

despite losing its South Waziristan base. Moreover, the hardest part of the mission for Pakistan's military has only just begun. Routing guerrilla forces with a modern army is not difficult; it is the "hold" phase of counterinsurgency that will prove the most challenging. The militants can now begin to practice the form of warfare at which they are best: sporadic guerrilla attacks against troops.

Moreover, for Pakistan's government to be successful, it will need to move against TTP leaders and cadre in other tribal areas—where they are seeking shelter—which will stretch the military's operations and make it more vulnerable to guerrilla attacks. Public support for military operations could fall if civilians feel increasingly insecure in their own homes, workplaces and cities. Public support for the army's actions in the tribal areas, currently at 51%, could also be jeopardized if the military bows to the pressure of the United States and its NATO allies and takes action against the hideouts of predominately Afghan Taliban militants, such as in North Waziristan and Baluchistan.²⁸ It is clear that Pakistan's security forces are still in the early stages of their perennial fight against Islamist militants intent on weakening the state.

Rahimullah Yusufzai is a senior Pakistani journalist and political and security analyst presently working as Resident Editor of the English daily The News International in Peshawar. He has been reporting on Afghanistan and Pakistan's North-West Frontier Province, Federally Administered Tribal Areas, and Baluchistan since the early 1980s.

The Internet and its Role in Terrorist Recruitment and Operational Planning

By Sajjan M. Gohel

THE VIRTUAL WORLD is fast becoming the most important meeting place for terrorists, and a major venue where extremists can make contact with like-minded individuals. Through these relatively anonymous contacts, an extremist can be brought into the terrorist fold and become physically involved in terrorist plots. Today, there are a growing number of cases in which terrorist groups, or jihadist radicalizers, have used the internet to recruit individuals in the West, providing them a starting point to engage in terrorist activity. By ignoring this developing issue, there is the risk of becoming complacent about an emerging threat that appears to be growing more significant with time.

This article will explore a now defunct network of terrorist cells that were located across the world and which became connected through the internet. By studying this network of cells, which the author identifies as the Digital Jihad Network, it becomes evident that the internet has become a key platform in cell formation and terrorist activity. Moreover, the article will also show how the internet is increasingly being used to recruit Westerners for jihadist operations at home and abroad. Finally, the article will identify the threat posed by "lone wolf" terrorism, which is made possible as a result of jihadist literature, online radicalizers and military training materials available on the web.

The Internet as a Staging Platform: A Case Study of the Digital Jihad Network

The internet is increasingly playing a critical role in linking together disparate terrorist cells around the world. An examination of one major global jihadist network reveals the sheer number of links and connections forged through the internet. The case involved Ehsanul Sadequee, who an Atlanta court found guilty of conspiracy to materially support terrorists in August 2009. His trial explored a nexus of extremists who were connected through the internet to plan attacks and form a global network linking North America, Europe and

South Asia. The trial resulted in eight terrorism cases involving several dozen defendants and years of complex international cooperation.¹

Born in Virginia with parents from Bangladesh, Sadequee exhibited radical sentiments in his teens. Soon after the September 11 attacks, he sent an e-mail to an extremist website expressing his desire to join the Taliban.² Sadequee's extremist activity intensified when he met Syed Haris Ahmed, a Pakistani-American student at Georgia Tech, at a mosque in Atlanta. The two made contact in a password-protected chat room.³ Transcripts of their internet conversations reveal that they fed off each other's outrage at the U.S. wars in Iraq and Afghanistan.⁴

It was in the virtual space, through murky web forums and radical chat rooms such as "Clearguidance," that an extremist network of like-minded individuals, together with Sadequee and Ahmed, was established and where ideas for terrorist training and plotting attacks were discussed.⁵ The network included a group of radicals from Canada, known as the "Toronto 18" led in part by Zakaria Amara, a gas station attendant;⁶ a Bosnian-born Swede named Mirsad Bektasevic who was planning attacks against Western interests in Sarajevo; and Aabid Khan from Manchester, England, who acted as a facilitator for various Pakistan-based terrorist organizations.⁷ The final actor in the network was Younis Tsouli, a former Moroccan diplomat's son living in London whose computer expertise made him the network's hub.⁸ Tsouli had also used the internet to build links to al-Qa`ida operatives in Iraq.⁹

1 "Atlanta Defendant Found Guilty Of Supporting Terrorists," U.S. Department of Justice, August 12, 2009.

2 Ibid.

3 Bill Gillespie, "The Case Against Canada's Plotters," Canadian Broadcasting Corporation, October 14, 2009.

4 Ibid.

5 Ibid.

6 "Toronto 18 Video Evidence Released," Canadian Broadcasting Corporation, October 20, 2009.

7 "Atlanta Defendant Found Guilty Of Supporting Terrorists."

8 Tsouli infamously was able to hack an FTP server operated by the Arkansas Highway and Transportation Department and turn it into an al-Qa`ida message board, providing detailed information on the art of hacking.

9 "Terrorist Use Of The Internet," Combating Terrorism

28 This poll is available at Gallop Pakistan, the findings of which were published on November 3, 2009.

In early 2005, Ahmed and Sadequee traveled to a Toronto mosque to meet with some members of the Toronto 18 to discuss possible attacks on the Centers for Disease Control and Prevention in Atlanta and oil refineries.¹⁰ Aabid Khan also flew in from London for the gathering.¹¹ None of the individuals had formal terrorist training, so they agreed as a first step to travel to Pakistan and spend three months in a training camp run by Lashkar-i-Tayyiba (LT), a Pakistani terrorist group that

“Through its relatively secure anonymity, the internet has become a key medium for Westerners to identify and connect with jihadist radicalizers and recruiters.”

orchestrated the Mumbai terror siege in November 2008.¹² Khan would make the necessary arrangements with the LT so that the network’s members could travel to Pakistan and begin training. Khan was also in contact with Jaysh-i-Muhammad (JM), another terrorist group in Pakistan that was partly involved in the abduction and murder of U.S. journalist Daniel Pearl in Karachi.¹³ The network’s members rented two basement apartments in Toronto as a

Working Group (CTWG), George C. Marshall European Center for Security Studies, June 16-17, 2009.

10 Gillespie.

11 Ibid.

12 Aryn Baker and Jyoti Thottam, “The Making of a Mumbai Terrorist,” *Time Magazine*, March 8, 2009. Interestingly, the anonymous nature of the internet also served as a tool to aid and mask the LT’s Mumbai attack. One of the handlers for the group sent an e-mail to an Indian TV channel claiming that the “Deccan Mujahidin” was responsible for the plot. Deccan, being an area in southern India, implied the plot was indigenous. Investigations subsequently found that the e-mail message originated in Lahore in Pakistan, before being routed to different locations through an anonymous “re-mailer” service. This is a system that acts as a mail intermediary and allows users to send e-mails to a destination anonymously. The ploy successfully misled many as to the origins of the group and could serve to act as a template for future attacks.

13 Nick Fielding, “Omar Saeed Sheikh: The British Jackal,” *Sunday Times*, April 21, 2002.

base from where they and others part of their internet chat group could gather before traveling to Pakistan.¹⁴

After their planned paramilitary training trip in Pakistan, the network intended to return to Toronto and choose targets to attack in Canada, the United States, the United Kingdom and continental Europe. They anticipated the attacks to be possibly the most coordinated terrorist assault ever seen. A few weeks after their trip to Toronto, Ahmed and Sadequee visited Washington, D.C. where they made more than 62 video clips of potential targets, including the Pentagon, the Capitol, and the World Bank headquarters.¹⁵ Sadequee e-mailed the scouting videos to Tsouli and Khan.¹⁶

Sadequee eventually traveled to Bangladesh to get married, and he continued his participation in the global network. Although Ahmed was able to travel to Pakistan, he and Khan were not able to arrange training for the global plotters because of the logistical difficulties in bringing them all together. In October 2005, Sadequee communicated via e-mail from Bangladesh with Tsouli in London and Bektasevic in Sarajevo, as the latter was obtaining explosives and weapons for a plot.¹⁷ They discussed a propaganda video that Bektasevic was preparing that would announce the formation of a group they called “Al-Qa`ida in Northern Europe.”¹⁸

By this time, however, law enforcement and intelligence agencies had finally traced their internet communications and were monitoring their activities on the web, in addition to keeping them under close physical surveillance. Within days, in October 2005, Bektasevic was apprehended in Sarajevo and British police arrested Tsouli in London.¹⁹ Bektasevic’s arrest revealed that he had already assembled a suicide vest attached to a detonator, suggesting

14 Ibid.

15 Sebastian Rotella, “Georgia Man Convicted of Aiding Terrorism Groups,” *Los Angeles Times*, August 13, 2009.

16 Ibid.

17 Ibid.

18 “Terrorist Use Of The Internet.”

19 Gordon Corera, “Al-Qaeda’s 007,” *TimesOnline*, January 16, 2008.

his plot was imminent.²⁰ Tsouli’s encrypted hard drive provided a wealth of information that led investigators to pursue other militant links across the world. Both Tsouli and Bektasevic are serving lengthy prison sentences after being convicted on terrorism-related charges. In March 2006, Ahmed was arrested in Atlanta by the FBI and Sadequee was detained in April 2006 in Bangladesh. Ahmed was convicted in June 2009 for conspiracy to provide material support to terrorism in the United States and abroad.²¹

In Britain, once the evidence had been gathered from the other plots, authorities quickly moved to apprehend the remaining members of the network. In April 2006, Scottish police arrested a student, Mohammed Atif Siddique, as he was in the process of boarding a flight to Pakistan to meet Aabid Khan who had been indoctrinating and radicalizing Siddique through the internet.²²

In June 2006, Toronto witnessed the dramatic arrests of several men also connected to the network. The Toronto 18 cell had been infiltrated by two police informants and was accused of planning attacks on two Toronto buildings and an Ontario military base. The cell members had in their possession large quantities of what they thought was ammonium nitrate.²³ In October 2009, Zakaria Amara pleaded guilty to knowingly participating in a terrorist group and intending to cause an explosion for the benefit of a terrorist group.²⁴ Investigations revealed that members of the Toronto cell, including Amara, were influenced by the internet sermons of U.S.-born Islamist ideologue Anwar al-Awlaki, who is believed to be based in Yemen.²⁵

20 Ibid.

21 “Atlanta Defendant Found Guilty Of Supporting Terrorists.”

22 *HMA v. Mohammed Atif Siddique*, October 23, 2007; Swann.

23 “Toronto 18 Video Evidence Released.”

24 Ibid.

25 Unlike other radicals, Anwar al-Awlaki understands Western culture and has used the internet to tailor his messages to directly influence young impressionable people. During his time in the United States, he served as an imam at San Diego’s Rabat mosque, where he met future 9/11 hijackers Khalid al-Midhar and Nawaf al-Hazmi and developed a close relationship with them. Al-Awlaki was also in communication through the internet with Nidal

Four days after the Toronto plotters were arrested, Aabid Khan was detained at London's Heathrow Airport as he disembarked from a flight from Islamabad in June 2006.²⁶ When police searched his luggage they found two computer hard drives, 16 CDs and a quantity of documents.²⁷ The contents of the material showed Khan inciting others to participate in terrorist activity through the internet, and evidence also showed that he had facilitated trips to Pakistan.²⁸ In August 2008, Khan was convicted of being a terrorist propagandist.²⁹

Hammad Munshi, a 16-year-old British schoolboy, was also caught in the network, becoming Britain's youngest convicted terrorist.³⁰ Munshi was a friend and recruit of Aabid Khan, and was convicted in September 2008 of possessing materials that were likely to be used in acts of terrorism.³¹ Munshi collected instructions for making napalm, explosives and suicide vests from the internet.³² A quantity of propaganda videos and audio recordings, stored on the family computer, were also found during a search.

This case study of the Digital Jihad Network reveals how the internet is being used as a platform to facilitate contact among like-minded aspiring jihadists. Moreover, it also plays a role in the preparation and plotting of

Malik Hasan, the U.S. Army officer who is charged with killing 13 people and wounding 30 at Fort Hood, Texas in November 2009. See Michelle Shephard, "The Powerful Online Voice of Jihad," *Toronto Star*, October 18, 2009; *The 9/11 Commission Report* (New York: W.W. Norton & Co., 2004), p. 221; Theo Emery, "The FBI Probe: What Went Wrong at Fort Hood?" *Time Magazine*, December 10, 2009. Al-Awlaki was characterized in court testimony as an inspiration by two of the six people convicted on conspiracy and other charges in a plot to kill U.S. military personnel at Fort Dix. A Facebook page devoted to the ideologue once had thousands of supporters. Following the Ft. Hood shooting, the page was removed by the website administrators.

26 Swann.

27 "Cases Concluded in 2008," The Counter-Terrorism Division of the Crown Prosecution Service, undated.

28 Ibid.

29 Ibid.

30 Swann.

31 Ibid.

32 Jenny Percival, "Yorkshire Teenager Becomes Britain's Youngest Convicted Terrorist," *Guardian*, August 18, 2008.

attacks. In the case of this network, it allowed members to come into contact with individuals with actual physical ties to terrorist groups, such as to the LT in Pakistan. The dismantling of the network led to dozens of arrests around the world. Worryingly, this template has also been used subsequently in the United States to recruit people for terrorist activity abroad.

Al-Shabab Recruits in the United States and the Pakistan-Virginia Case

In November 2009, federal authorities unsealed terrorism-related charges against men they say were key actors in a recruitment drive that led young Somali-Americans to join al-Shabab, a Somali insurgent group and an al-Qa`ida affiliate. In total, authorities have implicated 14 people in the case. Perhaps the most notorious is Zakaria Maruf, an American-Somali who had left Minnesota for southern Somalia to link up with al-Shabab and subsequently recruited men from the United States through a variety of means, including the internet.³³

This was the case of Mohamoud Hassan, a student at the Carlson School of Management, whose path toward extremism began through the internet with searches for jihadist videos and jihadist chat rooms. Like the Toronto 18, Hassan listened to the audio lectures of Anwar al-Awlaki.³⁴ Hassan then began to communicate frequently with Maruf who established contact through listservs, an antiquated form of sending e-mails, and conference calls arranged by an associate who distributed several hundred numbers and passwords so people could establish contact securely.³⁵

In November 2008, Hassan turned his back on a university education and with two other students left for Somalia to join an al-Shabab training camp where he linked up with his internet recruiter Maruf.³⁶ In September 2009, Hassan's grandmother received news from Somalia that her grandson was killed.

33 Amy Forliti, "Details Emerge About Somali Terrorists' Recruiting Methods," Associated Press, August 25, 2009; Andrea Elliott, "A Call to Jihad, Answered in America," *New York Times*, July 12, 2009.

34 Elliott.

35 Ibid.

36 Ibid.

It is unlikely that he will be the last Somali-American recruited by al-Shabab handlers to fight in Somalia. His case is a mere example of the problem.³⁷

More recently, in December 2009 five men from northern Virginia were arrested in Sargodha in Pakistan's Punjab Province on suspicion that they were plotting terrorist attacks and planned to fight in Afghanistan.³⁸ The Pakistani police interrogation report identified one of the suspects as Ahmed Abdullah Minni, who it claims regularly went on YouTube to watch Taliban attacks on the U.S. military in Afghanistan and left comments praising the actions.³⁹ His comments attracted the attention of extremists, and he was eventually contacted through the internet by a mysterious individual using the alias "Saifullah."⁴⁰ A Yahoo! e-mail account was set up so the accused and Saifullah could communicate.⁴¹

The suspects planned to travel to Pakistan, and then to Afghanistan. Once they arrived in Pakistan's port city of Karachi, the men left for Hyderabad.⁴² Pakistani authorities claim that they tried to connect with JM and Jama`at-ud-Da`wa (JuD), the parent wing of LT.⁴³ According to Pakistani authorities, neither JuD nor JM expressed any interest in recruiting the men.⁴⁴ During the past 10 years, however, both groups have actively recruited foreigners. It is likely that the two groups are reluctant to induct Americans at this time in light of the recent case of David Headley, a

37 Laura Yuen, "Fifth Minnesota Man Dies in Somalia," Minnesota Public Radio, September 5, 2009. In December 2008, al-Awlaki addressed al-Shabab followers in one of his blog entries stating, "We are following your recent news and it fills our hearts with immense joy."

38 "Interrogation Report, 'Profiles of the Foreigners Held,'" Punjab Police, Sargodha, Punjab Province, December 11, 2009.

39 Ibid.

40 Ibid.

41 Ibid. Interestingly, to avoid interception by law enforcement and intelligence agencies, e-mails were never sent from the account, but messages were left in the draft folder and deleted after reading, the online version of a "dead letter drop."

42 "Mosque of Americans Arrested in Pakistan Plans Investigation," CNN, December 11, 2009.

43 Jama`at-ud-Da`wa was proscribed by the United Nations following the Mumbai terror siege attacks.

44 "Interrogation Report, 'Profiles of the Foreigners Held.'"

Chicago resident accused of conducting reconnaissance on behalf of LT during the preparation for the 2008 Mumbai attacks, as well as conspiring to attack the offices of the Danish newspaper, *Jyllands-Posten*. Other reports state that the two terrorist groups thought that the men were working on behalf of Western intelligence agencies.

U.S. officials are exploring possible criminal charges against the northern Virginia men. The mystery man, Saifullah, has yet to be identified. The recent case is concerning because it shows how Westerners, in this case Americans, can be induced to partake in jihad through contacts made over the internet and travel to Pakistan for direct training. In many ways, the case is similar to the global network tied to Ehsanul Sadequee.

The Internet and its Role in "Lone Wolf" Terrorism

Another growing concern is the issue of "lone wolf" terrorism. This refers to an individual not connected to any particular cell or network, but who becomes radicalized as a result of jihadist literature online. Moreover, the individual can also become trained in explosives and other weapons through military training manuals available on the internet. The emergence of these self-generated violent extremists presents a significant challenge to law enforcement because they have few, if any, physical organizational links to other collaborators. This means that warning signs may only be seen in hindsight, after a plot has already been executed.

One of the most disturbing cases of "lone wolf" terrorism is Nicky Reilly, who attempted to carry out a suicide bomb attack in May 2008 in Exeter in the United Kingdom. Reilly, who has Asperger's syndrome, made an improvised explosive device (IED) out of soft drink bottles filled with paraffin, caustic soda and nails. He tried to detonate the IED in a café, yet the bombs exploded prematurely and Reilly was the only person injured.⁴⁵

Reilly, a Muslim convert, researched how to make IEDs on the internet. He also used the internet to obtain the IED's

components, as well as to investigate potential targets.⁴⁶ Importantly, he was in frequent contact via the internet with two unidentified men from Pakistan, with whom he discussed his intentions and from whom he received encouragement and information.⁴⁷ The unidentified individuals answered his questions and directed him to bomb-making websites.

Reilly's case is concerning because he never traveled to a foreign country for training, which is one reason why he was not discovered by authorities until he executed his plot. His case presents a

"Cases of 'lone wolf' terrorism show how the internet has the ability to at least somewhat become a substitute for physical military training, although the pattern so far implies that internet training alone reduces operational effectiveness."

worrying scenario because it was almost completely domestic, other than the virtual contacts forged over the internet. Furthermore, his two unidentified contacts were not apprehended, which means they can continue their attempts to foment jihad in Western countries through contacts made on the internet. Cases of "lone wolf" terrorism, of which Reilly is only one, show how the internet has the ability to at least somewhat become a substitute for physical military training, although the pattern so far implies that internet training alone reduces operational effectiveness.

Conclusion

Through its relatively secure anonymity, the internet has become a key medium for Westerners to identify and connect with jihadist radicalizers and recruiters. The internet is part

of the process connecting aspiring terrorists with like-minded individuals or actual terrorists operating out of countries such as Pakistan and Somalia. After consolidating relationships over the internet, the recruits can then plot and plan mass casualty attacks while remaining in contact with their handlers through the world wide web.

These factors raise serious challenges for Western governments, whose citizens are being lured into the terrorist fold over the internet. The internet has become a starting point for those seeking persuasive jihadist information, ideological guidance, practical military instructions and connections with jihadist handlers. To combat this threat, counterterrorism efforts will need to increasingly factor in the virtual battlefield in addition to the physical battlefield.

Dr. Sajjan Gobel is Director for International Security at the Asia-Pacific Foundation, an independent intelligence and security think-tank. He received his Ph.D. in International History from the London School of Economics & Political Science (LSE). His doctoral thesis, entitled, "The Evolution of Egyptian Radical Ideological Thought from Hasan al-Banna to Ayman al-Zawahiri," is in the process of being published. Dr. Gobel's primary research interests include: the security challenges in South Asia, the Middle East and the Horn of Africa and the connection with the West; radical ideological thought both present and historical; and the role that New Media plays in transnational terrorism.

⁴⁶ Adam Fresco, "Bomber Nicky Reilly was Brainwashed Online by Pakistani Extremists," *The Times*, October 16, 2008.

⁴⁷ Ibid.

⁴⁵ *HMA v. Nicky Reilly*, January 30, 2009.