FORT HOOD ATTACK • UNDERCOVER INFLUENCE • CYBER JIHAD • S.A.R.S.

The Counter Terrorist

Official Journal of the Homeland Security Professional

FEBRUARY/MARCH 2010

VOLUME 3 • NUMBER 1

U.N. PEACEKEEPING OPERATIONS IN AFRICA

0 74470 24633 6 02>

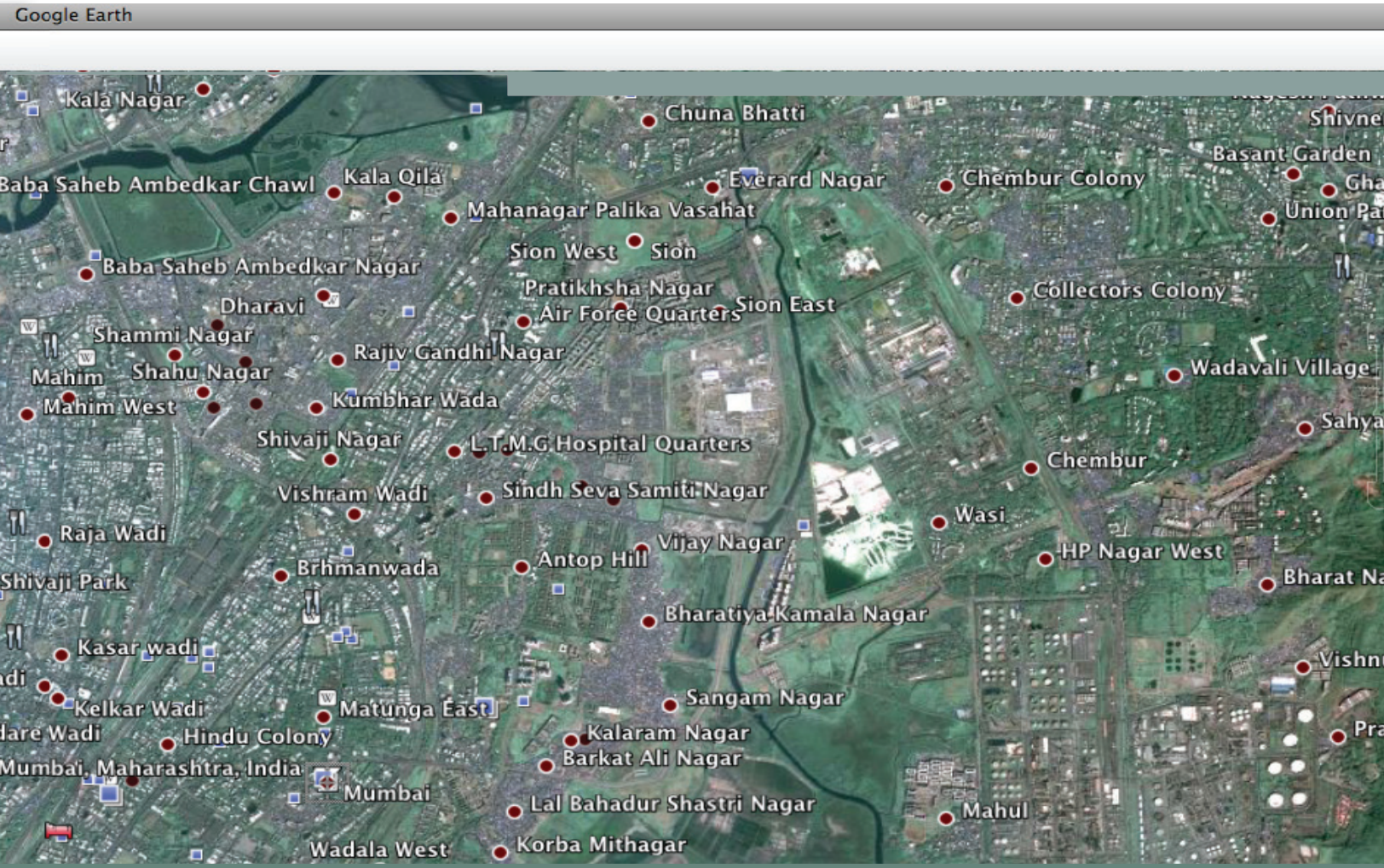
FEBRUARY/MARCH 2010
USA/CANADA $5.99

An SSI® Publication

www.thecounterterroristmag.com

By John Bumgarner and Michael Mylrea

Media coverage of jihadists has often focused on acts of violence in the physical world, such as suicide bombings and shooting sprees. Less publicized, however, is the growing importance of the virtual world to the extremist groups that make the news. The free territory of cyberspace offers them a virtual sanctuary where they may plan, train for, and finance physical attacks. The jihadists' operations are facilitated by web-based services and applications, such as social networking sites, encryption programs, and streaming video.



Organizations such as al-Qaeda and factions of the organizations Hamas and Hezbollah have used the Internet to propagate their extremist religious ideology. Members of these organizations use many of the most popular social-networking sites, including Facebook, Friendster, LiveJournal, MySpace,[1] and Twitter,[2] to spread propaganda. By providing access to a large network of users, these portals facilitate recruiting and fund-raising by extremist groups. These groups also use traditional social-networking sites, such as Yahoo! Groups or Google Groups.

The architecture for private, quasi-anonymous communication that is provided by many social-networking sites shelters members of extremist organizations from detection by most law enforcement efforts. Many social-networking sites feature user controls that allow extremist groups to prevent or detect infiltration. For example, individuals who seek to become group members might have to be approved or invited to join the group. Individuals requesting membership may thus be thoroughly vetted before they are permitted to view the content on the group's website or to participate in forum discussions with other group members. Additionally, many social-networking sites permit groups to monitor forum content

The 2008 attacks in Mumbai, India, involved the Internet at multiple stages. Prior to launching the attacks, the organizers used a variety of Internet sites, such as Google Earth, to research their targets.[16]

Some extremist websites are hosted on servers within the physical boundaries of the United States.

or other website activities. These elements are critical to ensuring the group's operational security.

Extremist groups have also learned to operate on social networking sites in a covert fashion. For example, public content may be carefully controlled to conceal the group's true purpose. A simple masking technique avoids using any phrases (e.g., Allahu Akbar) or terms (e.g., Al-Mujahidin) that would trigger a search engine detection alarm.

Despite the advantages of social-networking sites for centralized and controlled collaboration, they also pose security risks to the extremist sects that use them. Infiltration is one danger; just as extremist groups will attempt to hide their operations, law enforcement and intelligence agencies will attempt to discover them. Security may also be compromised because extremist groups do not own the social-networking sites they use. To counter these risks, some

extremists have established their own portals, most of which function on systems controlled by third-party hosts who are unaware of the extremists' activities.[3] Some extremist websites are hosted on servers within the physical boundaries of the United States. Access to these portals is often heavily guarded by the extremist groups that control them. For example, some groups restrict connections by their location of origin (e.g., Egypt). Access to forums may also be password protected, and forum participants may be thoroughly vetted before receiving a password. On the forums, participants discuss a variety of topics, from religious beliefs to the construction of improvised explosive devices (IEDs).

Forum organizers have begun to mask their communications through encryption, which presents a formidable challenge to efforts by law enforcement agencies to monitor the extremist groups' activities. As early as 1998, Louis Freeh, former director of the Federal Bureau of Investigation, testified before a Senate Appropriations Subcommittee that "encryption has become the most important issue confronting law enforcement. Widespread use of robust, non-recoverable encryption is beginning to devastate our ability to fight crime and terrorism."[4]

Evidence shows that extremist groups use and distribute sophisticated encryption programs. For example, in response to growing fears about eavesdropping, the Global Islamic Media Front[5] released an encryption application called *Asrar Al-Mujahidin* ("Mujahideen Secrets")[6] first on several restricted forums and later on dozens of publicly accessible file-sharing sites. Mujahedeen Secrets supports several advanced encryption algorithms, including the Advanced Encryption Standard (AES). In 2001 the U.S. government approved the AES to safeguard sensitive public information,[6] and in 2003 the National Security Agency approved the AES to protect top secret information.[7] Hezbollah has praised the brilliance of encryption programs such as Mujahedeen Secrets, which allow its members to communicate jihad messages without fear that they will be deciphered by "the Americans."

Extremist groups distribute other applications and programs on their websites as well. Many of these sites are digital repositories for bootleg copies of commercially available programs that might help members of an extremist group evade detection while planning or executing an attack. For example, some applications conceal Internet-surfing activities.[8] Others are designed to perform highly advanced anti-forensic tasks, such as securely deleting files via methods approved by the U.S. Department of Defense or erasing incriminating Internet-surfing trails from a member's computer.[9]

The extremist groups also distribute training materials on their restricted portals. These materials include copies of training manuals used by the U.S. military, especially the U.S. Army, which are available on many extremist sites. The manuals, which describe combat techniques, further link these extremist groups to violence. For example, *U.S. Army FM 3-23.35 Combat Training with Pistols, M9 and M1911*, which describes fundamental marksmanship techniques, is available for download from several extremist sites. The manual illustrates advanced shooting skills, such as the "controlled pair" or "double tapping" technique, which allows a trained marksman to quickly neutralize an opponent with two shots to the center of the chest or head at close range. One extremist site that provides access to this

manual advises its members to use public gun ranges to improve their handgun skills.[10]

Another manual, the *TM 31-210 Improvised Munitions Handbook*, created by the U.S. Army for Special Forces, has also been distributed on the websites of extremist groups. This technical manual offers practical advice on the construction of IEDs from materials that may be readily purchased from most home improvement centers. Although the techniques described in this book have been successfully exploited by terrorist groups for decades, the Internet has clearly lowered the cost of distributing these instructions.

Many jihadist organizations also develop and distribute their own training materials via the Internet. Improvements in streaming online video have expanded the capabilities of these virtual training aids. Web-based distribution confers other advantages to the groups as well. For example, web-based training may be more secure than physical training camps, which are vulnerable to physical attacks. Furthermore, aerial bombardment or skirmishes with ground forces pose a threat not just to the training camps but also to the people who attend them. By contrast, if a web-based training site is shut down, its members remain unharmed and live to fight another day.

Web-based distribution also allows jihadist organizations to train more individuals in combat techniques.[11] Web-based training materials may be disseminated quickly to members of extremist groups throughout the world. The materials may be downloaded (duplicated) by members at almost no additional cost and may be used by a large number of members simultaneously. The materials may also aid extremist organizations in their efforts to recruit and indoctrinate new members.

Virtual-training materials developed by extremist groups cover a wide range of topics, including IED construction and guidelines on the use of shoulder-fired surface-to-air missiles.[12] One video shows how to make an IED from common household items, such as a propane gas cylinder and a cell phone to serve as a detonator.[13] The video also highlights the importance of using nails or other standard construction materials to create shrapnel that make the device more lethal. Another video demonstrates techniques for making a vehicle-borne improvised explosive device, or car bomb.[14] Car bombs have been used successfully in many terrorist attacks, including attacks on the Marine barracks in Beirut, Lebanon, in 1983, Khobar Towers in Saudi Arabia in 1996, the U.S. embassy in Kenya in 1998, and the Danish embassy in Islamabad, Pakistan, in 2008.

Many videos advertise the effectiveness of radical violence by extremist groups. For example, some videos show the tactical effectiveness of roadside bombs used against coalition forces in Iraq. Others document brutality inflicted by extremist groups on their captives. Some videos highlight the path to martyrdom chosen by other group members. The *As Sahab Foundation for Islamic Media Publication*, which has supported various organizations known to be al-Qaeda Associated Movements (AQAM), created a unique video depicting the 2008 bombing of the Danish embassy that blends several of

these elements.[15] The video begins with an interview with a suicide bomber. It then uses computer animation to simulate a suicide bombing attack on the Danish embassy that ends in a massive fireball. The video has been widely distributed on many websites, including YouTube.

Video applications also play a pivotal role in the psychological warfare operations of extremist groups. Many videos direct persuasive communications toward a specific audience to propagate the groups' ideologies. AQAM organizations are increasingly featuring members who speak English in videos aimed at Western audiences. The release of a video may also be timed to achieve the greatest possible impact. For example, a cell-phone video of an IED attack may be released immediately following the event, which attracts media attention and possibly an ancillary following by the general public. The video may thus intensify the emotional response of the public to an attack that has taken place.

Extremist groups use the Internet not only to plan, prepare for, and publicize physical attacks, but also to execute them. The 2008 attacks in Mumbai, India, involved the Internet at multiple stages. Prior to launching the attacks, the organizers used a variety of Internet sites, such as Google Earth, to research their targets.[16] Satellite images and maps available online enabled the attackers to reconnoiter their targets in Mumbai remotely. Using Google Earth, the attacks could be planned from afar with great precision, down to the entrances and exits to be used at the primary targets. Such detailed preparation would reduce the likelihood of encountering unforeseen obstacles along the assault paths and increase the effectiveness of the attacks.

On the day of the Mumbai assault, the attackers reportedly communicated through the Internet with handlers in other locations. Armed with disposable cellular phones that were configured with subscriber identity module (SIM) cards obtained from different countries, the attackers shared updated intelligence with their handlers, who were listening on Voice over Internet Protocol equipment[17]. These steps made it more difficult for law enforcement agencies to intercept the calls or trace them after the attacks had taken place. It has also been speculated that the handlers used real-time television coverage to track the location of the police units and counter-terrorism commandos that had responded

to the attacks. Updates based on the media coverage were transmitted to the attackers via their cellular phones.[18]

The Mumbai attacks are not the first example of the exploitation of online imagery technologies by an extremist group for remote target reconnaissance. It has been alleged that al-Qaeda has used similar technologies to study potential targets within the United States, such as nuclear power plants and natural gas storage facilities.

There is evidence that extremist groups are planning to use the Internet itself as a weapon to attack critical infrastructure in the United States and disrupt the national economy. Computers captured from al-Qaeda show evidence of research on the logistics of cyber attacks against computers that control critical utilities, such as electric power plants and water treatment facilities[19]. Transportation systems have also been targeted. These critical computer systems are also vulnerable to physical attacks. For example, an explosive charge could be strategically positioned to incapacitate a communications choke point that routes emergency (911) calls. If people were unable to report incidents, emergency services would be delayed in their response.

By providing a number of applications and services that substitute for face-to-face contact and physical training camps, the Internet enables extremist groups to promote their agenda. Cyber-jihadist elements use the Internet to recruit, indoctrinate, and train new members to wage violent attacks. These groups have also used the Internet to coordinate physical attacks as they unfold. Furthermore, some extremist groups have begun to investigate ways to use the Internet itself as a weapon to launch cyber attacks that would have catastrophic consequences in the real world. Extremist groups will use the Internet more and more as their members gain more technical knowledge and as technology continues to improve. As cyber-jihadist elements continue to flourish, efforts to combat them must also grow more sophisticated. ●

ABOUT THE AUTHORS

Mr. Bumgarner is the research director for security technology at the U.S. Cyber Consequences Unit and a senior research fellow at the Fletcher School of Law and Diplomacy at Tufts University. He was formerly a member of the U.S. Army.

Mr. Mylrea is a Fulbright and critical Arabic language scholar in the Middle East. He has worked on various research projects for the Jebsen Center for Counter-Terrorism, Harvard Berkman Center for Internet & Society, and MIT Lincoln Laboratory.

ENDNOTES

[1] http://viewmorepics.myspace.com/index.cfm?fuseaction=user.viewAlbums&friendID=481927459

[2] Accessed at: http://twitter.com/arrahmah

[3] The Islamic website ekhlaas.org has been hosted by several United States service providers operating in Florida and Minnesota.

[4] United States Senate Appropriations Subcommittee on Commerce, Justice, and State, the Judiciary, and related Agencies. Federal Bureau of Investigation 1999 Budget Request. 105th Congress. Washington, D.C. March 3, 1998.

[5] Global Islamic Media Front Blog. http://gimf.wordpress.com

[6] Federal Information Processing Standards Publication 197. Announcing the Advance Encryption Standard (AES). Accessed at: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[7] NSA Suite B Cryptography. Accessed at: http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml

[8] Webroot - Window Washer. http://www.webroot.com/En_US/consumer-products-windowwasher.html

[9] O&O Software - Safe Erase. http://www.oo-software.com/home/en/products/oosafeerase/

[10] How Can I Train Myself for Jihad. Accessed at: http://www.alqimmah.net/showthread.php?p=19477

[11] Maujahideen Training/Fighting (Martial Arts). Accessed at: http://www.youtube.com/watch?v=Fh86eTspLPY

[12] Al-Qaeda Virtual Training. Accessed at: http://www.youtube.com/watch?v=yQFsQt8IJhQ

[13] Media Department of Ansar al-Sunnah (Army of Sunni Supporters), As Sahab Video. Accessed at youtube.com

[14] Media Department Ansar al-Sunnah (Army of Sunni Supporters), As Sahab Video. Accessed at: www.youtube.com/watch?v=LwjlCKuIGjc

[15] Accessed at: http://www.youtube.com/user/3rbi1#p/a/u/2/Z_dCl6qs-yc

[16] Jeremy Kahn, "Mumbai Terrorists Relied on New Technology for Attacks." *The New York Times*, December 8, 2008. Accessed at: http://www.nytimes.com/2008/12/09/world/asia/09mumbai.html

[17] Rhys Blakely, "Mumbai Terrorists Thwarted Security Agencies by Using Internet Telephones." *Times Online,* December 10, 2008. Accessed at: http://www.timesonline.co.uk/tol/news/world/asia/article5317075.ece

[18] Jeremy Kahn, "Mumbai Terrorists Relied on New Technology for Attacks." *The New York Times*, December 8, 2008. Accessed at: http://www.nytimes.com/2008/12/09/world/asia/09mumbai.html

[19] Kelli Arena and Ensor, David, "U.S. Infrastructure Information Found on al Qaeda Computers." *CNN*, June 27, 2008. Accessed at: http://edition.cnn.com/2002/US/06/27/alqaeda.cyber.threat/index.html