web as the primary information source even if the builder has a relatively high level of intelligence. Furthermore, the perpetrators of the Hyderabad attack in August 2007 apparently did not examine lessons learned from the Abdallah and Ahmed's failed attack and made some of the same resulting in only two of 19 exploding in that attack. Limited success continues to lead to would-be terrorists seeking face-to-face training sessions with the bomb-makers and planners. As result, the Internet as an information dissemination vehi-

[9] Janet Napolitano, "Common Threat, Collective Response: Protecting Against Terrorist Attacks in a Networked World" (New York, N.Y.: Council on Foreign Relations, 29 July 2009); www.dhs.gov/ynews/speeches/sp_1248891649195.shtm.

[10] "Charges Unsealed Against Five Alleged Members of Al-Qaeda Plot to Attack the United States and United Kingdom," Press Release (Washington, D.C.: Department of Justice, 7 July 2010); www.justice.gov/opa/pr/2010/July/10-nsd-781.html.

[11] Wilson, "Improvised Explosive Devices (IEDs) in Iraq and Afghanistan: Effects and Countermeasures."

cle rather than the knowledge transfer one remains predominant. The risk of today is the return of the foreign trained radicalized American to the US to initiate an attack. Tomorrow's threat is a sufficiently improved knowledge transfer process that allows the same individual to learn the trade over the Internet without leaving the country. Fifteen years ago, on-line learning was the purview of the for-profit and a handful of traditional universities. Today, on-line learning has been embraced by much of academia and is recognized as a viable learning method. Considering terrorists' propensity for simplicity, efficiency, and security, the continued evolution of a terrorist on-line classroom that begins to address previous weaknesses by integrating synchronistic student-instructor interaction, creating dynamic feedback, and establishing a viable community of practice might well change this dynamic.

Counter-terrorist experts must simultaneously seek to understand the current environment and develop counter-strategies for the future one. Domination of the communication battle space requires merging strategic and tactical approaches that encompass political and legal cooperation as well as proactive physical and virtual interdiction including disinformation and forensics. However, the initial steps are ones of documentation and communication. It is not clear that the threat posed by terrorists' activities on the Internet is readily recognized. Hopefully, the recent revelations about the global scope of the US-UK plot involving Zazi and others should draw attention to the influence of the information society. Still, an active communication campaign by governments is needed to enhance a public-private partnership aimed at curtailing accessibility.

International cooperation is required to reduce Internet influence. Public cooperation takes two forms, one is an agreement on the definition of providing material support to terrorism, which requires agreement on a definition of terrorism. The second is a willingness to prosecute those who violate the former. We are far away from both. However, government standards are insufficient. The private sector needs to be engaged in the process. A study conducted by the Intelligence and Terrorism Information Center revealed that Internet Service Providers (ISPs) from a variety of countries including the US and Canada routinely host terrorists' sites.[12] Controlling communication is a politically charged issue. While the issue of freedom of expression is a primary point of debate, the private sectors is happy to pursue business opportunities. The counter questions are whether a terrorist organization is a terrorist organization and if so should there be a differentiation between physical and virtual actions taken by these organizations? Currently, the legal interpretation is ambiguous and appears to favor the terrorist organization under the auspices of freedom of speech. While discriminating against access to and of information

[12] "The Internet as a battleground used by the terrorist organizations: How Hezbollah and Hamas exploit the Internet in the battle for the hears and minds, and how to combat them" (Intelligence and Terrorism Information Center (ITIC), Israel Intelligence Heritage & Commemoration Center (IHCC), 1 August 2007), p. 6, p. 12.

places one on the edge of a "slippery slope," when does the public good, "shouting fire in the crowded theater," replace a provider's right to freedom of speech? A potential remedy is not suggesting shutting down communication but simply requiring the provider to disclose the organizations whose sites they support and see whether market forces might dictate a change.

With the political and legal responses in disarray, interdiction offers another option. In order to interdict virtually, one must understand the Internet's ultimate use. The primary interdiction strategy has been shutting down sites, which is less than effective. Another approach might be to directly discredit messages by demonstrating the horrors of terrorist tactics – the response to the video of Richard Perle's beheading offers an indication that this method has value. However, the impact on potential radicals is unclear. John Horgan contends that the Internet is insufficient to establish the qualities needed to be a terrorist, but asks whether the terrorist recruiters are seeking "true converts" or "foot soldiers?"[13] To the contrary then, when is the Internet effective in dissuading involvement? Zazi and Shahzad would undoubtedly contend they are "true converts," but their willingness to provide information upon arrest demonstrates a lack of affinity or coalescence with the group associated with "true converts" to the cause and may be more appropriately termed "foot soldiers." However exposure to the horrors of the Salafi jihad did not turn them away. As a result, more research is needed around the soft commitment and when counter-messaging might sway opinions that interrupt the progression from radicalization to violence.

Exploiting the weaknesses of the Internet environment is another interdiction strategy. By focusing on the Internet's weakness for not developing strong coalescence or leveraging its anonymity, eroding trust among Internet users emerges as a strategy. This may be accomplished through disinformation such as counter-training sites or more nefarious methods such as hacking existing sites and changing information. Effective infiltration however requires an in-depth understanding of the adversary which is time consuming. Another method that may be easier to implement is to use the networked world to gather information on potential terrorist's virtual operation. Less group cohesion and increased ability to disseminate information via personal mobile technologies weakens security protocols and increases the possibility of the unintentional or purposeful release of useful information. Capturing and effectively analyzing this data, particularly considering its volume, remains a challenge but as data fusion technologies and techniques improve, monitoring social networking sites, gathering information via participatory sensing, and conducting accurate analysis might become viable strategies for identifying and ultimately tracking Internet terrorists.

Physical interdiction (i.e., arrests, targeted killings, and military action) remain key disruption strategies for a wide variety of terrorist operations. Continued face-to-face training is a weakness to be exploited because it necessi-

[13] Horgan, *Walking Away from Terrorism*.

tates overseas travel and thus enhances an opportunity for identifying perpetrators. Understanding what is sufficient training needed to launch an attack and how long such training might take is important information in separating the potential terrorists from the innocents. Unfortunately, the Internet is reducing the length of face-to-face training time and threatens to disrupt potential models. Zazi returned to the US with notes on his computer on bomb-making. While his communications with "Ahmed" upon returning provided another opportunity for identification, this process reflects the increasing value of the Internet as knowledge transfer mechanism. The perpetrator doing preliminary work on bomb-making on-line, travels to Pakistan for a few days to have his work reviewed, and returns to the US to execute the attack but has a facilitator available to answer questions, if needed. This may be indicative of the new challenge in this area. Physical interdictions also should include targeting those who facilitate the information supply chain. Although the long-term impact of eliminating a spiritual confident such as Anwar al-Awlaki still needs to be assessed, the short-term impact may again be sufficient to dissuade some from following through with terrorist acts. It also might deter others from assuming the role of the spiritual confidant.

Although terrorist groups have a propensity to using "tried and true" methods, they also will innovate and are notorious "copy cats." When the innovation undertaken by one group is successful, it is often adopted by others. The use of the Internet provides an example of how successful innovation proliferates and evolves. This paper has sought to outline how the Internet is being effectively used by terrorist organizations, the potential future uses for the Internet by terrorist groups, and finally offering some possible solutions for consideration. The reality is that we are at the beginning of the use of virtual technologies by terrorist groups to transfer knowledge and leverage the Internet's interactivity capabilities at the tactical, operational, and strategic level. Now is the time for counter-terrorist experts to begin understanding where we have been, where we are, and what the future might bring and how it might be countered.