CTX

Volume 2, No. 4 2012

SPECIAL ISSUE

Social Media in Jihad and Counterterrorism

ISSN 2162-6421 (online)
11/1/2012

CTX
Combating Terrorism Exchange

From the Editor

Welcome to our first special issue of CTX, "Social Media in Jihad and Counterterrorism," which is devoted to a wide-ranging exploration of social media and counterterrorism. Social media have become valuable tools for combating crime and terrorism. According to LexisNexis® Risk Solutions, four out of five respondents to their survey of law enforcement professionals reported using social media, particularly Facebook and YouTube, to aid investigations. One officer said he believed his department's use of social media allowed personnel to defuse a terrorist threat involving students at a local high school. Two-thirds said they thought access to social media helps solve crimes more quickly.

To better understand the role of social media in combating terrorism, the Naval Postgraduate School (NPS) in Monterey, California held a small workshop on Social Media and Counterterrorism this past June. Sponsored by the Combating Terrorism Fellowship Program, the workshop brought together a diverse group of people, including researchers, law enforcement and military officers, and media experts from the United States, Ireland, and the Philippines. Participants were invited to submit papers for inclusion in this special issue of CTX.

We are delighted to present here six papers that we received from participants of the workshop. In addition, we have included a seventh paper that was submitted independently to the journal, but which fit well with the workshop theme of social media and counterterrorism.

The first piece, "The New Battlefield: The Internet and Social Media," by Maria A. Ressa, CEO and executive editor of the online social news source *Rappler*, describes the role of social media in the jihad in the Philippines. A veteran journalist who served many years as CNN's bureau chief in Manila and then Jakarta, Ressa's article is an expanded excerpt from her book *10 Days, 10 Years: From Bin Laden to Facebook.*

The next two articles focus on the online social environment associated with the global jihad. "From al-Zarqawi to al-Awlaki: The Emergence and Development of an Online Radical Milieu," by Dr. Maura Conway of Dublin University, discusses the online radical milieu that gives rise to violent jihad. Conway shows that many of the characteristics found in traditional radical milieus also appear in the online versions, although the latter have unique features as well. She also observes that even so-called "lone wolf" terrorists these days are at least partially the product of some kind of online radical milieu.

"Rethinking the Role of Virtual Communities in Terrorist Websites," by Dana Janbek of Lasell College in Massachusetts and Paola Prado of Roger

Williams University in Rhode Island, examines the extent to which terrorist-related websites have embraced interactive Web 2.0 applications that build community through commentary, social networking, and streaming video. Janbek and Prado found that for the most part, the sites they evaluated did not fulfill this function, offering instead static, tightly moderated, and effectively closed environments that sought to inform, persuade, and transmit a particular message rather than support the free exchange of ideas.

The fourth article, "Countering Individual Jihad: Perspectives on Nidal Hasan and Colleen LaRose," by Peter Kent Forster, considers two cases where individuals embraced a violent jihadist ideology on their own, but then were incited to commit violence through their online interactions or, using Conway's terminology, through their online radical milieus. Like Conway, Dr. Forster shows that "lone wolf" jihadists rarely act in isolation, and argues that it might be possible to prevent terrorist acts by examining online activities for signs of intent to commit terrorism.

In "Artisanal Intelligence and Information Triage," Aaron Weisburd, founder of Internet Haganah and director of the Society for Internet Research, discusses how a forensic exploration of social media can detect unknown terrorists. Drawing on his own experience in counterterrorism and intelligence-related activities, Weisburd offers a targeted approach that focuses on the social network, using a variation of "snowballing" along with information triage.

Some of the workshop participants examined the application of social media beyond the scope of counterterrorism. The sixth piece, "Another Tool in the Influencer's Toolbox: A Case Study," by LTC Jamie Efaw and SFC Christopher Heidger, describes how social media can be used to influence a population at risk from radical messaging. Building on Efaw's earlier research on the application of social media to counterterrorism, the authors describe a project that successfully leveraged a Facebook site in order to reach, engage, and influence a target audience.

The final article, "Mining Twitter Data from the Arab Spring," by Rob Schroeder, Sean Everton, and Russell Shepherd of NPS, uses social movement theory to explain how Twitter may have played a role in the Arab Spring. By analyzing Twitter data from the period between December 2010 and Fall 2011, the researchers found that activists' use of Twitter may have facilitated the framing of grievances that resonated with their target audiences and helped inspire action.

In keeping with our theme, Sean Everton next delves into the State of the Art of dark networking. Even as social media offer us more and more opportunities to connect with friends, relatives, and colleagues around the world, they give terrorists, insurgents, and criminals the same easy means to connect and coordinate and plan. Meanwhile, the security sector is becoming increasingly skilled at extracting useful information from basic social media data. Without trying to guess where this spiral may lead in the longer term, Dr. Everton gives those of us who update our status or retweet something clever plenty to think about.

In this issue, we are happy to welcome Bradley Strawser, a new contributor to our regular Ethics column. Dr. Strawser tackles the topic professionalism, its origins in three ancient professions (*not* including the one some of you are thinking of), and then offers some ideas about how it applies to the military.

The book review by Joey Wang, *The Harkis: The Wound that Never Heals* takes us back a few decades to the end of the Algerian War of Independence, and the plight of the Harkis, Algerians who chose to join the French and fight against the insurgency. Largely ignored by the French after the war and targeted for death by the new Algerian regime, the survivors and their children tell anthropologist and author Vincent Crapanzano their story of betrayal and resignation.

As always, we encourage you to submit your work to CTX for review. See the back page of the journal for submission guidelines and make sure to note our new email addresses.

DOROTHY E. DENNING
Distinguished Professor, Department of Defense Analysis, Naval Postgraduate School
Chair, Workshop on Social Media and Counterterrorism

ELIZABETH SKINNER
Managing Editor

Special Issue: Social Media in Jihad and Counterterrorism

List of Contributors

Dorothy E. Denning, guest editor of this special issue of CTX, is Distinguished Professor of Defense Analysis at the Naval Postgraduate School (NPS). Her teaching, research, and publications have been mainly in the area of cyber security and cyber conflict. She is the author of *Cryptography and Data Security* (Addison-Wesley, 1982), and *Information Warfare and Security* (Addison-Wesley, 1998). She earned her doctorate from Purdue University, which later named her a Distinguished Science Alumna.

Dr. Denning has received numerous awards, including the Augusta Ada Lovelace Award, the National Computer Systems Security Award, and the Harold F. Tipton Award. She is a Distinguished Fellow of ISSA and a Fellow of ACM and (ISC)2, and was a featured security innovator in *Time* magazine.

Dr. Denning is one of 11 honorees selected to the inaugural class of the National Cyber Security Hall of Fame (October 2012). She and her colleagues were nominated and selected based on criteria that, among other things, distinguish them as leaders and innovators within the cyber security community.

Dr. Maura Conway is senior lecturer in International Security in the School of Law and Government at Dublin City University, Dublin, Ireland. Dr. Conway's articles have appeared in, among other publications, *Current History, First Monday, Media, War & Conflict,* and *Parliamentary Affairs.*

LTC Jamie Efaw serves as the Fort Story ASA Commander and Deputy Commander for Joint Expeditionary Base Little Creek-Fort Story in Virginia Beach. With a M.A. degree in Social Psychology, he taught in the Behavioral Science and Leadership Department at West Point, and branch transferred to Psychological Operations.

Sean Everton is an assistant professor in the Defense Analysis (DA) Department and the co-Director of the NPS CORE Lab. His recent monograph for Cambridge University Press is on using social network analysis to craft strategies for the disruption of dark (i.e., criminal and terrorist) networks.

Dr. Peter K. Forster is a senior lecturer, member of the graduate faculty, and the executive director of Online Education in the College of Information Sciences and Technology at Penn State University. He is the co-author, with Stephen J. Cimbala, of *Multinational Military Intervention* (Ashgate, 2010).

SFC Chris Heidger was the Senior Enlisted Military Information Support Advisor at USEUCOM in Stuttgart, Germany, where he and LTC Efaw managed the SETimes. A nine-year PSYOPS veteran, Chris has spent five years overseas with tours in Iraq, Afghanistan, Africa, and, most recently, Europe.

Dr. Dana Janbek is assistant professor of Public Relations at Lasell College in Newton, Massachusetts, where she teaches graduate and undergraduate communication courses. She is co-author, with Philip Seib, of *Global Terrorism and New Media: The Post Al-Qaeda Generation* (Routledge).

Dr. Paola Prado, assistant professor, Journalism and Digital Media at Roger Williams University, specializes in digital inclusion, digital media convergence, and multimedia production. She writes on topics related to digital inclusion, media diversity, and the effect of the internet on gender roles in Latin America.

Maria A. Ressa is the CEO and executive editor of the social news network *Rappler*. Ms. Ressa has been a journalist for more than 25 years, most of them as CNN's bureau chief in Manila and Jakarta. Her upcoming book is *10 Days, 10 Years: From Bin Laden to Facebook* (Powerbooks, October 2012).

Rob Schroeder is a research associate in the DA CORE Lab at NPS. He is researching the use of open source information to map the Syrian opposition, and the influences of external support to insurgencies.

Russell Shepherd earned his M.A. degree in International Policy Studies from the Monterey Institute of International Studies (2012), where he focused on economic and public policy analysis. While at the NPS CORE Lab, Russ developed methods to analyze unconventional data, including generating social networks from Twitter.

Dr. Bradley J. Strawser is an assistant professor in the DA Department at NPS, and a Research Associate at Oxford University's Institute for Ethics, Law, and Armed Conflict. His newest book is *Killing By Remote Control: The Ethics of an Unmanned Military* (forthcoming from Oxford University Press).

Joey Wang is an analyst with the U.S. Department of Defense. An alumnus of the National and International Security program for senior executives at Harvard's John F. Kennedy School of Government, his essays on international security and insurgency have received international recognition.

A. Aaron Weisburd is a node in a global ad hoc network of counterterrorism and intelligence professionals. He is the founder of the watchdog group Internet Haganah, and is recipient of an FBI Director's Commendation for his work on counterterrorism.

COVER PHOTO

Cairo, Egypt–February 9, 2011: A man works on a Toshiba computer during anti-government demonstrations in Tahrir Square. Social networking and the internet played an important role in the Egyptian Revolution. Photo by Joel Carillet via iStockPhoto.com.

DISCLAIMER

This journal is not an official DoD publication. The views expressed or implied within are those of the contributors and do not necessarily reflect the views of any governmental or non-governmental organization or agency of the United States of America or any other country.

TERMS OF COPYRIGHT

The New Battlefield: The Internet and Social Media[1]

Maria A. Ressa

On November 6, 2011, a Filipino man with long hair uploaded a three-minute, twenty-second video on YouTube, the world's second largest search engine. It was a video of himself, wearing a camouflage jacket and a mask covering his face and head. He was speaking in Arabic and asking Muslims around the world to support and contribute to the jihad in the Philippines. Identified as Commander Abu Jihad Khalil al-Rahman al-Luzoni, the man in the video called on Muslims to unite and help their brethren, saying there was "no way to restore the Islamic Caliphate and the glory of the religion but through jihad."[2]

It was the first of its kind for the Philippines, triggering a wave of video clips, letters, and audio messages from Filipino jihadists, which were promoted on al Qaeda linked sites and jihadist websites like Shumukh al-Islam and Ansar al-Mujahideen English Forum. They declared allegiance to al Qaeda online and on social networks.

Intelligence sources from at least three different countries told me that the man with the long hair—Abu Jihad Khalil al-Rahman al-Luzoni, who also went by the shorter pseudonym Abu Jihad—is 31-year old Khalil Pareja, a Christian convert to Islam who took over the leadership in 2005 of the Rajah Solaiman Movement (RSM), also known as the Rajah Solaiman Islamic Movement. RSM worked closely with the groups Abu Sayyaf, a violent Islamist insurgency in the southern Philippines, and Jemaah Islamiyah, al Qaeda's arm in Southeast Asia. Their alliance carried out numerous attacks, including the Superferry bombing in 2004, one of the world's worst maritime terrorist attacks and the second most lethal in Southeast Asia since the 2002 Bali bombing; and the Valentine's Day bombings in 2005—two near-simultaneous explosions in General Santos City and Davao City, followed an hour later by an explosion on a bus in Makati.

A Philippine intelligence report obtained and verified by *Rappler* said that Pareja not only posted jihadi materials on YouTube, he was also active on Facebook—a case study of how one man can connect jihadists and terrorists from multiple countries through social media.[3]

Pareja not only posted jihadi materials on YouTube, he was also active on Facebook.

About a month before he posted his YouTube video, Pareja told authorities, he joined the Arabic Student Forum on Facebook. Several of the members asked him if he knew Abu Jihad, but he said he was cautious about security so he pretended to know nothing. Then he received a private message online from a man who introduced himself as Gerald.[4] They became friends and started chatting through private messages regularly. Over time, Gerald told Pareja he was a member of al Shabaab, a group of Islamist militants that controls much of southern Somalia.[5] The relationship between al Shabaab and

Al Shabaab's leadership pledged allegiance to al-Zawahiri on a video uploaded to the internet by al Qaeda's media arm.

al Qaeda dates back to the 1990s, when al Qaeda began providing funding and training to the Somali fighters. It seems Osama bin Laden's death in 2011 helped pave the way for closer ties between the two groups. In February 2012, al Shabaab's leadership pledged allegiance to Ayman al-Zawahiri, who replaced bin Laden as al Qaeda's new leader. This was announced on a video uploaded to the internet by al Qaeda's media arm. This agreement showed that despite bin Laden's death, al Qaeda continues to spread.[6]

Pareja told Gerald he was Abu Jihad. Gerald invited him to go to Yemen to join the jihad led by al Qaeda's Yemeni affiliate, al Qaeda in the Arabian Peninsula or AQAP. Counterterrorism officials and analysts characterize AQAP as the "most active and lethal Qaeda affiliate, intent on striking at both the U.S. homeland and regional targets."[7] In mid-2012, authorities used a CIA sting operation to foil an AQAP plot to bomb U.S.-bound airplanes with explosives hidden in the bodies of terrorists. Experts said AQAP's master bomb-maker, Ibrahim al-Asiri, had been working on body bombs, surgically implanted explosives in the stomach or rectal cavity. AQAP was also involved in other foiled plots against U.S. targets: the "underwear bomb" used in an attempt to take down Northwest flight 253 in 2009, and the "printer bombs" in the failed cargo bomb plot in 2010.[8]

Anwar al-Awlaki was a "master in the use of the Internet."

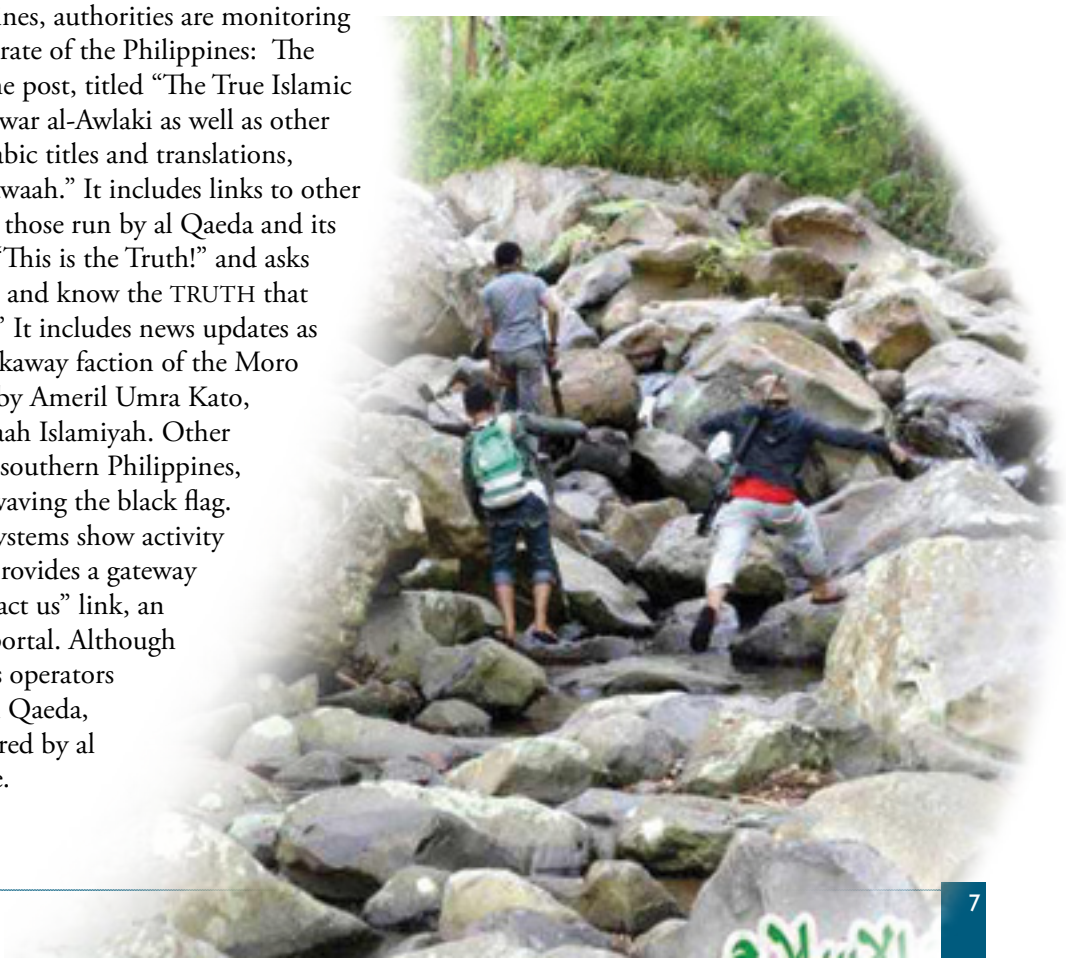
One of AQAP's leaders, American Anwar al-Awlaki, was a "master in the use of the Internet,"[9] and although he was killed by the United States in 2011, his messages continue to resonate and win recruits online. Awlaki was prolific on YouTube; among those he influenced were the London attackers who carried out simultaneous subway and bus bombings on July 7, 2005 (commonly referred to as 7/7, or "Britain's 9/11"). He had his own website (now taken

down by authorities), which attracted extremists including the head of AQAP, bin Laden's secretary, Nasir al-Quhaishi. Al-Quhaishi consulted bin Laden and appointed Awlaki the head of AQAP's external operations, in charge of terrorist attacks outside Yemen and Saud Arabia; this was his position when he was killed by a drone strike while in Yemen. Awlaki became a cyberworld superstar because he was an eloquent speaker and understood how to use social media. His ideas were incorporated by AQAP, which continues his online recruitment efforts. Eleven years after 9/11, al Qaeda is degraded, but it has evolved into a social movement. It continues to spread its virulent ideology, now in the virtual world and on social media. This is the new battlefield.

Pareja said Gerald told him AQAP "had established an Islamic state in the province of Abian in Yemen,"[10] and had already recruited "Filipinos studying from the Islamic schools in Saudi Arabia, Egypt, and Sudan."[11] Gerald asked Pareja to join the jihad in Yemen and help lead the Filipinos. He said they would stay in Yemen for ten years. After five years, they could choose to return to the Philippines, at which point AQAP "would provide them funds to continue jihad to establish an Islamic Caliphate."[12] Gerald offered to pay Pareja's travel expenses to Yemen. Pareja accepted the offer and was scheduled to travel between April and June of 2012, but he never made it because Filipino authorities arrested him on March 1.

The website provides a gateway for radicals: there is a "Contact us" link, an online poll, and a donation portal.

Pareja's story doesn't end with his arrest, however. When he uploaded his video exhorting support for jihad in the southern Philippines in 2011, it showed him speaking in front of a black flag. Other extremist websites, video messages, and social media accounts around the world, including in the Middle East, Afghanistan, Somalia, and Yemen, prominently display the black flag. In the Philippines, authorities are monitoring a website called "Islamic Emirate of the Philippines: The Black Flag Movement."[13] One post, titled "The True Islamic Hero," shows a picture of Anwar al-Awlaki as well as other al Qaeda operatives, with Arabic titles and translations, including "The Martyr of Dawaah." It includes links to other extremist websites, including those run by al Qaeda and its proxies. Another entry says: "This is the Truth!" and asks the reader to "open your eyes and know the TRUTH that the commercial media hides." It includes news updates as well as photographs of a breakaway faction of the Moro Islamic Liberation Front led by Ameril Umra Kato, who sheltered leaders of Jemaah Islamiyah. Other photos show Filipinos in the southern Philippines, where Abu Sayyaf operates, waving the black flag. While all public measuring systems show activity on the site isn't alarming, it provides a gateway for radicals: there is a "Contact us" link, an online poll, and a donation portal. Although it is unclear whether the site's operators have any real-world link to al Qaeda, it's clear they have been inspired by al Qaeda lore and its subculture.



The black flag taps into a secret motivation of al Qaeda: a "narrative that convinces them that they're part of a divine plan."[14] Al Qaeda's mythology holds that its black banners herald the apocalypse that would bring about the triumph of Islam, based on what they believe is a hadith, or a saying of the prophet Muhammad: "If you see the black banners coming from Khurusan, join that army, even if you have to crawl over ice; no power will be able to stop them, and they will finally reach Baitul Maqdis [Jerusalem], where they will erect their flags."[15] Khurusan is a name for a historical region covering northeastern and eastern Iran and parts of Turkmenistan, Uzbekistan, Tajikistan, Afghanistan, and northwestern Pakistan. This is where al Qaeda believes the Islamic version of Armaggedon will emerge. Osama bin Laden's 1996 declaration of war against the United States ends with the dateline, "Friday, August 23, 1996, in the Hindu Kush, Khurusan, Afghanistan."

In August, 2012, Philippines authorities recovered video explaining the black flag's symbolism on the laptop of a Malaysian jihadist, during an offensive targeting Southeast Asia's most wanted terrorists, Jemaah Islamiyah leaders Marwan and Muawiyah. These men also were the targets of the first U.S. smart bomb attack in the Philippines, February 2012 in Jolo, but both escaped and fled to central Mindanao.

The video found in the laptop verifies what CIA sources and former FBI agent Ali Soufan, who has closely studied al Qaeda's ideology, have said regarding the virtual links between jihadists. All this brings us back to Pareja. Before he was scheduled to leave the Philippines, Gerald asked him to do one more thing: "to establish the link between the group of Marwan and the AQAP."[16] Although Pareja was arrested before he could do that, it seems someone else may have had the same intent. The Malaysian who owned the laptop with the black flag video arrived in the Philippines in April 2012, and found his way to the central Mindanao camp of Marwan and Muawiyah. Among the weapons and rocket launchers recovered by authorities when they attacked that camp in August, they also found a hardcover book written in English. Its title is "Islami Emirate Afghanistan." Below the title was the logo of the Islamic Emirate of the Philippines.

More recently, on September 20, 2012, authorities in the Philippines stormed an Abu Sayyaf training camp in Zamboanga City, freeing Chinese hostage Yuan-Kai Lin and seizing a black flag they found there. During the twenty-minute battle, police forces claimed they wounded Abu Sayyaf leader Khair Mundos, who carries a $500,000 reward from the U.S. Department of Justice. Mundos had been captured previously in 2004, and confessed he arranged funds for terrorist attacks in Mindanao. Working with his brothers, he funnelled money from Saudi Arabia to the Abu Sayyaf, which has had a historical link to al Qaeda. As early as 1988, al Qaeda's financial network in the Philippines was

established by Osama bin Laden's brother-in-law, Mohammed Jamal Khalifa, and al Qaeda leaders, including Khalid Shaikh Mohammed, the architect of the 9/11 attacks, have trained members of the Abu Sayyaf. Mundos escaped from prison in 2007 and became head of the the Abu Sayyaf group in Basilan. During the September 20 raid, intelligence sources said they discovered not only the black flag, but also training manuals from Jemaah Islamiyah, once al Qaeda's arm in Southeast Asia, inside the camp. Mundos escaped.

Jihadists connect with other like-minded individuals from the safety of their homes, sitting at their computers.

This black flag symbol has resurfaced in high-profile violence since September 11, 2012, the eleventh anniversary of the 9/11 attacks. On that day, a violent mob stormed the U.S. consulate in Benghazi, Libya, raised the black flag and killed four Americans, including Ambassador Christopher Stevens. U.S. officials blamed the violence on an al Qaeda-linked group, which they said took advantage of protests against clips from an anti-Islam film that had recently spread across the internet to launch an attack.

Chat rooms and blogs mean that jihadists no longer have to physically meet.

In a little more than a week, protests against the film spread to more than twenty countries, and more than thirty people were killed. Black flags were raised by angry mobs in countries like Egypt, Tunisia, and Yemen. Coincidentally or not, a day before the attack in Libya, al Qaeda leader Ayman al-Zawahiri released a forty-two minute video confirming the death of his deputy, Abu Yahyah al-Libi. From Yemen, AQAP said the attack in Libya was to avenge the June killing of al Qaeda's number two, and urged Muslims to kill U.S. diplomats in Muslim countries.

The centralized command structures of both al Qaeda and Jemaah Islamiyah have collapsed in the years since 9/11, but remaining networks and cells continue to spread their virulent ideology, not just physically but in the virtual world through the internet and social media. Smaller, more ad hoc and less professional cells carry out attacks without central coordination. The challenge for authorities today is how to contain a social movement that simmers just beneath the surface.

New technology now allows jihadists to connect with other like-minded individuals from the safety of their homes, sitting at their computers. Individuals from Southeast Asia, Europe, and the

United States have become politically radicalized, learned operational details like how to make bombs and suicide vests, and connected with others who have acted as mentors in their radicalization, all online.[17] The chat rooms and blogs act as echo chambers. They're harder for authorities to detect, and they mean that jihadists no longer have to physically meet. These individuals are free to read, participate, and ask questions in the privacy of their homes, lowering the risk of detection. Plus, never before has one platform connected so many: Facebook now links together more than a billion accounts. Gerald, allegedly recruiting for AQAP, didn't have to meet Pareja in person in order to get him to commit to AQAP's jihad.

Let me end with the Facebook page created by Pareja. Filipino authorities say one of his "friends" is a Facebook pseudonym used by Marwan, who even while on the run updates his page. Pareja has other "friends" from around the world, whose pages prominently and publicly display a picture of the black flag like a secret code. These are clear visual reminders of how the jihadi virus spread through the years, from bin Laden to Facebook. ❖

ABOUT THE AUTHOR

Maria A. Ressa is the CEO and executive editor of *Rappler*, a social news network that combines professional journalism with citizen journalism and crowdsourcing. Ms. Ressa has been a journalist in Asia for more than 25 years, most of them as CNN's bureau chief in Manila (1987–1995), then Jakarta (1995–2005). She was CNN's lead investigative reporter focusing on terrorism in Southeast Asia, and wrote *Seeds of Terror: An Eyewitness Account of al-Qaeda's Newest Center of Operations in Southeast Asia* (Free Press, 2003). She is a graduate of Princeton University. Her upcoming book is *10 Days, 10 Years: From Bin Laden to Facebook* (Powerbooks, Fall 2012).

PHOTO CREDITS

Photos pages 6, 7, 8, and 9 courtesy of the author.
Photo this page via iStockPhoto.com.

NOTES

1 This is a compilation of two articles originally written for the online social news network *Rappler*, and includes excerpts from the author's book, *10 Days, 10 Years: From Bin Laden to Facebook* (forthcoming from Powerbooks, Fall 2012).

2 English translation of Arabic message from Abu Jihad Khalil al-Rahman al-Luzoni. The video was uploaded to YouTube on November 6, 2011.

3 Details are from a classified Philippine intelligence document, "Dinno-Amor Rosalejos Pareja @Abu Jihad/ Khalia/Ur Rahman/Muhammad/Rash/Ahmad/Arlan/ Al-Luzoni/Jake Fajardo," CTD-DRP-03052012-014, Philippine National Police, March 5, 2012.

4 Gerald may or may not be his real name. Terrorists use pseudonyms frequently, and the internet allows anonymity to reach new heights. What's clear is that the private messages between Pareja and Gerald continued to the point that Pareja was convinced of Gerald's identity and started to make plans based on his offers.

5 Al Shabaab's formal name is al Shabaab al-Mujahideen. It has waged an insurgency against Somalia's government and the government's Ethiopian supporters since 2006. In the 1990s, al Qaeda set up a base of operations in the Somali state similar to what it had in Afghanistan.

6 "Al-Shabaab joining al-Qaeda, monitor group says," CNN, February 9, 2012: http://articles.cnn.com/2012-02-09/africa/world_africa_somalia-shabaab-qaeda_1_al-zawahiri-qaeda-somali-americans?_s=PM:AFRICA; accessed on October 6, 2012.

7 Jonathan Masters, "Al-Qaeda in the Arabian Peninsula (AQAP)," Council on Foreign Relations, Washington, D.C., May 24, 2012: http://www.cfr.org/yemen/al-qaeda-arabian-peninsula-AQAP/p9369; accessed on October 6, 2012.

8 Maria Ressa, "Al-Qaeda and Afghanistan: 1 year after bin Laden's death," *Rappler*, May 2, 2012: http://www.*Rappler*.com/world/4663-al-qaeda-afghanistan-1-year-after-bin-laden-s-death; accessed on October 6, 2012.

9 Rohan Gunaratna, "Al-Qaeda after Awlaki," *The National Interest,* October 19, 2011: http://nationalinterest.org/commentary/al-qaeda-after-awlaki-6026; accessed on October 6, 2012.

10 "Dinno-Amor Rosalejos Pareja," 12.

11 Ibid.

12 Ibid.

13 Available at http://islamicemirateofthephilippines.webs.com/; accessed on October 6, 2012.

14 Ali H. Soufan, "The Black Banners: The Inside Story of 9/11 and the War Against al-Qaeda," (New York: W.W. Norton & Company, 2011), loc 196 of 10851 on Kindle.

15 Ibid., loc. 148 of 10851. Soufan explains the meaning of the black flag and the narrative al Qaeda created connecting religion and jihad.

16 "Dinno-Amor Rosalejos Pareja," 12.

17 See Peter Forster's article in this issue, "Countering Individual Jihad: Perspectives on Nidal Hasan and Colleen LaRose," for more on this phenomenon.

From al-Zarqawi to al-Awlaki: The Emergence and Development of an Online Radical Milieu

Maura Conway

Milieu: *the physical or social setting in which something occurs or develops; syn:* environment.
—Merriam-Webster Online, 2012

Radical milieus have been described as specific social environments whose culture, narratives, and symbols shape both individuals and groups, and the social networks and relationships out of which those individuals and groups develop and emerge. Researcher Peter Waldmann and his co-authors attribute distinct and independent qualities to these environments, portraying them as social entities in their own right, that is, a collective of people sharing certain perspectives and a unitary identity: a "subculture" or a "community." This does not mean that conflict is absent between any given radical milieu and the violent extremist or terrorist group(s) that emerges from within it. Milieus have their own interests that lead them not just to interact with, but oftentimes to criticise and sometimes even confront their violent offshoots. Perhaps most importantly, Waldmann's conception of radical milieus appears not merely to have social relationships as a core characteristic, but necessitates, implicitly or explicitly, face-to-face interaction amongst the members of any given milieu.[1]

Many of the basic characteristics of traditional radical milieus are also apparent in their online counterparts.

Waldmann has raised the question of virtual versus "real world" interaction, and the merits or demerits of each, asking whether "the Internet and its chat forums offer a substitute to face-to-face contacts as a base of mutual support [for violent radicals]?"[2] While he doesn't venture an answer, given that the internet, and Web 2.0 in particular, has been shown to facilitate the virtual establishment of strong social and personal bonds in many different contexts,[3] there is no reason to believe that this should not hold true with respect to violent political extremists. The purpose of this article is therefore to expand the concept of the radical milieu to the virtual sphere by showing that many of the basic characteristics of traditional radical milieus are also apparent in their online counterparts, while acknowledging the latter's own unique characteristics and complicating factors. The emphasis here is on the emergence of the violent jihadi online milieu, although as noted in the conclusion, this is probably not the only well-developed online radical milieu in existence.

Shared Characteristics of Online and Traditional Radical Milieus

It was the advent of Web 2.0 that offered violent radicals the means to transform their largely broadcast internet presences into meaningful interactive radical milieus.[4] Osama bin Laden's cadres had used the internet for communication and propaganda purposes prior to the attacks in the United States

on September 11, 2001, but their use of the internet increased exponentially thereafter.[5] This had two interrelated causes: 1) the loss of al Qaeda's Afghan base and the consequent dispersal of its leaders and fighters; and 2) the rapid development of the internet itself, the global spread of internet cafes, and the proliferation of internet-capable computers and other gadgets, such as mobile telephones.[6] Until the emergence of Web 2.0, with its emphasis on the integration of user-generated content, social networking, and digital video, bin Laden and "al Qaeda Central" maintained some level of control over the al Qaeda narrative. It was Abu Musab al-Zarqawi and the group al Qaeda in Iraq (AQI) who instigated a separate online strategy in the interregnum between the sunset of the early Web and the full ascent of Web 2.0, thus marking the beginning of violent jihad's transformation from a movement with a significant internet component to a genuine online radical milieu.

Abu Al-Zarqawi instigated violent jihad's transformation from a movement with a significant internet component to a genuine online radical milieu.

Like traditional radical milieus, online radical milieus are communities within which the perpetrators of violence are a sub-group. In other words, terrorist groups and violent attacks spring from radical milieus (i.e., these are violently radicalizing environments), and therefore terrorist groups and attacks can also spring from their online variants. "What distinguishes the milieu from simple sympathizers is that within the former, there exists a form of social structure responsible for the observed in-group cohesion. It is not merely a sum of individuals holding similar political/cultural attitudes."[7] A violent online jihadi milieu worthy of the name thus emerged when the "jihadisphere" came to encompass a wide cross-section of producers and consumers, from al Qaeda Central to the media arms of various al Qaeda franchise organisations, to the globally dispersed array of "jihobbyists" with no formal links to any violent jihadist organisation, all contributing to the everyday making and remaking of the violent jihadi narrative.[8]

A violent online jihadi milieu emerged when the "jihadisphere" came to encompass a wide cross-section of producers and consumers.

Al-Zarqawi's Online Exploits as Turning Point

In a little over four weeks in April and May 2004, Abu Musab al-Zarqawi shot to worldwide fame—or more appropriately, infamy—by a strategic combination of extreme violence and internet savvy. In early April 2004, al-Zarqawi posted online a thirty-minute audio recording that explained who he was, why he was fighting, and details of the attacks for which he and his group were responsible. Researcher Paul Eedle described the latter as "a comprehensive branding statement."[9] The internet allowed al-Zarqawi to build a brand very quickly: "Suddenly this mystery man had a voice, if not a face, and a clear ideology to explain his violence." But what was AQI's purpose in building a brand and establishing a public profile in this way? The answer, according to Eedle, clearly was to magnify the impact of their violence.[10] Prior to the initiation of his internet-based public-relations campaign, each of al-Zarqawi's attacks had to kill large numbers of people in order to get noticed amid the chaos and mounting daily death toll in Iraq. By going online however, al-Zarqawi was able to both control the interpretation of his violent message and achieve greater impact with smaller operations. In May 2004, al-Zarqawi pushed the internet's force-multiplying effect to the maximum by having himself filmed personally cutting off the head of American hostage Nicholas Berg, and posting the footage online.[11] The purpose of this beheading was precisely to videotape it. The images gripped the imaginations of AQI's allies and enemies alike. Al-Zarqawi risked nothing

Al-Zarqawi pushed the internet's force-multiplying effect to the maximum by personally cutting off the head of Nicholas Berg, and posting the footage online.

in the endeavour, while making himself a hero to jihadis worldwide.[12] It was only after these online exploits that al-Zarqawi was actually endorsed by Osama bin Laden as "Emir" (i.e., leader) of al Qaeda in Iraq.

Government officials' and policymakers' fears of the potential for the internet to act as a vehicle for violent radicalisation spring from the alleged effects of extreme political violence like al-Zarqawi's, combined with the advantages of the cyber world (e.g., potentially vast audience, geographical reach, and multimedia capabilities). Al-Zarqawi was, however, a terrorist who migrated some of his activity to the internet, rather than himself emerging out of an online radical milieu. It was the legions of fans inspired by al-Zarqawi's online activity who took up the banner of violent jihad online, thus generating more of the same, in a spiral effect that eventually coalesced into the contemporary violent jihadi online milieu.

Changes in the Internet Landscape Leading to the Emergence of the Violent Jihadi Online Milieu

It was the legions of fans inspired by al-Zarqawi's online activity who took up the banner of violent jihad online.

Al-Zarqawi's exploitation of the internet wasn't the only catalyst for heightened concern regarding violent online radicalization. The emergence of the violent jihadi online milieu was also influenced by changes in the internet landscape, in terms of both access and technologies, that were gaining pace at around the same time al-Zarqawi's publicity strategy came to the world's attention. First, large numbers of people gained cheap and easy access to the internet. Today, always-on mobile internet access is speedily becoming the norm, especially among youth who increasingly go online using mobile telephones and other mobile devices. Second, online social networking, an integral part of Web 2.0, took off in the mid-2000s. Consider that Facebook was established in 2004 and is now thought to have a billion regular users,[13] while YouTube, which only came into existence in 2005, currently has 72 hours of video uploaded to it *every minute.*[14] It was these changes that caused *Time* magazine to name "You" as their 2006 "Person of the Year,"[15] and it was the same changes that ushered in the violent jihadi online milieu instigated by al-Zarqawi. These developments had transformed the internet environment by the time al-Zarqawi's most prominent online successor, Anwar al-Awlaki, appeared in 2008.[16]

Official and semi-official websites were no longer the only important jihadi cyber spaces.

No figure immediately emerged from within the ranks of al Qaeda-affiliated groups to fill the cyber-gap left by al-Zarqawi's death in June 2006. But such a figure was no longer integral to the buoyancy of al Qaeda's online presence. Official and semi-official websites were no longer the only important jihadi cyber spaces.[17] Increasing numbers of violent jihadi websites and amounts of content began to be available in English, French, German, Spanish, and Dutch, signifying both the rise of violent jihadism in the West and growing efforts by violent jihadist voices to reach Western (Muslim) populations online.[18] Changes in the nature of the internet encouraged increasing numbers of supporters of violent jihad to post and re-post articles and analyses, exchange information, voice opinions, and debate ideas on blogs, websites, and forums that they themselves established. The proliferation of fan sites acted as free publicity for the violent jihadi cause. Today, new websites

appear—and also disappear—frequently, popular chat rooms have stringent admission policies, and most sites display technical savvy on the part of their producers, including all the latest internet tools and gadgetry. Al Qaeda did not and does not provide financing or have any management role in these sites; nonetheless, they act as an invaluable force-multiplier for the group's cyber-based incitement strategy.

The proliferation of fan sites acted as free publicity for the violent jihadi cause.

Recognising this benefit, al Qaeda assured its "internet brothers" early on that "the media war with the oppressive crusader enemy takes a common effort and can use a lot of ideas. We are prepared to help out with these ideas."[19] From this came al Qaeda's official media production arm, largely audio and video, known as as-Sahab or "the Clouds" in 2001. Violent jihadi online content takes three major forms: basic text, including forum postings, magazines/journals, books, and written statements; audio, such as statements by leaders, sermons by violent jihadi preachers, *nashid* (chants); and video. Genres of video include political statements, by al Qaeda leaders and Western "spokesmen;" attack footage; "pre-martyrdom" videos, such as that made of 7/7 bomber Mohammed Siddique Khan; instructional videos, of both theological and military-operational sorts; memorial videos commemorating persons and/or events; music videos; and beheadings. With the advent of easy digital video composition and fast download, huge amounts of violent jihad-supporting video began to be produced, distributed, and consumed. Between 2002 and 2005, for example, as-Sahab issued a total of 45 tapes; there was an exponential increase in 2006, which saw the distribution of 58 productions.[20] 2007 too was a banner year, with 97 original productions.[21] As-Sahab began to lose ground from 2008, however, as both the quality and volume of their productions decreased. This slack was taken up by a host of new producers, including both formal production outfits and individual "jihobbyists." Together these contributions added up to a tremendous input into what Osama bin Laden repeatedly said was his, and remains al Qaeda's, top priority: the instigation to violent jihad of as many Muslims globally as possible.[22]

As as-Sahab began to lose ground, this slack was taken up by both formal production outfits and individual "jihobbyists."

This violent jihadi content increasingly migrated to global portals such as YouTube, which had the effect of making the content much easier to locate for anyone, regardless of Arabic language skills or level of internet literacy. Consider too that these global portals are known and attractive to young people in particular, and that multi-media content, especially moving images, is thought to be more convincing than text in terms of its ability to influence. Couple this with the internet's crowd-sourcing properties, and the violent jihadi online milieu is born. Masses of violent jihadi texts that were originally produced in Arabic began to be translated into a multitude of other languages. Large amounts of violent jihadi video began to have subtitles, again in multiple languages, added by fans. All of this modified material is then re-uploaded for consumption online, or easy copying and dissemination via links embedded in emails and Tweets, instant messages, SMS/text messages, etc., but also through VHS tapes, CDs, DVDs, and mobile phones.[23] The spread of such content across multiple platforms and in multiple formats means that it is increasingly difficult to counter, especially because portals such as YouTube and Twitter generally cannot be shut down in the same way as, for example, jihadi online forums.

Large amounts of violent jihadi video began to have subtitles in multiple languages, added by fans.

Critical Voices

It is important to note here that while radical milieus can be largely characterized as that segment "of a population which sympathizes with terrorists and supports them morally and logistically,"[24] this support is not wholly uncritical:

> [N]otwithstanding their shared experiences and perspective and their general approval of violent action, radical milieus do not unconditionally support or approve of terrorist groups and their violent campaigns. What emerges is a complex and ambivalent relationship, which may include interactions and close social ties as well as dynamics of separation and isolation; and entails solidarity and support as well as controversies and confrontation.[25]

The same holds true for online radical milieus. At least one function of al-Zarqawi's original audio statement mentioned above, for example, was to alert audiences that he viewed the world rather differently from Osama bin Laden, conceiving the enemy to be not just American troops, but also Kurds and Shi'ite Muslims. On a different occasion, Ayman al-Zawahiri criticised the young online followers of al-Zarqawi for their preoccupation with the staging of blood-soaked media spectacles, writing:

Al-Zawahiri criticised followers of al-Zarqawi for their preoccupation with the staging of blood-soaked media spectacles.

> Among the things which the feelings of the Muslim populace who love and support you will never find palatable, also, are the scenes of slaughtering the hostages. You shouldn't be deceived by the praise of some of the zealous young men and their descriptions of you as the Sheikh of the Slaughterers.[26]

Clearly, the effort put into the production and circulation of "images signifying Muslim suffering, Western hypocrisy, Jihadist heroism and so on was intended to create effects; to legitimise violence and recruit and mobilise supporters," facilitated by what some analysts term the "new media ecology."[27] As the latter also point out, however, the very openness of this new ecology led to a loss of control over the "core message" or "single narrative," as new and differing interpretations and conflicting versions of the violent jihadi message began to appear, and new figures emerged to explicitly challenge the position of al-Zawahiri and others.[28] This explains al-Zawahiri's rebuke of al-Zarqawi's independent, implicitly competing, online strategy.

In fact, in 2006, the violent jihadi media production outlet al-Boraq Media Institute published what could be called a "policy document" on this issue, entitled *Media Exuberance,* which sought to curb the uncontrolled and "exuberant" production and distribution of violent jihadi fan content.[29] Similarly, the posting guidelines for the al-Faloja online discussion forum "primly exhort posters to avoid material likely to give offense or create *fitna* (division) in the community, as well as, interestingly, information on subjects such as how to make bombs."[30] Many violent jihadi discussion forums are, in fact, tightly controlled in this way.[31] One researcher provides the example of a conversation on the English-language Islamic Awakening forum, in which a member complains of having been ejected from the

The very openness of this new media ecology led to a loss of control over the "core message" or "single narrative."

al Qaeda-affiliated forum Al-Ikhlas, after commenting on al Qaeda in Iraq's tendency to kill Muslims. To this another poster responded that the disbarred member deserved it, and that the mujahedeen must be dismayed at the persistence of such questions.[32] This illustrates another vitally important aspect of the contemporary violent jihadi online milieu: It was not intentionally constructed, and thus has aspects that are lamented by some users, especially those elements of the movement directly affiliated with al Qaeda, but also some of the grassroots.[33] Having said this, the concept of the online radical milieu draws our attention to the way in which "official" voices must now co-exist with "unofficial" ones, or those seeking to seize the mantle of officialdom within the jihadisphere. The violent jihadi online milieu is not—despite the best efforts of some—"owned" or controlled by any one group, but encompasses a plurality of overlapping, and sometimes clashing, cyber spaces and voices, which contribute to making it a milieu.

"Official" voices must now co-exist with "unofficial" ones, or those seeking to seize the mantle of officialdom within the jihadisphere.

Precursor or Credible Alternative to "Real World" Activism?

Over time, online jihadist activity came to have standing in its own right through popular texts such as Muhammad bin Ahmadal-Salim's *39 Ways to Serve and Participate in Jihad,* which extolled "performing electronic jihad" as a "blessed field which contains much benefit."[34] In fact, the success of violent online jihad led some analysts to contend that, "The virtual or media Jihad has not only gained prominence and credibility as a wholly legitimate alternative to traditional conceptions of jihad, but has also progressively outpaced the militaristic or physical Jihad in the modern era."[35] In other words, all of this online activity had the effect of constituting a powerful new community, here termed the violent jihadi online milieu, that had to be acknowledged by al Qaeda leaders and, indeed, any individual or group that wished to play a prominent role within violent jihadism. It was by dint of these virtual jihadis' efforts, at least as much as those purveying solely "real world" violence, that violent jihadism continued to prosper from the mid-2000s onward. Thence, for example, al-Zawahiri's agreement to an online question-and-answer session in 2007–2008;[36] it also explains the emergence of Anwar al-Awlaki as a major figure within violent jihadism, at least in the West (he does not seem to have been personally known to Osama bin Laden).[37] Al-Awlaki, an English-speaking Yemeni-American cleric, was considered by some, largely because of his video-taped speeches, which were distributed online, and his involvement in the publication of *Inspire* magazine, to be "Terrorist No. 1" in terms of the threat he posed to the United States;[38] this at least partially explains his targeted killing by a U.S. drone attack in Yemen in September 2011. This is a significant development when one considers that al-Awlaki was not known to have ever personally engaged in political violence. In fact, the killing of al-Awlaki raises a matter of ongoing debate: the ability of online radical milieus to produce "real world" terrorists.

It was these virtual jihadis' efforts, at least as much as those purveying solely "real world" violence, that allowed violent jihadism to prosper.

Arguments against a prominent role for the internet in violent radicalization processes take two main forms. One position holds that claiming violent extremist online content radicalizes individuals into committing violence makes no sense given that other consumers of the same content do not commit violent attacks. Alternatively, it may be argued that while such

Europol's director general emphasized his belief that the "Internet has replaced Afghanistan as the terrorist training ground."

content can buttress an already sympathetic individual's resolve to engage in violence, it is not generally the originating cause of such a commitment.[39] The second position suggests that most, though not all, contemporary violent online extremists are dilettantes, in the sense that they restrict themselves to using the internet to support and encourage violent extremism, but pose no "real world" threat. Put another way, there is the possibility that the "venting" or "purging" political extremists engage in online satisfies their desire to act. Their internet activity, rather than becoming an avenue for violent radicalization and leading to potential offline action such as, in the most extreme instances, large-scale terrorist attacks, instead becomes for many a mechanism to dissipate the desire for violent action.[40]

The alternative view, of course, is that the violent extremist cyber-world is a progressively more important staging post for "real world" violence. Security personnel and policymakers appear increasingly swayed by this argument, as it relates to violent jihadists in particular. Europol has, for example, described the internet as "a crucial facilitating factor for both terrorists and extremists."[41] Europol's director general emphasized his belief that the "Internet has replaced Afghanistan as the terrorist training ground, and this should concern us the most."[42] The British government also underscored that:

> Al Qa'ida and some Al Qa'ida affiliates have increasingly encouraged acts of terrorism by individuals or small groups independent of the Al Qa'ida chain of command and without reference to, or guidance and instruction from, the leadership. The internet has enabled this type of terrorism by providing material which encourages and guides radicalisation and instructions on how to plan and conduct operations. In practice some attacks have been conducted or attempted by groups or sole individuals seemingly at their own initiative; in other cases they have had some contact with other terrorist networks.[43]

Manfred Murck, head of the Hamburg branch of Germany's domestic intelligence service, has made similar comments: "The tradition of terrorism is more or less a tradition of groups. But now we see that the group is not always necessary and that the Internet functions as a kind of virtual group."[44]

Such concerns have been stoked by a rash of both successful and thwarted terrorist attacks in which the internet played a role, including the failed July 21, 2005 London bomb attacks, the shooting deaths of two U.S. airmen at Frankfurt Airport in March 2010, and the so-called "Irhabi007" and "Jihad Jane" cases.[45] These cases and others have involved internet users who run the gamut, from prominent figures in the "jihadisphere" who spent large portions of their lives networking, and consuming and producing jihadi online content, to youths who entered the violent jihadi online milieu, consumed its products—largely or entirely in isolation from other denizens of the milieu—and acted on the basis of what they absorbed.

An example of the former type was Abu Dujana al-Khurasani, a well-known administrator of the al-Hesbah jihadi forum, who launched a suicide attack at U.S. Forward Operating Base Chapman in Afghanistan in December

2009, killing seven CIA operatives and a member of Jordan's General Intelligence Directorate.[46] He was described by his wife as "constantly reading and writing. He was crazy about online forums."[47] Al-Khurasani was immortalized online after his death in videos, photo montages, and poetry, including an ode entitled "Our James Bond."[48] British Muslim student Roshonara Choudhry is an example of the other type. She was jailed for life in November 2010 for attempting to murder a British M.P. Ms. Choudhry claimed she was radicalized over the course of just a few weeks after navigating from YouTube to a stream of videos featuring extremist preacher Anwar al-Awlaki.[49]

Al-Khurasani was described by his wife as "constantly reading and writing. He was crazy about online forums."

Al-Awlaki was implicated in a number of additional attacks and plots, including Major Nidal Hasan's shooting spree at Fort Hood in 2009, and the attempted Times Square car bombing in 2010. Both Hasan and Faisal Shahzad, the Times Square bomber, were thought to have been in online contact with the preacher prior to their attacks. For many, including policymakers and security practitioners, these cases and others like them illustrate the violent radicalizing properties of radical online milieus. For others however, they raise more questions than answers. Up until recently, al-Awlaki's sermons were widely available on mainstream Islamic websites. At the time that it came to the attention of U.S. authorities in 2008, for example, his popular lecture "Constants on the Path of Jihad" was available on Ummah.com, a mainstream site that, according to U.S. authorities, was receiving approximately 48,300 visits per month from the United States alone.[50] Some of these visitors must surely have viewed "Constants," but presumably never acted on al-Awlaki's advice to carry out attacks within the United States and abroad. Are direct contacts with violent extremists therefore more important than simply consuming violent extremist content? Can this factor explain the attacks carried out by Hasan and Shahzad? If so, what about Roshonara Choudhry and the influence of al-Awlaki's video sermons on her decision to assassinate a member of the British parliament?

Outright denials of a role for the internet in the process of violent radicalization seem to be premature.

While such questions cannot yet be adequately answered, outright denials of a role for the internet in the process of violent radicalization, such as the following quote from Jason Burke, seem to be premature:

> Twitter will never be a substitute for grassroots activism. In much of the Islamic world, social media is only for super-connected local elites or supporters in far-off countries. Neither are much use on the ground, where it counts. Social media can bring in donations or some foreign recruits. It can aid communication with some logistics and facilitate propaganda operations, but it is not much use in a firefight with Saudi, Iraqi or Pakistani security forces. Twitter won't help al-Shabaab retake Mogadishu or the Taliban reach Kabul in any meaningful way.[51]

Burke thus seems to dismiss out of hand all those preparatory steps—donations, foreign recruits, logistics, propaganda—and the potential role of violent online radical milieus in facilitating these that together culminate in "firefights." Burke also draws attention to issues of access; in large parts of the Muslim world, he says, online social networking is restricted to elites

The violent jihadi online milieu is a component of the wider jihadi milieu, with ideas from each penetrating the other in multiple ways.

and is thus not "much use on the ground, where it counts."[52] It is certainly true that home-based internet penetration rates are low in, for example, the Middle East as compared to the West, but internet cafes are widely popular and the region is seeing soaring rates of mobile phone usage.

While widespread fast, always-on internet is doubtless preferable in terms of instituting a durable Web-based political violence strategy, it is not crucial. The internet, and Web 2.0 in particular, facilitates small contributions—whether of money, content, or other types of virtual labour—by large numbers of people, along with large contributions by small numbers of people, that together can constitute a significant whole. Nor is it necessary for all those engaged in any activist project, violent or non-violent, to be themselves internet users. Internet-based content can circulate not only online, but can also be disseminated via photocopying, audio tapes, VHS and CDs, text-messaging, and plain old word-of-mouth, depending on its nature. In the context of the present analysis, the violent jihadi online milieu is a component of the wider jihadi milieu, with ideas and content from each penetrating the other in multiple ways. The same can be said of the events of the so-called "Arab Spring," in which internet tools played an important—though not determining—role "on the ground" for users and non-users alike. The wider Middle Eastern social-political environment is presently undergoing seismic changes, which will doubtless also influence the jihadi milieu, including its online component, in ways which may or may not be conducive to the violent jihadi agenda in the longer term.

Concluding Remarks

One does not radicalize oneself in cyberspace, any more than one becomes radicalized by oneself in the "real world." The concept of the violent online radical milieu emphasizes that although so-called "lone wolf" terrorists—from Robert Hasan and Arid Uka to Roshanara Choudhary and Anders Breivik—may act alone, oftentimes they are at least partially the product of some radical online milieu. Hasan, Uka, and Choudhary, as exemplar products of the jihadi online milieu, raise a further important concern: the likelihood that the internet plays a greater role in violent jihadi radicalization processes in Western countries than in other parts of the world. This would seem to make sense on the basis not just of widespread access in the West to cheap—often free—fast, always-on internet with less content restrictions than in most parts of the Muslim world, but also because it seems less likely that persons on the ground in "hot" conflict zones become radicalized via their online content consumption and interactions. Their personal experiences are likely to be far more of a catalyst, versus those of people living in stable Western countries who come to share the same violent jihadi commitments. This hypothesis needs testing, however.

The internet may play a greater role in violent jihadi radicalization processes in Western countries than in other parts of the world.

It is important to underline that violent radicalization is not something that should be explored only in the context of jihadism; thence the mention of Anders Breivik, the Norwegian right-wing radical who massacred dozens of young people at an island retreat in 2011. What is happening in the Middle East or the Muslim world more widely, and how this may affect violent

jihadism, both off- and online, should not be our sole consideration. If the internet has a role in some violent jihadis' radicalization processes, then it follows that it could play a role in other violent political extremists' radicalization, too. The online strategies of these other violent political extremists, including so-called "old" terrorist organizations (e.g., national-separatists and ethnic-separatists) and the extreme right wing, therefore need to be explored in much greater depth and at much greater length than they have been to date. Do these other violent extremist online spaces also constitute radical milieus as described herein? If so, why; if not, why not? Consistent cross-comparative research of this sort is crucial if we are to accurately characterize the role of the internet in violent radicalization. ❖

It is important to underline that violent radicalization is not something that should be explored only in the context of jihadism.

ABOUT THE AUTHOR

Dr. Maura Conway is Senior Lecturer in International Security in the School of Law and Government at Dublin City University (DCU) in Dublin, Ireland. Her principal research interests are in the area of terrorism and the internet, including academic and media discourses on cyberterrorism, the functioning and effectiveness of violent political extremist online content, and violent online radicalization. She has discussed these issues before the United Nations in New York, the Commission of the European Union in Brussels, the Royal United Services Institute (RUSI) in London, and elsewhere. Dr. Conway's articles have appeared in, amongst others, *Current History, First Monday, Media, War & Conflict,* and *Parliamentary Affairs.*

NOTES

1 See Peter Waldmann, "The Radical Community: A Comparative Analysis of the Social Background of ETA, IRA, and Hezbollah," *Sociologus* vol. 55, no. 2 (2005); Peter Waldmann, "The Radical Milieu: The Under-Investigated Relationship between Terrorists and Sympathetic Communities," *Perspectives on Terrorism* vol. 2, no. 9 (2008); Peter Waldmann, Matenia Sirseloudi, and Stefan Malthaner, "Where Does the Radicalisation Process Lead? Radical Community, Radical Networks and Radical Subcultures," in Magnus Ranstorp, ed., *Understanding Violent Radicalisation: Terrorist and Jihadist Movements in Europe* (London and New York: Routledge, 2010).

2 Waldmann, "The Radical Milieu," 27.

3 Nancy K. Baym, *Personal Connections in the Digital Age* (Cambridge: Polity, 2010), chapter 6; Emese Csipke and Outi Horne, "Pro-Eating Disorder Websites: Users' Opinions," *European Eating Disorders Review* vol. 15, no. 3 (2007): 196–206; Ayumi Naito, "Internet Suicide in Japan: Implications for Child and Adolescent Mental Health," *Clinical Child Psychology and Psychiatry* vol. 12, no. 4 (2007): 583–597.

4 Maura Conway, "Terrorist Web Sites: Their Contents, Functioning, and Effectiveness," in Philip Seib, ed., *Media and Conflict in the Twenty-First Century* (New York: Palgrave, 2005).

5 Maura Conway, "Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet," *First Monday* vol. 7, no. 11 (Nov. 2002); Philip Seib and Dana M. Janbek, *Global Terrorism and New Media: The Post-al Qaeda Generation* (London and New York: Routledge, 2011), 26.

6 Michael Scheuer, *Imperial Hubris: Why the West is Losing the War on Terror* (Washington D.C.: Brasseys, 2004), 78.

7 Peter Waldmann, "The Radical Milieu," 25.

8 Jarret M. Brachman, *Global Jihadism: Theory and Practice* (Abingdon: Routledge, 2009), 19.

9 Paul Eedle, "Al Qaeda's Media Strategy," in Karen G. Greenberg, ed., *Al Qaeda Now* (Cambridge: Cambridge University Press, 2005), 124–125.

10 Ibid.

11 Al-Zarqawi himself is on record stating that he was Berg's killer. The CIA also identified al-Zarqawi as the likely executioner: see "Zarqawi Beheaded US Man in Iraq," *BBC News* (Middle East), May 13, 2004. Others have raised doubts as to the authenticity of the beheading video and the likely perpetrator of the beheading, however; see, for example, Richard Neville, "Who Killed Nick Berg?" *The Sydney Morning Herald,* May 29, 2004, 33.

12 Eedle, "Al Qaeda's Media Strategy," 126.

13 Of these, 543 million are said by Facebook to access the site through mobile devices. See Facebook's "Key Facts" page at: http://newsroom.fb.com/content/default.aspx?NewsAreaId=22; accessed August 29, 2012.

14 Further, over 4 billion videos are viewed on YouTube each month, three hours of video are uploaded per minute to the site from mobile devices, and 70% of YouTube traffic comes from outside the United States. See YouTube's "Statistics" page at: http://www.youtube.com/t/press_statistics; accessed August 29, 2012.

15 Lev Grossman, "You—Yes, You—Are TIME's Person of the Year," *Time Magazine,* 25 December 2006.

16 Alexander Meleagrou-Hitchens, "As American as Apple Pie: How Anwar al-Awlaki Became the Face of Western Jihad," International Centre for the Study of Radicalisation and Political Violence, Kings College London, 2011, 56, 70.

17 Seib and Janbek, *Global Terrorism and New Media,* 36.

18 Madeline Gruen, "Terrorism Indoctrination and Radicalization on the Internet," in Russell D. Howard and Reid L. Sawyer, eds., *Terrorism & Counterterrorism: Understanding the New Security Environment,* second ed. (McGraw Hill/Dushkin, 2006), 363–364; see also Europol, "TE-SAT 2011: EU Terrorism Situation and Trend Report," European Police Office, The Hague, 2011, 10.

19 As quoted in Scheuer, *Imperial Hubris,* 81.

20 Hanna Rogan, "Abu Reuter and the E-Jihad: Virtual Battlefronts from Iraq to the Horn of Africa," *Culture & Society* (Summer/Fall 2007): 91.

21 Seib and Janbek, *Global Terrorism and New Media*, 32.

22 Ibid., 29.

23 Ibid., 35.

24 Waldmann, "The Radical Milieu," 25.

25 Stefan Malthaner, "The Radical Milieu: Conceptualizing the Social Environment of Radicalization and Terrorist Violence," unpublished paper, University of Bielefeld, Germany, November 2010, 3.

26 As quoted in Akil Awan, Andrew Hoskins, and Ben O'Loughlin, *Radicalisation and Media: Connectivity and Terrorism in the New Media Ecology* (London: Routledge, 2011), 31.

27 Ibid., 128.

28 Ibid.

29 Ibid., 54.

30 Gilbert Ramsay, "Relocating the Virtual War," *Defence Against Terrorism Review* vol. 2, no. 1 (2009): 35.

31 For more on the characteristics of these websites, see "Rethinking the Role of Virtual Communities in Terrorist Websites," by Dana Janbek and Paola Prado, in this issue.

32 Ramsay, "Relocating the Virtual War," 42.

33 Daniel Kimmage, "The Al-Qaeda Media Nexus: The Virtual Network Behind the Global Message," Radio Free Europe/Radio Liberty (RFE/RL), Washington, D.C., 2008; Nelly Lahoud, "Beware of Imitators: Al-Qai'da Through the Lens of its Confidential Secretary," Combating Terrorism Center, United States Military Academy West Point, New York, June 4, 2012, 43, 59.

34 As quoted in Awan et al., *Radicalisation and Media,* 56.

35 Ibid., 64.

36 Seib and Janbek, *Global Terrorism and New Media*, 55.

37 Meleagrou-Hitchens, "As American as Apple Pie," 11.

38 Rep. Jane Harman, as quoted in Gordon Lubold, "Why is Anwar Al-Awlaki Terrorist 'No. 1'?" *The Christian Science Monitor,* 19 May 2010.

39 Jonathan Githens-Mazer, "Radicalisation Via YouTube? It's Not So Simple," *The Guardian,* 4 November 2010: http://www.guardian.co.uk/commentisfree/2010/nov/04/youtube-radicalization-roshonara-choudhry; accessed on October 8, 2012.

40 Awan et al., *Radicalisation and Media,* 58–59 and 64–65; and Ramsay, "Relocating the Virtual War," 35.

41 Europol, "TE-SAT 2011," 11.

42 Ronald K. Noble, "Preventing the Next 9/11," *International Herald Tribune,* September 5, 2011.

43 "Contest: The United Kingdom's Strategy for Countering Terrorism," U.K. Home Office, Westminster, 2011, 25.

44 William Maclean, "Islamist Videos, Populists Stir German Worries," *Reuters*, September 5, 2011.

45 Peter Forster details the latter two cases in his article "Countering Individual Jihad: Perspectives on Nidal Hasan and Colleen LaRose," in this issue.

46 It has since come to light that the al-Hesba online discussion forum was actually run by the CIA; see Awan et al., *Radicalisation and Media,* 125.

47 Ibid., 63.

48 Ibid., 64.

49 Vikram Dodd, "Roshonara Choudhry: Police Interview Extracts," *The Guardian,* November 4, 2010.

50 Meleagrou-Hitchens, "As American as Apple Pie," 56.

51 Jason Burke, "Al-Shabab's Tweets Won't Boost its Cause," *The Guardian,* December 16, 2011.

52 Ibid.

Rethinking the Role of Virtual Communities in Terrorist Websites[1]

Dana Janbek and Paola Prado

Many security officials, policy analysts, and researchers are quick to identify the internet as a powerful terrorist recruiting tool that poses a growing security threat. Some worry that rapidly evolving technical capabilities offer terrorist groups a new strategic weapon with which to attack their enemies.[2] Al Qaeda and the Zapatista National Liberation Army (EZLN) in Mexico were among the first such organizations to lead the migration of terrorist rhetoric to the Web, spearheading the exponential growth of such sites from a mere dozen in 1997 to more than 6,000 today.[3]

Researchers have established that most extremist websites seek to fulfill five basic goals: to disseminate propaganda, organize the membership, communicate information, fundraise, and recruit new members.[4] In 2001, Jenine Abboushi Dallal suggested that terrorists were embracing the Web as a platform from which to recast their images.[5] In her view, extremist groups went online not so much to engage in dialogue, but rather to offer a "counter information system," and to create a virtual community. Dallal contended that these sites were not meant to be participatory or interactive, but rather were created to promote a tightly controlled authoritarian narrative.

Extremist groups went online not to engage in dialogue, but to offer a "counter information system."

Given the rapid proliferation of participatory applications on the Web in recent years, we set out to examine whether terrorism-related websites had embraced the Web 2.0 interactive applications that build community through commentary, social networking, and streaming video. Is there evidence that the internet has successfully generated virtual communities around websites run by terrorist groups?

To answer this question, between 2009 and 2010 we analyzed the discursive strategies and representations of virtual communities on 38 terrorist-related websites, 28 published in Arabic and 10 in Spanish (see Appendix A). Our content analysis identified in each case: 1) the sender of a message; 2) the content of that message; 3) the intended publics (readers of the message); and, 4) the interactive and multimedia features available to users of that particular website. The 38 websites we coded were filtered from an initial list of 80 Muslim-based and 20 Spanish-language extremist sites identified in studies conducted since 2000. For the purposes of this analysis, "extremist" sites were defined as sites that explicitly endorsed hatred and violence, and actively promoted their ideologies online. The filtered core list was expanded using the external links on each site, the Google search engine in Arabic and Spanish, and the back-link function of BacklinkWatch (this function helps researchers determine what websites link to the website they are studying).

A Terrorist Counter-information System

In 2004, researcher Gilles Kepel wrote: "Al Qaeda was less a military base of operations than a database that connected jihadists all over the world via the Internet."[6] The hyperlinks that connect the websites of these organizations to

Al Qaeda connects like-minded organizations in cyberspace, reinforcing the real-world extremist network with a virtual community mirror.

one another confirm this argument. Rather than relying solely on real-world physical connections, al Qaeda also connects like-minded organizations and their members in cyberspace, reinforcing the real-world extremist network with a virtual community mirror. Yet the results of our analysis suggest that these organizations limit user interactivity in the virtual communities they create by maintaining tight control of all discourse, while avoiding the most common and popular Web 2.0 interactive applications.

Common Features

Looking through these Arabic- and Spanish-language websites, we saw common trends.

Most of the websites presented a static narration of the organization's mission, history, and goals.

More than two-thirds of the Arabic-language websites and half of the Spanish-language ones offered responsive search functions and featured multimedia displays in the form of audio files, video files, pictures, or a combination of the above. Most of the websites displayed user-friendly navigation, ample content, and working hyperlinks that presented a static narration of the organization's mission, history, and goals, in a format that we now associate with the early days of the "read-only" Web. Interactive features were notably absent from all sites.

Arabic- and Spanish-language websites displayed different categories of content in their photos. While all websites showcased images of local people, guerrillas, fighters, and clashes with security forces, the Arabic-language ones included more graphic photos of blood-spattered bodies and corpses. The content of the audio and video files for all websites frequently featured talking heads, or a narration that provided a romanticized view of the organization and its members. Overall, the websites were user-friendly and sought to engage and entertain users by providing multimedia offerings. A few of the sites offered variable download speeds, a feature meant to enhance the user experience. While the availability of multimedia content hints at a level of technical sophistication, however, formatting errors such as broken multimedia hyperlinks were plentiful, possibly hinting at a scarcity of technical resources.

Overall, the websites were user-friendly and sought to engage and entertain users.

As mentioned, interactive features were sparsely available. One-third of the Arabic-language websites included listservs, forums, RSS features, guest books, or a comments section. None made chat rooms or blogs available to users. Five of the ten Spanish-language websites we coded offered users RSS feeds and the opportunity to register their e-mail (presumably, although this was not clearly stated, for the purposes of joining a mailing list). Only two of those five provided fora where users might register their comments; these consisted of moderated environments where comments were subjected to review and approval prior to publication. Editorial controls on most of the 38 sites prevented users from posting comments uncensored, and forum rules restricted comment threads. Likewise, when sites provided room for user feedback, the feedback was sometimes deleted (users complained accordingly). It is thus possible that the organizations allowed like-minded individuals to post comments but suppressed dissenting views. None of the sites provides links to social networking applications and tools, thus discouraging users from easily sharing or commenting upon the content. This choice of

format and tight editorial control seem to indicate that the primary goal of these sites is to inform, persuade, and communicate a structured discourse, rather than to engage users in dialogue.

The primary goal of these sites is to inform, persuade, and communicate a structured discourse, rather than to engage users in dialogue.

Target Audiences

Of the 38 sites we coded, most consistently proffered a discourse and message that resembled those of real-world resistance movements that seek to capture the media spotlight through violent acts of terror. Most sites framed their overall mission as a struggle to end foreign occupation through armed resistance. Prominently displayed banners and seals associated the organizations with patriotic or religious armed resistance movements. The few sites that listed the names of their martyrs and detailed the operations in which the martyr died stressed the importance of armed resistance and sacrifice. Among Muslim organizations, the farewell videos posted by aspiring "martyrs" on their websites justified the planned violent suicides by borrowing heavily from the *Qur'an*.

Most of the sites targeted current members and potential recruits, or local and international media audiences, with customized messages. News releases published online, while ostensibly targeted to the news media, also seemed geared to deliver information to current members and potential recruits, providing political analysis that countered mainstream news reports. Published in a variety of languages, these releases seem to confirm that the organizations sought to influence foreign public opinion beyond the Arabic- or Spanish-speaking worlds.

News releases published online seemed geared to deliver information to current members and potential recruits.

While the majority of the sites seemed to target male users, a notable few had sections geared to women, and two sites included content meant for children. This may indicate the beginning of a shift in the mostly patriarchal groups that some researchers identified as predominant on the internet.[7] Overall, however, the online discourse remains predominantly masculine in tone.

A few sites had sections geared to women, and two sites included content meant for children.

Multimedia applications provide a compelling alternative to text-based content among younger or semi-illiterate audiences. One of the sites offered mobile ring tones, confirming its intent to connect to a younger, media savvy demographic. The same site boasted mobile video footage, possibly indicating the involvement of a younger generation in the production of jihadist propaganda. A few sites included user-generated information, but in each instance user content was submitted to a moderator for approval prior to publication, presumably to allow for editorial control of the narrative and censorship of critical or opposing views.

Research has shown that video and interactive content features and applications that allow users to stay connected with the organization and interact with other members are central to the promotion of virtual community.[8] Such features have been shown to foster virtual ties between the organization and its supporters. Yet, the near total absence of interactive components in the websites we analyzed is consistent with a "read-only" online environment, where the narrative is tightly controlled in a way that eschews the participatory and community-building capabilities of the interactive Web.

The near total absence of interactive components in the websites is consistent with a "read-only" online environment.

Conclusions

Twelve years after Dallal reached her conclusions concerning the limited ways terrorists were likely to use websites, it does indeed seem that terrorist groups continue to rely on the internet to communicate a "resistant discourse," and propose a counter-hegemonic narrative through a traditional unilinear mode of communication. No matter how active or tame their online presence, these groups for the most part have yet to leverage the power of interactive Web 2.0 applications to create vibrant participatory communities.

Whereas the rapidly increasing availability of interactive and collaborative Web features now allows for real-time dialogue among users worldwide, terrorism-related websites remain static, tightly moderated, and effectively closed Web environments. They monitor user-generated content, shy away from adopting Web 2.0 technologies that enable users to develop unique voices or attract a personal following, and curtail messages that contradict or challenge the organization's viewpoint. Forgoing Web 2.0 interactive features, these terrorist sites provide a controlled model of information flow, a unidirectional narrative that eschews the possibility of dialogue. True to their ideological purpose, the sites seek to inform, persuade, and communicate a predetermined message, rather than to offer a public space for the free exchange of ideas. The websites thus work to reinforce existing beliefs and to connect like-minded individuals in the virtual world.

Terrorism-related websites cater to audiences that perceive the underlying organizations as legitimate political movements.

For the most part, extremist or terrorism-related websites cater to audiences that perceive the underlying organizations as legitimate political movements. They publish online content that counters traditional media discourse, acknowledges shared grievances, and reframes narratives of political conflicts. This content resonates among those who share an alternative worldview that more often than not remains marginalized by the mainstream press. Having adopted the internet as a strategic tool, these groups offer an alternative media source and provide an online forum that engages audiences in a closely moderated dialogue. In this corner of cyberspace, like-minded individuals share online virtual communities where the narrative rigidly follows the ideological party line. ❖

ABOUT THE AUTHORS

Dr. Dana Janbek is assistant professor of Public Relations at Lasell College in Newton, Massachusetts, where she teaches graduate and undergraduate communication courses. Her research focuses on terrorist use of the internet as a media outlet, and the use of information and communication technologies in developing nations, specifically the Middle East. Dr. Janbek is co-author, with Philip Seib, of *Global Terrorism and New Media: The Post Al-Qaeda Generation* (Routledge, 2010). She earned a Ph.D. in Communication from the University of Miami. Dr. Janbek is originally from Jordan and is fluent in English and Arabic.

Dr. Paola Prado, assistant professor, Journalism and Digital Media at Roger Williams University, specializes in digital inclusion, digital media convergence, and multimedia production. Her research focuses on the adoption of

information and communication technologies for development and social change in Latin America. She is the co-creator of the *Community Communicators* journalism and multimedia workshop program, which trains community reporters in Colombia and the Dominican Republic. She is the author of journal articles and book chapters on topics related to digital inclusion, media diversity, and the effect of the internet on gender roles in Latin America. Dr. Prado earned a Ph.D. in Communication from the University of Miami. She is fluent in English, French, Portuguese, and Spanish.

APPENDIX A: EXTREMIST WEBSITES ANALYZED IN THIS STUDY[9]

Arabic-language websites

1 Islamic Army in Iraq
2 Tawhid and Jihad Forum
3 Islamic Resistance in Lebanon
4 Baghdad Sniper
5 Al-Aqsa Martyrs Brigade
6 Gama'a al-Islamiyya (Islamic Group)
7 Brigades of the Martyr Ezzedeen Al-Qassam
HAMAS (Islamic Resistance Movement)
8 Palestine Liberation Front (PLF)
9 Popular Front for the Liberation of Palestine (PFLP)
10 PFLP-General Command (PFLP-GC)
11 Ansar al-Islam
12 The Jihadi Empowerment Network
13 Al-Nasser Salah Addin's Brigade
14 Jihad and Reform Front
15 Jamaat Ansar Al-Sunna
16 Al-Muslmeen Army in Iraq
17 Army of Saad bin Abi Waqas
18 The Army Men of Al-Nakshabandia Way
19 Islamic Front for the Iraqi Resistance, Jame3,
The Brigades of Salah Al-Deen Al-Ayoubi
20 The Islamic Resistence Movement—Hamas
Iraq—Al-Fatih Al-Islamy Brigades
21 Jihad and Change Front
22 High Command of Jihad and Liberation
23 Al-Rashedeen Army
24 The Brigades of the Martyr Abu-Ali Mustafa—Media Site
25 Jihad on the Land of Rafedean Brigades—News Network
26 The Nationalist and Islamic Front
27 Al-Mojahden
28 The Voice of Jihad

Spanish-language websites

29 National Liberation Army—Eln Voces
30 National Liberation Army—Frente de Guerra Oriental
31 National Liberation Army, Patria Libre
32 National Liberation Army, Occidente Rebelde
33 Zapatista National Liberation Army, EZLN
34 Zapatista National Liberation Army, Zezta Internazional
35 Zapatista National Liberation Army Radio
36 Rebeldia Magazine
37 EZLN Letters and Communications
38 Revolutionary Army of the Insurrectionist People

NOTES

1 The authors thank Shannon Hodge, student at Lasell College, for her research assistance.

2 Gabriel Weimann, "Terror on the Internet: The New Trends," speech delivered at the University of Miami School of Communication, Coral Gables, Florida, October 23, 2008.

3 Jon Swartz, "Terrorists' Use of Internet Spreads," *USA Today,* February 21, 2005: http://www.usatoday.com/money/industries/technology/2005-02-20-cyber-terror-usat_x.htm; accessed September 19, 2012.

4 Barbara Berman, "Remarks by Barbara Berman," in "Combating Terrorist Uses of the Internet," Ashley Deeks, Barbara Berman, Susan Brenner, and James A. Lewis, eds., Proceedings of the American Society of International Law Annual Meeting, 2005, 104–108; Fred Cohen, "Terrorism and Cyberspace," *Network Security* vol. 5 (2002): 17–19; Steven Furnell and Mathew Warren, "Computer Hacking and Cyberterrorism: The Real Threats in the New Millennium," *Computers and Society* vol. 18, no. 1 (1999): 28–34; Timothy Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning,'" *Parameters* vol. 33, no. 1 (2003): 112–123; and Gabriel Weimann, "Www.terror.net: How Modern Terrorism Uses the Internet," United States Institute of Peace, Washington, D.C., 2004: http://www.usip.org/files/resources/sr116.pdf; accessed on October 8, 2012.

5 Jenine Abboushi Dallal, "Hizballah's Virtual Civil Society," *Television New Media* 2 (2001): 367–372.

6 Gilles Kepel, *The War for Muslim Minds: Islam and the West* (Cambridge, Mass.: The Belknap Press of Harvard University Press, 2004), 6.

7 Fernando Reinares, "Who are the Terrorists? Analyzing Changes in Sociological Profile among Members of ETA," *Studies in Conflict & Terrorism* vol. 27, no. 6 (2004): 465-488; and Charles Russell and Bowman Miller, "Profile of a Terrorist," *Terrorism: An International Journal* vol. 1, no. 1 (1977): 17–34.

8 "Jihad TV: Terrorism and Mass Media," Paul Eedle, producer, Films Media Group, Princeton, New Jersey, 2006; Thomas, "Al Qaeda and the Internet," 112–123.

9 The above websites were active from 2009 to 2010, when the data for this study were coded. Counterterrorism agencies worldwide work continuously to disable websites linked to extremist groups. For that reason, some of these websites may no longer be in service and/or their content may have migrated to mirror sites.

Countering Individual Jihad: Perspectives on Nidal Hasan and Colleen LaRose

Peter Kent Forster

In December 2011, U.S. Homeland Security Secretary Janet Napolitano told an interviewer that the risk of attacks by so-called "lone wolves," individuals with no apparent ties to known extremist networks or conspiracies, is on the rise, and is an indication that the global terrorist threat has shifted.[1] Secretary Napolitano's statement is a sobering assessment of the violent Islamist threat to the United States. While her definition characterizes a particular kind of perpetrator, however, in today's networked world the individual is not as isolated, and is perhaps more dangerous, than previously assumed. To deal with these changes, new counter-measures need to be adopted.

Online activities create "digital exhaust" that erodes the individual jihadist's anonymity.

The internet has been widely recognized as a multi-faceted tool for terrorist groups for quite some time, but recent digital innovations such as social media networks have improved the virtual connectivity of the individual, not simply to an organization but to the entire terrorism process.[2] Exemplified by the Unabomber, the stereotypical "lone wolf" is a person who acts alone without orders or even connections to an organization.[3] These independent terrorists are still a danger, but access to the internet has given rise to others who consciously seek motivation and training online, or are systematically identified and cultivated by online facilitators, such as spiritual advisers, recruiters, or "link-men," to pursue violent jihad.[4] These individual jihadists are not as isolated as we assume the "lone wolf" to be. Digital forensics show that their online activities, such as email communications, on-line searches for information on potential targets, and even online ideological statements, create "digital exhaust" that erodes the individual jihadist's anonymity.[5]

The individual embraces a violent Salafist ideology in his or her personal world, but is ultimately incited to actual violence through virtual interactions.

The debate regarding the internet's effectiveness in inciting an individual's progression from "indoctrination" to "jihadization," (i.e., violent Islamist extremism) continues.[6] This article contributes to this debate by examining the individual jihad, in which the individual embraces a violent Salafist ideology in his or her personal world, but is ultimately incited to actual violence through virtual interactions. It examines this phenomenon's impact through two U.S.-centric cases that provide evidence that on-line "jihadization" can occur when inspired or systematically managed by an online facilitator. The first explores how virtual interactions contributed to Nidal Hasan's decision to attack fellow soldiers at Fort Hood in November 2009. The second shows how internet communications were used to identify, vet, and ultimately impel Colleen LaRose to recruit individuals, solicit funds for a terrorist organization, and plan an attack.

A decade after the attacks of September 11, 2001, extreme Islamist terrorism reflects the maturation of al Qaeda's ability to inspire through ideology even as the core organization deteriorates. It is the manifestation of an ideological

raison d'etre that exploits an environment in which violent Salafism can spread, and an individual be incited to act, without any face-to-face interactions. This process is accomplished through a progressive exploitation of the internet and associated technologies as powerful tools for communication, information sharing, and information analytics.

Against this background, the following questions provide a context for examining the individual jihadist who has a global reach and global connections through digital media:

- How are terrorists using the internet to incite individuals to violence?
- When does radical belief constitute terrorism and a security issue in an online environment?
- How might counterterrorist experts combat the individual jihad?

This article challenges some of the traditional perspectives on the role of the internet in motivating terrorism. As proposed here, it may be possible to prove intent to commit terrorism without waiting for a physical act of violence, by assessing the "digital exhaust" from online activities. After discussing the two case studies of Hasan and LaRose, the article suggests some potential counter-strategies available through forensic analysis.

It may be possible to prove intent to commit terrorism without waiting for a physical act of violence.

Technology Extends the Jihad

The "multiplicity and interconnectedness of threats and actors," including the fact that small groups have greater access to lethal technologies, is considered by U.S. officials to be the most serious danger to U.S. national security.[7] This reality is not lost on the terrorists. Technology has played a role in both al Qaeda's growth and its devolution. Al Qaeda's Afghanistan-based core, responsible for planning and executing terror attacks from 1998 to 2002, embraced technology both as a media platform and a planning tool. The 9/11 Commission Report describes Muhammad Atta emailing flight schools to ask the cost of training, and using the internet to conduct financial transactions and find housing while planning the 9/11 attacks.[8] After al Qaeda was driven from its Afghan safe haven in 2002, the internet's importance to jihadists increased. Between 2003 and 2007, al Qaeda's central media group grew its operations from six to 97 annual productions, which were disseminated primarily via the internet.[9] Internet jihadists such Younis Tsouli (a.k.a. Irahibi007) and Malika al Aroud used the online environment to recruit, propagandize, train for, and conduct cyber-attacks.[10] By 2008, al Qaeda's core recognized that the internet reduced the time and costs of operational communications while increasing the scope of information-sharing among geographically disbursed groups.[11] The jihadists had shifted from being consumers of information to "networked participants." This process has continued and will intensify as operational competency migrates to associated movements.[12]

The jihadists had shifted from being consumers of information to "networked participants."

Osama bin Laden was pre-occupied with attacking the United States, perhaps to the detriment of considering regional targets and other strategies.[13] His diminished relevance over the past few years and subsequent death, however, led to a resurrection of the individual jihad. A primary advocate

of this strategy is Abu Musab al-Suri, a strategic-minded, innovative, and ideologically grounded al Qaeda leader, who either escaped or was released from a Syrian jail in February 2012. Prior to his capture in November 2005, al-Suri openly disagreed with bin Laden's "America first" strategy in favor of the individual jihad, the foundation of which is found in his treatise, *The Global Islamic Resistance Call.* His arguments have recently been re-printed in the online magazine *Inspire*, produced by the group al Qaeda in the Arabian Peninsula (AQAP). In these articles, al-Suri extolled the value of the individual jihad as a reasonable response to Islam's "humiliation."[14] He declared that military success would result from spontaneous operations that confuse local and international intelligence, while such actions would also provide operational security for the larger organization by ensuring that the disruption of one cell does not influence another.[15] The individual jihad is, as he described it, geographically independent. As reflected in the 2005 London bombings, which he masterminded, al-Suri encouraged individuals to resist assimilation and participate in jihad where they are.[16] He also advocated centering the jihad in Yemen.[17] His strategy was further endorsed by Anwar al-Awlaki, the now-deceased American-born imam and AQAP leader, who called upon Muslims in the West to either leave and live among Muslims, or stay behind and follow the violent example of Nidal Hasan, the individual jihad's poster child.[18]

Al-Suri declared that military success would result from spontaneous operations that confuse local and international intelligence.

The online environment is reducing geographic distance, improving security, and accelerating the individual jihad. By leveraging connectivity, the virtual environment globalizes local issues and creates a broad self-selecting echo chamber in which a community forms around shared ideas, indoctrinates itself, and blurs the incremental movement from radicalization to violent jihad. The echo chamber serves the individual jihad well. It allows individuals to bond virtually to the ideology and religious perspectives of extremists, a key part of the training process that usually occurs in the training camps, but it does not create the human bond of direct contact.[19] Furthermore, attacks such as Abdulhakim Muhammad's on an Arkansas army recruiting center in 2009, or Mohamed Merah's killing of three school children and three French paratroopers in Toulouse in March 2012, epitomize the individual jihad's effectiveness, particularly when juxtaposed against the failures of centrally planned plots.

The virtual environment blurs the incremental movement from radicalization to violent jihad.

The internet's anonymity and accessibility also change the operational paradigm by providing opportunities for online vetting, training, and operational direction. Increasingly, Facebook and Twitter serve to re-post material and share content more quickly, thus expanding the capability of the individual jihad.[20] The internet keeps the constituency in constant contact with the material and each other, while frustrating attempts by law enforcement and intelligence agencies to disrupt access. Leveraging online networks is accelerating the linkages between the successors of long-established groups with organizational structure (i.e., command and control, and a training apparatus), and a new collection of self-radicalized individuals.[21] While both "lone wolves" and individual jihadists can be characterized as self-recruited, leaderless thrill seekers connected via cyberspace,[22] the latter participate in an interactive online environment with a facilitator, rather than on their own.

The Individual Jihad: Two Cases

The individual jihad has many faces and unique operational tendencies. The ability of law enforcement and intelligent analysts to recognize a "lone wolf" is hindered by a lack of information about the perpetrator, his motives, and objectives. As noted by U.S. Senator Joseph Lieberman, a "lone wolf's" available profile typically is limited, attacks are planned without guidance, and the lack of co-conspirators makes it less likely that intelligence analysts and law enforcement will be able to identify a plot or the plotter prior to the attack.[23] The cases of Colleen LaRose (a.k.a. Jihad Jane) and Nidal Hasan, by contrast, represent individuals who are connected and recognizable. These cases provide insight into the individual jihad process in the United States, and represent a threat that is contrary to both the conventional wisdom of the "lone wolf" and the assumption that face-to-face contact is needed to incite effective jihadization. Each perpetrator had ongoing interactions with an online facilitator, although the roles of those individuals differed. In the Hasan case, Anwar al-Awlaki's spiritual guidance compelled Hasan to become a jihadi foot soldier. LaRose interacted with a handler who developed her as a "manager."[24] While both facilitators sought to channel their charges' desires to participate in violent jihad, the handler in the LaRose case took a more active role in vetting his recruit and then operationalizing a plot. Together these cases illustrate a variety of virtual interactions, and suggest inferences between the online interactions and ultimately violent action. Furthermore, a review of the indictments and court transcripts help define the legal threshold online interactions must cross to establish terrorist intent.

Both "lone wolves" and individual jihadists can be characterized as self-recruited, leaderless thrill seekers connected through cyberspace.

Nidal Hasan

U.S. Army Major Nidal Hasan opened fire at the Soldier Readiness Center in Fort Hood, Texas on November 5, 2009, killing 13 and wounding 32 before being wounded himself and captured. The following brief synopsis of events leading up to the shooting focuses on the importance of Hasan's online interactions with al-Awlaki as the catalyst to his jihadization. Although Hasan harbored radical ideas prior to renewing communications with al-Awlaki in 2008, the online communications are possibly significant in his decision to take action.

Hasan responded to al-Awlaki by asking if he were allowed to kill fellow soldiers.

Hasan first met al-Awlaki in 2001, while the latter was the imam at the Dar al-Hijrah Mosque in Falls Church, Virginia, where Hasan worshiped.[25] The cleric reportedly presided at Hasan's mother's funeral around that time.[26] The death of his mother and his connection to al-Awlaki were possible catalysts to Hasan's radicalization.[27] Hasan became increasingly vocal in expressing his Islamist beliefs, and his radicalization apparently reached a "crescendo" in 2007-2008, when he is believed to have published a pamphlet entitled "Martyrdom in Islam versus Suicide Bombing;" after that, however, his public displays dissipated.[28] In December 2008, after a seven-year hiatus, he renewed e-mail contact with al-Awlaki, and over the next ten months communicated with him eighteen times. At one point, al-Awlaki sent Hasan a copy of "44 Ways of Supporting Jihad," which urges Muslims to defend Islam through violence.[29] Hasan responded by asking if he were allowed to kill fellow soldiers.[30]

While reports indicate that al-Awlaki did not order Hasan to take action, when understood within the context of al-Awlaki's ability to inspire individuals to violent action, his counsel was likely influential.[31] Al-Awlaki had inspirational and operational contacts with a range of terrorists, including Umar Farouk Abdulmutallab, the Nigerian who tried to blow-up a U.S.-bound flight from Amsterdam on December 25, 2009, and Faisal Shahzad, who tried to set off a homemade car bomb in New York's Times Square in May 2010. Furthermore, al-Awlaki proudly claimed Hasan as "one of his students."[32] Finally, a February 2011 report by U.S. Senators Joseph Lieberman and Susan Collins clearly indicates that failure by the FBI and the Defense Criminal Investigation Service to flag Hasan's numerous communications with al-Awlaki, through which one plausibly could infer the radicalizing nature of the relationship, was instrumental in their inability to recognize him as a threat.[33]

The FBI neglected the counterterrorism process of inferring capability and intent.

At a minimum, Hasan's interactions with al-Awlaki were an accelerant to jihadization, but how this fact is addressed at trial illustrates a significant obstacle to successfully countering the individual jihad. In the Hasan case, the FBI focused on the occurrence (or previous non-occurrence) of a terrorist act, rather than the individual's apparent intent to commit violence, and thereby neglected the counterterrorism process of inferring capability and intent.[34] The prosecution might use the virtual connections with al-Awlaki to demonstrate intent to commit terrorism, but these probably will be considered secondary to the murder evidence. Thus, the commission of a clearly prosecutable crime is the basis of the Hasan case. His online interactions, however, provide evidence that he posed a security risk prior to the attack.

Colleen LaRose

On February 1, 2011, Colleeen LaRose, a Pennsylvania woman, pleaded guilty to 34 accounts of material support to terrorism. Often dismissed for its amateurism and lack of operational security, the LaRose case has received less scrutiny than Hasan's. Her case demonstrates that Islamist extremists are using the internet to identify and develop potential recruits in the United States. Furthermore, it increases our understanding of the internet's role in the individual jihadist movement, from inciting an individual to go from aspirational to operational activities, to enabling a handler to vet prospective recruits online and evaluate with some assurance whether they will take action. Counterterrorism experts are using data from the case to establish different criteria for how online interactions pose a prosecutable security threat.

Islamist extremists are using the internet to identify and develop potential recruits in the United States.

A self-proclaimed fan of Anwar al-Awlaki, LaRose, using the pseudonym Jihad Jane, posted a YouTube video in June 2008 expressing her "desperate" desire to help suffering Muslims.[35] This was sufficient information for Islamist extremists, trawling the internet for potential recruits, to initiate an online evaluation of her. For eleven months beginning in December 2008, LaRose communicated online with a variety of people who vetted her, supported her operationally, and ultimately directed her avowed commitment to jihad toward violent action.

In December 2008, LaRose received a response to her June post from a male in South Asia (co-conspirator #1 according to court records) who engaged

her in an online conversation about their shared desire to wage jihad, and proposed that she consider becoming a shaheed, or Islamic martyr.[36] In January 2009, a Western European resident (co-conspirator #2) emailed LaRose that he desired to become a martyr and although unsuccessful, he would continue to try. LaRose responded that she also desired martyrdom. In a February 2009 communication, LaRose confided to CC#1 that her physical appearance allowed her "to blend in with many people," a factor that could help her online contact achieve his jihadi goal. The revelation about her physical appearance created sufficient interest to warrant additional attention from her correspondents, and in March a third individual (co-conspirator #3) interjected himself into the conversation. He assumed the role of handling LaRose by developing an incremental process in which he would be responsible for evaluating the recruit's commitment to acting, and for operationalizing an attack. Information revealed later in the indictment indicates those initial communications between LaRose and the first two men were apparently random exchanges between "like-minded" individuals; CC#3, however, asks LaRose to tell him about CC#2, evidence of how terrorists seek to exploit social networks to identify other potential recruits.

A male in South Asia engaged her in an online conversation about their shared desire to wage jihad.

CC#3 initially established minimal bona fides for himself by telling LaRose that he was familiar with explosives. Concurrently, he suggested LaRose use the internet to "invite" another unidentified male fighter to join CC#3 for training in "the South Asian country."[37] He then reiterated that LaRose's nationality allowed her freedom of movement, and asked LaRose to marry him so he could travel to Europe. LaRose agreed to marry him and made inquiries of the Swedish embassy about obtaining residency. At this point, CC#3 played a bit of a psychological game and allowed two weeks to pass after the marriage agreement before he contacted her again. This allowed her time to conduct the residency inquiries, but it is quite plausible that it also was a test of her reliability, to see whether she would go to the police or had a true psychological commitment to the cause. On March 22, 2009, CC#3 directed LaRose to go to Sweden to kill the cartoonist Lars Vilks.[38] LaRose agreed immediately.

Co-conspirator #3 would be responsible for evaluating the recruit's commitment to acting.

Upon accepting the mission, LaRose assumed an operational role as a fundraiser and global recruiter. She posted online solicitations for funds to support terrorism, and electronically distributed a carefully worded questionnaire that aimed to determine whether other Western women harbored an interest in jihad.[39] Between December 2008 and March 2009, LaRose also had online discussions with Ali Damache, an Algerian man residing in Ireland who had expressed interest in martyrdom.[40] Damache helped develop the questionnaire that LaRose distributed. In August 2009, LaRose started an online dialogue with Jamie Paulin-Ramirez, a Colorado woman, ultimately convincing her to travel Ireland to participate in jihad.[41] When she reached Ireland with her young son, Paulin-Ramirez married Damache, a man she had never before met face-to-face. Simultaneously, LaRose gathered intelligence on Vilks, including joining his online community. She ultimately told her handler that it was "an honor and great pleasure to die or kill" for him.[42] Nevertheless, there is no evidence that she ever travelled further than Ireland, where she was supposed to marry "co-conspirator #3."[43] She was arrested upon her return, unmarried, from Ireland in October 2009.

CC#3 directed LaRose to go to Sweden to kill Lars Vilks. LaRose agreed immediately.

The Significance of the Online Jihadist

The effectiveness of online recruitment and the process of engagement in these two cases are chilling. LaRose's public pronouncements made her easily identifiable as a potential *shaheed* recruit, but the potential usefulness of her physical appearance changed the dynamics. LaRose underwent a virtual vetting process, in which she performed a series of tasks to prove her commitment and willingness to act. As she completed each task, the handler became more confident in her. This process resembles a traditional face-to-face vetting process that focuses on psychological processes to determine commitment and aid indoctrination.[44] Furthermore, the process was completed relatively quickly. Within nine months from the initial contact, LaRose was travelling to Europe to execute the operation.

LaRose underwent a virtual vetting process to prove her commitment and willingness to act.

The case of "Jihad Jane" portrays the individual jihadists as part of a virtual network of participants with global reach and global connections. LaRose was incited to jihadization through online engagements and without any face-to-face contact. It was her poor personal and operational security, particularly a number of provocative online comments, that apparently alerted a private group known as Youtube Smackdown to track her posts and eventually tip off the FBI.[45] The public nature of her discussions permitted extensive internet tracking that adds to our understanding of the online world's role in the individual jihad. According to Assistant U.S. Attorney Jennifer Arbittier Williams, the electronic evidence gathered from LaRose's online interactions with co-conspirators would be sufficient to prove she traveled to Europe to locate Vilks, and that she attempted to raise funds for terrorists and recruit trainees in Europe and Asia.[46] While conspiracy to kill in a foreign country and travelling to Ireland in support of violent jihad may have been the catalysts for authorities to arrest her, the majority of the 34 "overt acts" noted in her indictment dealt with her online recruiting and fund solicitation activities.[47]

The majority of the 34 "overt acts" in her indictment dealt with her online recruiting and fund solicitation activities.

The differences between Hasan and LaRose contribute to our understanding of the breadth of individual jihadi strategies and tactics. Both reflect the desire by jihadist groups to recruit Americans, and the importance of the internet in this process. While al-Awlaki's message prompted LaRose to become more vocal in her radicalization, the imam's direct contact with Hasan inspired Hasan to self-directed action. Rather than relying on LaRose to take action on her own, her handler vetted her and provided specific direction towards supporting the jihad. Another lesson is found in the range of potential goals of online recruitment and action. Judging from the post-attack statements regarding Hasan, the execution of the attack was the culmination of his service to the individual jihad. He was meant to be a *shaheed*, a foot-soldier in the struggle. LaRose's recruitment of others who could travel in the West without detection, her solicitation of funds, and her broadening social network suggest her handler's goal was to develop a virtual cell leader. LaRose's lack of anonymity eroded her value to the jihadi network, but the lessons learned from her case will not be lost on her handler and others. Future recruitment and vetting can be expected to target less public individuals, who can assume the management roles of a network node facilitator, and perhaps cell leader, without creating as much digital exhaust. In sum, the online environment will continue to be a recruitment venue for the individual

jihad; recruitment objectives will vary; and through an online vetting process, various decisions will be made regarding the individual's role in jihad.

The lessons learned from the LaRose case will not be lost on her handler and others.

These cases indicate how the online environment is evolving, and will continue to influence and accelerate the radicalization and jihadization processes. Virtual networks, the internet, and associated media allow information to be shared quickly and permit active participation that enhances learning, cooperation, and innovation, thus enabling small groups and even individuals to accomplish big things. A recent White House meeting with local law enforcement identified three homegrown-terrorist warning signs: joining a group that advocates violence, receiving support from a network that plans violence, and seeking out a charismatic leader.[48] Today, these connections may occur entirely in the virtual environment, reducing the isolation associated with the "lone wolf."

Counter-strategies

Identifying and implementing effective counter-strategies against the individual jihad is a complex problem that requires cooperation, patience, and perhaps some luck. Innovative thinking, using technology as an investigative tool, and combating networks with networks are the strategies advocated by FBI Director Robert Mueller.[49] While the terrorists continue to exploit internet technologies to perform many tasks, the same technologies offer new avenues for law enforcement and intelligence services to track and identify terrorists. The virtual environment provides opportunities for collecting data, identifying linkages, tracking activities, and recognizing patterns. For example, by analyzing Colleen LaRose's online linkages, local law enforcement rolled up Ireland's first known jihad cell and arrested a co-conspirator in Maryland in May 2012.[50] Facebook and Twitter are repositories of voluntary information that may be collected and sorted to yield a searchable database from which less apparent linkages and warnings may be derived.[51] Existing open-source tools in the hands of individuals with a modicum of Excel skills and situational awareness of an event can extract commonalities and patterns from Twitter posts. Crowdsourcing, the evaluation of voluntary public information from groups, and participatory sensing, directed information collection or an informant 2.0 of sorts, also are valuable forensic methods. Increasingly, analytic techniques are making better sense from real-time online information and categorizing behavioral patterns through the analysis of digital exhaust. Still, it remains difficult to build a criminal case around intent derived from internet communications.

By analyzing Colleen LaRose's online linkages, local law enforcement rolled up Ireland's first known jihad cell.

Facebook and Twitter are repositories of voluntary information from which less apparent linkages and warnings may be derived.

The U.S. PATRIOT Act, passed in the wake of 9/11, expanded geographic authorization for FISA (Foreign Intelligence Surveillance Act) warrants, and the U.S. attorney general's office has provided some legal guidelines for their use. Confronting the individual jihad requires a comprehensive counterterrorism strategy that includes legal reforms, partnerships that facilitate intelligence gathering and sharing, community outreach, and education. Efforts at legal reforms that would criminalize the *intent* to do bad things through the analysis of online communications raise ethical and legal issues, and have had varying results. Mexico brought charges of terrorism against two individuals who used Twitter and Facebook to spread rumors about a school attack in Veracruz that resulted in real chaos.[52] Although the state

prosecutors argued that the perpetrators' virtual statements were equivalent to real ones, the case was dismissed. During riots in the United Kingdom in 2011, a number of people were arrested by British police and charged with inciting others to riot through Facebook and on Blackberries.[53] In the aftermath of the riots, British Prime Minister David Cameron advocated a law that would allow the government to shut down internet access to people the government considered a threat. While the legal threshold of intent seemed to shift with the successful prosecution of some of those arrested, their convictions still required the prosecution to link physical actions to their online activities. These verdicts reflect a likely result in the Hasan case, in which his physical actions, not his online activities, will be the basis of conviction.

Legal reforms to criminalize the *intent* to do bad things raise ethical and legal issues, and have had varying results.

The LaRose case, however, reflects a further evolution in the legal approach to online activity. The case against her was based in large part on 34 counts of providing material support to terrorists, primarily related to her online behavior.[54] As previously cited, U.S. Attorney Williams charged that her online fundraising and recruiting for a terrorist organization were prosecutable actions under the "material support" statue, equal to her intent to attack Vilks.[55] Her guilty plea, however, left it unclear whether a jury would have convicted her on all, or any, of those counts.

Judges may have greater latitude in the United States to try terrorism cases based on online intent.

The fact that the case was heard on the basis of the digital evidence seems to indicate that judges will have greater latitude in the United States to try terrorism cases based on online intent. The results of two other cases, one involving Tarek Mahanna, who was convicted of providing material support to terrorists include "translating and distributing" materials meant to inspire others to participate in jihad, and the other involving Jesse Curtis Morton, the leader of Revolution Muslim, convicted of using the internet to solicit murder and encourage violent extremism, also are evidence of a shifting paradigm.[56] Along with the broadening of the definition of cyber-terrorism, these cases establish a firmer precedent for prosecution based on establishing intent by examining online statements and activities. These cases, as well as the LaRose case, also contribute to the debate surrounding First Amendment protection of freedom of speech, in light of an emerging perspective that words and information that promote terrorism are dangerous. Both France and the United Kingdom have criminalized "advocacy" and "glorification" of terrorism.[57] In the United States, some have advocated lowering the threshold for prosecution by implementing a "clear and present danger" standard originally recommended in 1919.[58] Another approach is to amend the "material support" statute to encompass advocacy as a punishable offense. While such approaches would offer new legal tools for combating the individual jihad, they pose serious constitutional questions, particularly regarding the First Amendment. For example, when is advocacy of an opposing point of view something other than part of a legitimate democratic process guaranteed by law? As Sahar Aziz noted, the First Amendment is owned by everyone and is not discriminatory.[59] Echoing Aziz, First Amendment supporters in the United Kingdom and United States warn that forays into this area risk starting down a slippery slope that could jeopardize civil rights, and embrace government censorship of the internet and eavesdropping on personal communications.

In its 2011 "National Strategy for Counterterrorism," the White House stated, "The United States alone cannot eliminate every terrorist or terrorist organization … Therefore, we must join with key partners and allies to share the burdens of common security."[60] Inter-government, intra-government, and public-private partnerships are indispensible to countering terrorism, as both the Hasan and LaRose cases illustrate. Greater access to Hasan's earlier communications with al-Awlaki might have allowed the FBI to better understand his virtual relationship with al-Awlaki and understand the threat he posed. LaRose's extremist tendencies were initially recognized by a participant in the Middle East Performing Arts online forum. Having information and being able to effectively prosecute an individual based on that information, however, are two different things.

Such approaches pose serious constitutional questions, particularly regarding the First Amendment.

Conclusions

Eli Pariser warned, "A world constructed from the familiar is a world in which there's nothing to learn."[61] The internet is globalizing local issues and expanding the multi-ethnic composition of groups and causes. The online jihadi echo chamber is creating a fertile ground for indoctrination into extreme ideologies and operationalization of extremist plots. The cases of Nidal Hasan and Colleen LaRose demonstrate that individuals radicalized via the internet in their personal space can be incited to violent action through the same medium. While Homeland Security Secretary Napolitano's concern about the rising risk of "lone wolf" terrorism is well placed, it is also important to recall Sun Tzu's famous admonishment, "Know your enemy and know yourself, and you need not fear the result of a hundred battles."[62] While not disregarding the "lone wolf" phenomenon, it also is important to recognize that a presumed "lone wolf" may actually be linked to recruiters, inspirationalists, and planners in a virtual environment—in essence, creating virtual terrorist cells.

Individuals radicalized via the internet in their personal space can be incited to violent action through the same medium.

When compared to the isolation of the solely self-directed person, individuals who have maintained continuous internet interactions establish influential relationships, and can become willing to take violent action. While the effectiveness of online recruitment and indoctrination is understood, the debate continues over whether advocating extremism or participating in activities online constitute illicit actions. There is an emerging threshold, however, across which online interactions and activities are being considered a sufficient security risk to catalyze intervention. A basis from which to pursue legal prosecution of an individual based upon intent rather than strictly action is gradually emerging. The cases of Nidal Hasan and Colleen LaRose provide evidence of this changing paradigm. ❖

The debate continues over whether advocating extremism or participating in activities online constitute illicit actions.

ABOUT THE AUTHOR

Dr. Peter K. Forster is a senior lecturer, member of the graduate faculty, and the executive director of Online Education in the College of Information Sciences and Technology at Penn State University. His primary areas of interest are terrorism/counterterrorism, risk and crisis management,

international relations, and national security. He is a member of the NATO/OSCE Partnership for Peace Consortium Combating Terrorism Working Group, and has been involved with Penn State's Homeland Security program since its inception. He is the co-author of books on NATO's military burden-sharing and intervention, including most recently, with Stephen J. Cimbala, *Multinational Military Intervention* (Ashgate, 2010).

NOTES

1 Janet Napolitano, "Napolitano: Lone Wolf Terror Threat," CBS News, December 2, 2011: http://www.cbsnews.com/8301-201_162-57336080/napolitano-lone-wolf-terror-threat-growing; accessed January 31, 2012.

2 Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, D.C.: U.S. Institute of Peace Press, 2006), 109.

3 Edwin Bakker and Beatrice de Graaf, "Preventing Lone Wolf Terrorism: Some CT Approaches Addressed," *Perspectives on Terrorism* vol. 5 (2011): 43: http://www.terrorismanalysts.com/pt/index.php/pot; accessed March 13, 2012. The Unabomber, eventually identified as Ted Kaczynski, evaded capture for years while carrying out a terror campaign against people he held responsible for environmental damage. He lived as a recluse in the state of Montana, from where he sent out mail bombs that killed three and injured 23.

4 Mitchell D. Silber, *The Al Qaeda Factor: Plots Against the West* (Philadelphia: University of Pennsylvania Press, 2012), 4. See also Maura Conway, "From al-Zarqawi to al-Awlaki:The Emergence and Development of an Online Radical Milieu," in this issue.

5 "Global Trends 2025: A Transformed World," NIC 2008-003, National Intelligence Council, Washington D.C., November 2008: http://www.aicpa.org/research/cpahorizons2025/globalforces/downloadabledocuments/globaltrends.pdf; accessed on 5 September 2012; and, "Where Tomorrow Will Take Us: The New Environment for Intelligence," Center for the Study of Intelligence, Washington D.C. 2009.

6 Mitchell D. Silber and Arvin Bhatt, "Radicalization in the West: The Homegrown Threat," New York City Police Department, 2007: http://www.nypdshield.org/public/SiteFiles/documents/NYPD_Report-Radicalization_in_the_West.pdf; accessed March 13, 2012.

7 James R. Clapper, Director of National Intelligence, "Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community for the House Permanent Select Committee on Intelligence," House of Representatives, Washington, D.C., February 10, 2011, 2.

8 "Al Qaeda Aims at the American Homeland," National Commission on Terrorist Attacks Upon the United States, 2004, 162-190: http://www.9-11commission.gov/report/911Report_Ch5.htm; accessed September 5, 2012.

9 Bill Braniff and Assaf Moghadom, "Towards Global Jihadism: Al-Qaeda's Strategic, Ideological, and Structural Adaptations since 9/11," *Perspectives on Terrorism* vol. 5, no. 2 (2011): http://www.terrorismanalysts.com/pt/index.php/pot/article/view/braniff-towards-global-jihadism/html; accessed March 1, 2012.

10 "Al Qaeda's Top Cyber Terrorist," *Defensetech* (January 26, 2008): http://defensetech.org/2008/01/26/al-qaedas-top-cyber-terrorist/; accessed February 4, 2012.

11 Weimann, *Terror on the Internet,* 115–116.

12 Mark Stout, Jessica M. Huckabey, John R. Schindler, and Jim Lacey, *The Terrorist Perspectives Project: Strategic and Operational Views of Al Qaida and Associated Movement* (Annapolis, Maryland: Naval Institute Press, 2008).

13 Greg Miller, "Bin Laden Document Trove Reveals Strain on al-Qaeda," *The Washington Post,* July 1, 2011: www.washingtonpost.com/national/national-security; accessed March 1, 2012.

14 Abu Musab Al-Suri, "The Jihad Experiences: The Open Fronts and Individual Initiative," *Inspire* (Fall 2010): 17-19; http://www.ahashare.com/torrents-details.php?id=100525; accessed on October 18, 2012.

15 Ibid., 17.

16 Ibid., 32.

17 Author interview with U.S. Department of Defense personnel, who asked to remain anonymous, Washington, D.C., April 2012.

18 "Al-Awlaki in Previously Unreleased Video Message to Muslims in the West: 'You Have Two Choices… Leave and Live Among Muslims, or …Stay Behind and Follow the Example of Nidal Hassan and Others,'" *MEMRI,* December 20, 2011: http://www.memri.org/report/en/0/0/0/0/0/0/5932.htm; accessed December 20, 2011.

19 Adam Lankford, *Human Killing Machines: Systematic Indoctrination in Iran, Nazi Germany, Al Qaeda, and Abu Ghraib* (Lanham, Maryland: Lexington Books, 2009), 69.

20 "The invasion of Facebook: Al Qaeda calls for a 'cyber-jihad' to plan attacks on the West," *Mail Online,* July 13, 2011: http://www.dailymail.co.uk/news/article-2014194/The-invasion-Facebook-Al-Qaeda-calls-cyber-jihad-bid-attack-West.html; accessed December 20, 2011.

21 "Global Trends 2025."

22 Marc Sageman, "The Next Generation of Terrorism," *Foreign Policy* (February 19, 2008): http://www.foreignpolicy.com/articles/2008/02/19/the_next_generation_of_terror; accessed on December 20, 2011.

23 Joseph Lieberman and Susan Collins, "A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack," Special Report for the United States Senate Committee on Homeland Security and Government Affairs, Washington, D.C., February 2011, 19: http://www.scribd.com/doc/48113252/A-Ticking-Time-Bomb-Counterterrorism-Lessons-From-The-U-S-Government-s-Failure-To-Prevent-The-Fort-Hood-Attack; accessed December 20, 2011.

24 Lankford, *Human Killing Machines,* 74–75.

25 "Profile Anwar al-Awlaki," *ADL* (November 2011): http://www.adl.org/main_Terrorism/anwar_al-awlaki.htm; accessed December 20, 2011.

26 Richard Esposito, Rehab El-Buri, and Brian Ross, "From Yemen, Anwar Awlaki Helped Inspire Fort Dix, Toronto Plots," *ABC News,* Nov. 11, 2009: http://abcnews.go.com/Blotter/anwar-awlakis-terrror-ties/story?id=9055322#.UEZuC2ii8zE; accessed September 4, 2012.

27 Clint Watts, "Major Nidal Hasan and the Fort Hood Tragedy: Implications for the U.S. Armed Forces," Foreign Policy Research Institute (June 2011): http://www.fpri.org/enotes/201106.watts.forthood.html#ref1; accessed February 4, 2012.

28 Lieberman and Collins, "A Ticking Time Bomb," 35.

29 Ibid.

30 *ADL,* "Profile Anwar al-Awlaki."

31 David Johnston, and Scott Shane, "U.S. Knew of Suspect's Ties to Radical Cleric," *The New York Times,* November 9, 2009: http://www.nytimes.com/200 9/11/10/us/10inquire.html; accessed December 21, 2011; and Catherine Herridge, "American cleric used more than 60 e-mail accounts to contact followers including Hasan," *Fox News,* June 15, 2012: http://www.foxnews.com/politics/2012/06/14/al-awlaki-used-dozens-email-accounts-to-reach-followers-including-hasan/; accessed June 16, 2012.

32 "Awlaki's latest rant," *Investigative Project on Terrorism,* May 24, 2010: http://www.investigativeproject.org/1971/awlakis-latest-rant; accessed February 4, 2012.

33 Lieberman, and Collins, *A Ticking Time Bomb,* 38–39.

34 Ibid., 39.

35 "United States of America v. Colleen R. LaRose," U.S. District Court for the Eastern District of Pennsylvania, March 4, 2010, 3: http://www.scribd.com/doc/28104790/Indictment-1; accessed September 5, 2012.

36 The information in this paragraph comes from ibid., 3–5, 8.

37 Ibid. 4.

38 Vilks was targeted for death by extremists because of some cartoons he had drawn in 2007 depicting the prophet Mohammed as a dog.

39 "United States of America v. Colleen R. LaRose," 5–6.

40 Ibid., 3.

41 "United States of America v. Colleen R. LaRose, Jamie Paulin Ramirez," Case 2:10-cr-00123-PBT Doc. 31, Superseding Indictment, U.S. District Court for the Eastern District of Pennsylvania, April 1, 2010, 6–7.

42 "United States of America v. Colleen R. LaRose," 8 (see note 35 above).

43 Dale Maryclaire, "MD teenager pleads guilty in terror case in Pa." *Associated Press,* May 4, 2012: http://www.usnews.com/news/us/articles/2012/05/04/md-teenager-pleads-guilty-in-terror-case-in-pa?s_cid=related-links:TOP; accessed June 1, 2012.

44 Lankford, *Human Killing Machines,* 69.

45 "I turned in Colleen 'Jihad Jane' LaRose to the FBI," *The Jawa Report,* March 11, 2010: http://mypetjawa.mu.nu/archives/201487.php; accessed September 9, 2012.

46 Peter Hall, "'Jihad Jane' pleads guilty in terrorism case," *The Morning Call,* February 1, 2011: http://articles.mcall.com/2011-02-01/news/mc-jihad-jane-guilty-plea-20110201_1_jihad-jane-jamie-paulin-ramirez-guilty-plea; accessed September 11, 2012.

47 See "United States of America v. Colleen R. LaRose, Jamie Paulin Ramirez," (see note 41 above).

48 "Police chiefs meet at White House to discuss fight against homegrown terror," *Associated Press*, January 18, 2012: http://www.syracuse.com/news/index.ssf/2012/01/police_chiefs_meet_at_white_ho.html; accessed September 5, 2012.

49 Robert S. Mueller III, speech given at the RSA Cyber Security Conference, San Francisco, California, March 1, 2012: http://www.FBI.gov/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies: accessed September 10, 2012.

50 Maryclaire "Md. teenager pleads guilty."

51 See "Artisanal Intelligence and Information Triage," by Aaron Weisburd, and "Mining Twitter Data from the Arab Spring," by Rob Schroeder, Sean Everton, and Russell Shepherd in this issue, for more about the uses of voluntary information derived from social media.

52 "Mexico: Death by Social Media," *ISN ETH Zurich* (September 28, 2011) http://www.isn.ethz.ch/isn/Security-Watch/Articles/Detail/?lng=en&id=133074; accessed on October 19, 2012.

53 Josh Halliday, "David Cameron considers banning suspected rioters from social media," *The Guardian,* August 11, 2011: http://www.guardian.co.uk/media/2011/aug/11/david-cameron-rioters-social-media?INTCMP=ILCNETTXT3487; accessed February 4, 2012.

54 "United States of America v. Colleen R. LaRose," 3 (see note 35 above).

55 Hall, "'Jihad Jane' pleads guilty."

56 "United States of America v. Tarek Mehanna," Cr. No.09-10017-GAO, Government's Proffer and Memorandum in Support of Detention, U.S. District Court Massachusetts, November 5, 2009, 10; and "Leader of Revolution Muslim Sentenced to 138 Months for Using Internet to Solicit Murder, Encourage Violent Extremism," FBI Press Release, Washington, D.C., June 22, 2012: http://22.FBI/gov/washingtondc/press-release/2012/ Leader of Revolution Muslim Sentenced to 138 months for Using Internet to Solicit Murder, Encourage Violent Extremism/; accessed June 22, 2012.

57 Gary Schmitt, "Terrorism and the First Amendment," *The Weekly Standard,* January 23, 2012: http://www.weeklystandard.com/articles/terrorism-and-first-amendment_616735.html; accessed on September 11, 2012.

58 This was the case of *Schenck v. United States*; see ibid.

59 Sahar F. Aziz, "Homegrown Terrorism" *The American Muslim,* June 12, 2012: http://theamericanmuslim.org/tam.php/features/articles/speech-at-duke-university; accessed September 11, 2012.

60 "National Strategy for Counter-terrorism," The White House, Washington, D.C., June 28, 2011: http://www.whitehouse.gov/sites/default/files/counterterrorism_strategy.pdf; accessed September 5, 2012.

61 "Invisible sieve: Hidden, specially for you," *The Economist,* June 30, 2011: http://www.economist.com/node/18894910; accessed September 5, 2012.

62 Sun Tzu, *The Art of War,* trans. Lionel Giles (New York: Barnes & Noble: 2003), 17.

Artisanal Intelligence and Information Triage

A. Aaron Weisburd

Social media hold out the promise of discovering previously unidentified threats, as well as the peril of information overload. It is possible to utilize social media to find the unknown unknowns, those violent extremists who we can assume exist but whose identities are not currently known to us. It is also possible to triage social media profiles in order to identify those most likely to generate useful investigative leads. As a practitioner of "artisanal intelligence," I collect, analyze, and report for further investigation social media data related to a broad range of violent extremist threats—by hand, not with software. While the work requires a certain attention to detail, the result is a high degree of familiarity with various threat groups. Most importantly, it is a method that works.

Consider the Princess.[1] She presents herself on a prominent social media site as being in her mid-20s, an ethnic Somali who was raised in Nairobi. She very clearly self-identifies with the Somali insurgent group al-Shabaab, describes her favorite music as "Anasheed," and says her favorite movies are "Jihad Movies."[2] This information may be of passing interest but is hardly actionable. However, the Princess also identifies herself as a "Cashier/Hostess" for an airline operating out of a country in the Arabian Peninsula. Even if it turns out the position only gives her access to an airport, and not to any of her employer's aircraft, *that* is a good lead.

Experience suggests that a more targeted approach to social media yields better results more quickly, with fewer false positives and less invasion of privacy.

The collection and analysis of social media profiles raises the specter of data mining, with its attendant controversy, methodological critiques, and negative public perceptions.[3] In addition to the questionable efficacy and the political volatility of wholesale data mining, experience suggests that a more targeted approach to social media yields better results more quickly, with fewer false positives and less invasion of privacy.

This more targeted approach is a variation on snowball sampling, a technique that has long proven useful in the study of deviant behavior in small populations.[4] Start with individuals who can be found on social media, and who are known to be involved in the movement or organization of interest. For example, upon hearing that Samir Khan had left for Yemen (and his ultimately fatal partnership with Anwar al-Awlaki and al Qaeda in the Arabian Peninsula),[5] I began an analysis of the social networks of extremists who support al Qaeda in the United States by examining Samir Khan's profile on a popular social media site. Figure 1 is the initial social network diagram that came out of this investigation.

Typology of Samir Khan's Network

Samir Khan is the red node. Known U.S.-based associates of Khan are blue, and include people such as Proscovia Kampire Nzabanita (node 26), aka Umm Talha, wife of convicted Revolution Muslim activist Zachary Chesser,

aka Abu Talha al-Amriki. Ordinarily the people to the right, with only one connection to the network, would be dropped. Given that their one connection is to Samir Khan, however, I left them in. The remaining nodes, in green, are believed to be outside the United States. The members of Samir Khan's network can be roughly divided by type, and this typology will characterize other networks of violent political actors, not only jihadist networks. Understanding these types can both help to understand the network and guide efforts to combat it.

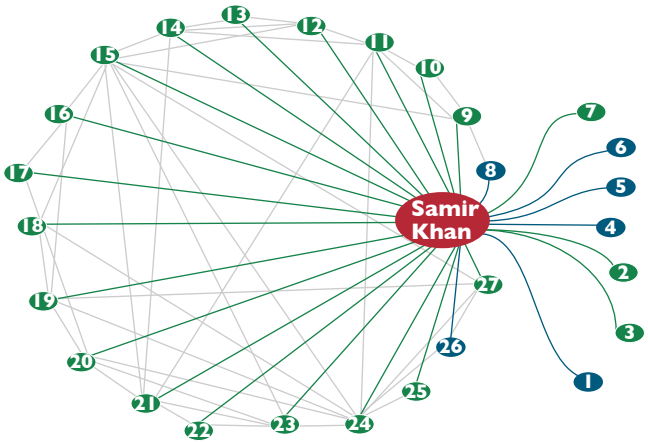


Figure 1. Online social network of Samir Khan aka Abu Risaas

Celebrities

In the case of Samir Khan's network, the celebrity is Moazzam Begg (node 24), a former Guantanamo detainee and self-described human rights activist. Begg has many thousands of friends online, from a broad range of backgrounds and political perspectives. While these virtual friendships likely have little meaning for Begg, for Samir Khan and his friends to be able to reach out and connect to a public figure may have been important to them in the course of their radicalization.

Leaders

Leadership figures are in this case represented by Abdullah el-Faisal (node 11). Based in Jamaica, Sheikh Faisal has been imprisoned, detained, deported, and barred from flying or entering quite a few countries as a result of his frequent calls for violent jihad. Of note here is that while el-Faisal has almost as many connections to other network members as Moazzam Begg, el-Faisal's online friends number a few hundred rather than many thousands, increasing the likelihood that virtual friendship with Sheikh Faisal might be significant.

For Samir Khan and his friends to connect to a public figure may have been important to them in the course of their radicalization.

Mobilizing Structures

These are organizations, typically larger and less radical than the extremist groups that emerge from within them. For Samir Khan's network, the mobilizing structure was a Salafist study group that operates both online and from a suburb of London. The group itself does not espouse violence, and yet Samir and a number of his friends could be found there. This is node 20.

El-Faisal's online friends number a few hundred rather than many thousands, increasing the likelihood that virtual friendship with him might be significant.

Anomalies

Anomalies are individuals who associate with extremists while presenting a reassuringly peaceable face to the world. Here the anomalous individual is node 23. The reasons for this apparent disconnect between how someone presents themselves in public and who they associate with are many. One obvious scenario is that they feel a need to hide how they view events in the world, or what activities they may be involved in.

While it is possible that a person happens to be friends with only like-minded individuals, Samir Khan's network, like all such networks I have examined, was composed of people linked to Khan for a variety of reasons. Some were clearly relatives, or people Khan went to high school with. There

was no need to collect any information about them. Often this type, the people of no interest to us, may be the largest part of the network.

Information Triage

We can assess profiles in order to focus on a smaller pool of individuals more likely to be involved in extremist activity.

Social media profiles alone are unlikely to provide evidence of an imminent terrorist threat. We can assess profiles using an assortment of measures in order to focus further investigative work on a smaller pool of individuals more likely to be involved in extremist activity. The following is not a complete list of the components of a social media profile, but it might be used to start a discussion of these elements and their assessment or measurement.

Connectedness

Human judgment and information triage identified the Princess as a potential threat where data mining and its algorithms may have overlooked her.

While a subject's social network can be quantified, graphed, and analyzed, the analyst also needs to make a *qualitative* assessment of the subject's associates. Success as a terrorist is a function of whom one associates with, and whom or what those associates know. Although violent extremists are often inclined to share their political opinions and concerns, experience says this is not always the case. Taimour al-Abdaly, for instance, launched a complex attack on Christmas shoppers in Stockholm, an attack that fortunately resulted only in his own death when his suicide vest exploded prematurely. Arid Uka opened fire on a U.S. military bus at the Frankfurt airport, killing two service members and wounding two others before being captured. Neither man displayed anything on their social media sites that would suggest they saw themselves as part of the global jihad, let alone that they were preparing to carry out an attack. Both were, however, openly associating with networks of known extremists: al-Abdaly with Samir Khan's network and Uka with radical Salafist/jihadist activists in Germany—the very network that also included the Princess. There is no reason to think the Princess was previously known to any security service, nor might she have been suspected of links to a known network of violent extremists, yet human judgment and information triage identified her as a potential threat where data mining and its algorithms may have overlooked her. The presence or absence of visible support for violent extremism needs to be assessed in light of the quantity and quality of known associates.

Location

More often than not, the reason people are friends on the internet is that they already know each other.

While in theory the internet enables globe-wide communications and the development of long-distance relationships, in practice the most gain is seen in local relationships.[6] Existing social ties are strengthened more than new ties are formed, and real-world proximity appears to be a determining factor in the development of online ties. There are many reasons why people may be friends on the internet, but more often than not, the reason is that they already know each other. Online social networks tend to mirror real-world social networks.[7] One consequence is that even when a subject declines to reveal his or her location, the location of friends can be used to discover where the subject is now, or was in the past. Conversely, if we are looking for unknown agents from a particular country who may be "sleepers" in our country, we could scour social media for any citizen of that country now living here. We could, for example, try to identify every Iranian-American and/or every Iranian national living in the United States who has a social

media account, and then examine each one in the hopes of finding those who self-identify with some element of the Iranian Revolutionary Guard Corps (IRGC). But there is a better way. A more targeted approach would start with individuals in Iran who are known to be involved with the IRGC, and work outwards searching for associates who are now in the United States.

Textual Analysis

Analysis of the text presented on a social media profile can at least place the subject somewhere on the ideological spectrum. The problem with focusing on what people say online is that, while it *might* provide some indication as to their intent, it is unlikely to shed light on their capabilities. In practice, people who become involved in terrorism may actually state their desire to be a terrorist; may say quite a lot without providing any clear expression of terrorist intent; or may say nothing at all.

The political nature of extremists means they will often communicate through imagery what they might not verbalize.

Visual Analysis

Even when subjects self-censor the text they post to their profile, the political nature of extremists means they will often communicate through imagery what they might not verbalize. The Princess of jihad who worked for the airline made no explicit threats on her social media profile, but her profile picture was of a group of women who were members of al-Shabaab, holding AK-47 assault rifles and copies of the Qur'an in the air. In the case of someone linked to the IRGC, imagery associated with recent events may support an assessment that the connection is more, or other than, a reflection of a personal relationship. Many people may support the uprising of Shi'a Muslims in Bahrain, and some may support the Ba'athist regime of Bashar al-Assad of Syria. But someone who simultaneously supports protesters in Bahrain and the slaughter of protesters in Syria is reflecting the current political objectives of the most radical elements in the Islamic Republic of Iran. The visual elements in this case will typically be the prominent display of images of Bahraini protesters being beaten or killed, side by side with Syrian flags and flattering images of Assad.

The Princess's profile picture was of a group of women who were members of al-Shabaab, holding AK-47 assault rifles.

Link Analysis

The hyperlink is at the heart of the Web, and extremists can be counted upon to link to both what they like and what they hate. It is common, for example, that jihadists will list the forum they spend most of their time on as "their" website, even though they are not involved in the site's management. In this regard, as in many others, violent extremists are not significantly different from the rest of us.

Focus on the Network

The objective of this analytical triage is to seek out both exculpatory *and* inculpatory information. It seeks to identify patterns and assess the degree to which these elements all point in a similar direction, and to identify anomalies or breaks in the pattern. It makes note of people who present as non-extremist, or who reveal little or nothing about themselves, but who are found to be associated with extremists all the same. It also notes those who, while linked in some way to known extremists, are not themselves a threat. As one pursues first the friends, and then the friends of friends, of people already involved in terrorism, this triage technique helps maintain the focus of

Analytical triage seeks to identify patterns, and anomalies or breaks in the pattern.

the investigation. The end result is a network of weakly tied but like-minded people. Given that this network was mapped out based on the social media profiles of bona fide terrorists, it is likely that from within it individuals and strongly-tied groups will emerge and try to involve themselves in terrorism.

While we can identify the components of such networks, and map out their interrelationships and locations, there are too many other factors involved for us to be able to predict who the next terrorist will be. Unable to know exactly who will emerge from the network and strike, we therefore need to undermine the network of extremists as a whole. The strength of weak ties is in their ability to move information from ideology to actionable intelligence.[8] The weakness of weak ties lies in their vulnerability to infiltration. A strongly tied group may constitute an operational unit, but in becoming so it invariably breaks the weak ties to the community it emerged from. Successful counterterrorism exacerbates this process, causing the network itself to wither.

An artisanal approach to social media analysis places individuals in a network that may be observed for evidence of impending violence, or undermined and dismantled.

An artisanal approach to social media analysis bypasses the various problems inherent in a big-data approach, and bears fruit more rapidly by developing a context in which to assess an individual as a potential target for investigation or recruitment. It also places individuals in a network that may be observed for evidence of impending violence; infiltrated and exploited; or undermined and dismantled. ❖

ABOUT THE AUTHOR

A. Aaron Weisburd is a node in a global ad hoc network of counterterrorism and intelligence professionals. He is the founder of watchdog group Internet Haganah, and a recipient of an FBI Director's Commendation. In addition to research and operational activities, Weisburd instructs on the behavioral aspects of extremist use of the internet to elements of the intelligence community. He has a Bachelor of Science degree in Information Systems Management, and an MA in Criminology.

NOTES

1 The individual's real name is not known to me, and particular details of her employment and location have been redacted. Her profile is no longer publicly available.

2 *Anasheed*, commonly referred to as *nasheeds*, are *a cappella* songs of jihad and martyrdom favored by jihadists.

3 Bruce Schneier, "Data Mining for Terrorists," Schneier on Security website, March 9, 2006: http://www.schneier.com/blog/archives/2006/03/data_mining_for.html; accessed June 12, 2012.

4 Patrick Biernacki and Dan Waldorf, "Snowball Sampling: Problems and Techniques of Chain Referral Sampling," *Sociological Methods Research* vol. 10, no. 2 (November 1981): 141–163.

5 At the time, Khan was a central figure in a loosely knit confederation of activists who operated under the rubric Revolution Muslim, and made vigorous use of social media. Investigations and arrests across the United States following Khan's departure led to the dissolution of Revolution Muslim. The remnants now operate in several states under the banner of "Sharia4–," e.g., Sharia4Kentucky, Shariah4NewMexico, etc. Khan himself was killed along with his mentor al-Awlaki in a September 2011 U.S. drone strike in Yemen.

6 Jacob Goldenberg and Moshe Levy, "Distance is Not Dead: Social Interaction and Geographical Distance in the Internet Era," Hebrew University, Jerusalem, 2009.

7 A. Aaron Weisburd, "Jihadist Use of the Internet and Implications for Counter-Terrorism," in *Terrorism and Political Islam: Origins, Ideologies, and Methods* 3rd edition (Washington, D.C.: FBI Counter-Terrorism Division, forthcoming).

8 Mark S. Granovetter, "The Strength of Weak Ties," *The American Journal of Sociology* vol. 78, no. 6 (May 1973): 1360–1380; http://www.jstor.org/stable/2776392; accessed September 24, 2012.

Another Tool in the Influencer's Toolbox: A Case Study

LTC Jamie Efaw and
SFC Christopher Heidger

Much of the recent writing within military circles surrounding social media has centered on what can be learned from "bad guys'" use of social media sites, or the role social media played (and play) in events such as the Arab Spring and Haiti disaster relief. However, from an information operations perspective, the "golden ticket" in our operations is the ability to influence behavior and attitudes. The questions we address in this article are: "Can an information operator use social media to influence audiences, and if so, how?" Attitudes and behaviors cannot be changed overnight; doing so requires exposure to a persuasive message repeatedly over an extended period of time—a task social networking tools are perfectly designed to accomplish. One should not, however, view social media as the single best way to exert influence, but rather, see online networking as another tool in the communicator's toolbox that enhances larger influence campaigns. In this paper, we will share some of our experiences from putting theory into practice, our phased approach, some lessons learned, and recommendations for getting started in your own organization.

Getting Started and Building the Target Audience

In the winter of 2008, I (Jamie Efaw) published a paper in *IO Sphere* titled "Social Networking Services: The New Influence Frontier."[1] I had been thinking about these ideas for quite a while, and at the time, the paper was largely theoretical, focused on the "whys" and "hows" of social networking platforms and their application toward counterterrorism efforts. In 2009, my new NCOIC (non-commissioned officer in charge) and co-author Chris Heidger and I arrived at the United States European Command (EUCOM) in Stuttgart, Germany at the same time. We found we had inherited an eight-year old regional Web news and information initiative called the Southeast European Times or SETimes, which had an accompanying eight-month old Facebook companion presence.[2] We both saw this situation as a perfect opportunity to leverage social media and apply the theoretical framework I'd developed in my paper to a real-world situation. As a starting point, we identified four goals for having a social media presence:

1. Take advantage of the existing social media community to introduce and draw them to SETimes.com.
2. Provide an additional forum that exposes our target audience to our themes and messages.
3. Provide a convenient place for the SETimes community to discuss regional topics of interest and interact in an environment where they are comfortable and familiar.
4. Establish a communication platform we could use during a crisis, humanitarian assistance, or disaster relief operation.

In an effort to minimize the risk of our enterprise failing to catch hold or committing a public relations foul, while simultaneously maximizing learning and flexibility, our social media expansion efforts took a very deliberate five-phase approach, which is laid out in detail below:

Phase 0: Establish a Facebook Presence
Phase I: Research and Improvement
Phase II: Focused Advertising
Phase III: Increased User Interaction
Phase IV: Shift Focus onto Established Social Networks

Figure 1 summarizes the SETimes' Facebook fan growth by phase from March 2010–January 2011.

Figure 1. Fans by Phase

Phase 0: Establish a Facebook Presence (March 2009–February 2010)

Phase 0 started prior to our arrival at EUCOM, and consisted of creating a Facebook page for SETimes, adding a RSS feed from the webpage to the Facebook page, and putting a Facebook link at the top of the SETimes homepage.

During our first six months on the job we made no changes; noting that readership ("fans") and interaction (fans "liking" a post or making a comment) on the Facebook page did not increase over that time, however, we realized that in preparation for Phase 1 we needed to benchmark the current initiative. We do not see ourselves as competitors with the Department of State (DoS), but we used official DoS Facebook pages to serve as a yardstick for our site, since they have a comparable presence around the globe. A year after its creation, the SETimes' Facebook page gained an average of less than one fan per day, for a total of 306, and ranked in the bottom 15% when compared to similar DoS pages. Our audience was largely U.S.-based, and there were more English-speaking fans than all other languages combined (see Figure 2).

Fans by...

Country		Language	
44	Turkey	110	English (US)
40	United States	35	English (UK)
38	Macedonia	32	Turkish
34	Serbia	22	Macedonian
23	Greece	22	Albanian
19	Bulgaria	18	Greek
13	Germany	13	Bulgarian

Figure 2. Phase 0 Results

Phase 1: Research and Improvement (March–June 2010)

In March of 2010, we began our research and improvement phase, which started with the question: "What is the dominant social media platform in Southeast Europe?" A good surface-level tool for this research is Alexa.com,

which identifies the most popular sites in a targeted region. With Facebook rated as the frontrunner (which will not always be the case), we then evaluated successful Facebook presences similar to SETimes, such as U.S. government pages and those of other regional news organizations, to get an idea of what they were doing right.

Based on our findings, we took a few minor steps to improve our Facebook page. First, we opted to manually post content in lieu of RSS feeds, which for a social platform we decided were too impersonal, mechanical, and annoying. Second, we added new features such as photo albums and a discussion tab with conversation topics, in an effort to promote a social atmosphere that was more in line with Facebook's interactive environment.

Third, we published a story on SETimes.com about Facebook in Southeast Europe, which also encouraged readers to join our Facebook page (see Figure 3).[3]

Figure 3. SETimes Article about Facebook in Southeast Europe

Lastly, in May 2010, we provided basic Facebook instruction at our annual SETimes writers' conference, and encouraged our contributors to become "fans" and interact on our page.

Despite focusing on Southeast European audiences, Figure 4 shows that we still had a very large U.S.-based audience and an even larger ratio of English-speaking fans than we had at the end of phase 0. While we understood that we still had a long way to go, we were encouraged that our new fans per day had doubled, indicating an increase in the page's appeal.

Fans by...

	Country		Language
109	Macedonia	222	English (US)
68	United States	83	English (UK)
65	Serbia	52	Macedonian
49	Turkey	35	Turkish
36	Greece	23	Bulgarian
31	Bulgaria	23	Albanian
21	Albania	20	Serbian

Figure 4. Phase I Results

Phase II: Focused Advertising (July–October 2010)

Phase II, which started in July 2010, is where our project started gaining significant momentum. The first noteworthy change was the introduction of advertising to Facebook users in SETimes' twelve core countries (see Figure 5).

We chose a rate of $5/day, which made Facebook advertising a cost-effective as well as user-friendly tool. Getting started requires only a credit card, some small thumbnail images, an introductory sentence, and an intended audience. Once established, advertising costs are set through a daily geographically-dependent bidding process that ranges from less than U.S. 10 cents to more than $1.00 per ad click.

Figure 5. Facebook Advertisement

Demographic data are the greatest advantage that Facebook provides a planner. These data include age, sex, country, city, marital status, education level, and even interests, all of which are gathered as users establish and update their profiles. These are the data that focus advertising and provide excellent, real-time, demographically separated measures of performance. Although we have used Facebook ads only to increase the number of fans on our Facebook page, these ads can satisfy other objectives such as advertising an event, directing people to a website, or simply getting a target audience to download an application.

While advertising was an important step, we also added some additional features to enhance the users' overall experience during this phase. First, we added the "Like" button to individual articles on SETimes (Figure 6).

When SETimes readers who are also Facebook users click that they "like" something, the action is indicated on their Facebook pages, and shows up on their friends' pages, along with a link to the "liked" content. Second, we added prompts to our Facebook posts in order to encourage interaction. Typically, we would link to a recently published SETimes article and then post a related question or comment. For example, we posted an article about the start of the Croatian president's second year in office, along with the following question: "Josipovic started his 2nd year as President of Croatia. How do you think he did in his 1st year? Share your thoughts."

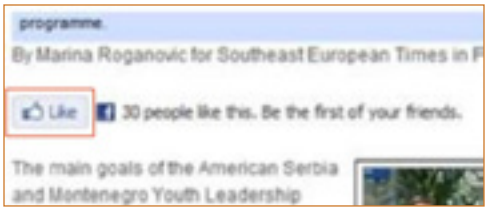


Figure 6. Facebook Like Button on SETimes Article

Fans by...

Country		Language	
1,092	Bosnia	613	English (US)
766	Macedonia	591	Turkish
587	Turkey	575	Croatian
564	Bulgaria	513	Bulgarian
402	Albania	501	Macedonian
298	Serbia	432	Bosnian
166	Romania	429	Albanian

Figure 7. Phase II Results

Throughout Phase II we saw a sharp increase in the growth of fans from our target region (see Figure 7). Due to focused advertising, we now gained a daily average of 35 new fans, 99% of whom were from our target audience. As also depicted in Figure 7, U.S. readers dropped off the readership chart, and English language usage as a proportion diminished.

After four months of posting content to our page once every five days, we realized that Facebook users tended to visit pages other than their own only on the day new content appeared on their wall. The "if you build it, they will come" model, in other words, does not apply in social media. In the world of "new media," consumers no longer actively seek out or pull information; instead, they subscribe to topics of interests and have the information fed to them. In Phase III we adjusted our approach to fit this model.

Phase III: Increased User Interaction (November–December 2010)

Phase III began in November 2010. The goals in this phase were to implement lessons learned from Phases I and II, increase fan interaction, and test some of the more specific advertising techniques.

Observations from previous phases revealed that the timing of Facebook posts affected interaction levels. For two weeks we logged hourly Facebook traffic from 0600–2300. This showed us that peak traffic for our target audience occurred between 0900–1000 and 1700–1830. Based on these findings, we began posting to Facebook twice a day, during each of these periods. We reasoned that this technique would optimize views and reader interaction while minimizing the risk of becoming a nuisance. To further encourage interaction, we started producing exclusive content for our Facebook page such as video essays, and we introduced a weekly "hook," such as a survey question, a "complete the sentence" statement, a "fan of the month" post, or a quote of the week.

Other early engagement efforts taught us several useful lessons. First, heavier content, such as the re-posting of a SETimes feature article, performed better in the morning, while lighter posts received better traction in the evening. These lighter interactive evening posts (often devoid of core themes and messages) were essential to keep the page in line with the social nature of Facebook. Finally, we found that simple encouragement such as, "Thanks for your comment, we value your insight," or "Interesting photo, can you tell us more about it?" proved invaluable as a method to keep fans engaged and let them know we were paying attention to them.

Lighter interactive posts were essential to keep the page in line with the social nature of Facebook.

From our advertising campaign, we observed another interesting trend. During Phases I and II, audiences from our lower-priority countries (based on existing national and command guidance) quickly used the majority of our daily advertising budget by clicking on our ads more frequently than higher priority-country audiences. To rectify this, we divided our increased advertising budget of $10/day in accordance with SETimes' established three-tier priority system. Tier 1 (highest priority) audiences received $5/day, while Tier 2 audiences received $3/day, and Tier 3 received only $2/day.

Lastly, due to the steadily increasing number of fans and interaction, we anticipated a need for a Facebook Terms of Service statement that would provide general information about SETimes, and codify acceptable and unacceptable member conduct.[4] Our Terms of Service proved useful later when dealing with inappropriate reader comments.

The return on investment dropped off very rapidly as daily advertising increased.

Until this phase, EUCOM command policy was to block all social media sites, so all these Facebook activities had to be managed from non-government computers. After months of dialogue with communicators across the staff, Admiral James Stavridis, the EUCOM commander, published a comprehensive social media policy granting command access to social media sites. In addition to making our Facebook campaign far more convenient to maintain, workplace access enabled us to determine peak traffic times, increase posting frequency, and continuously monitor our Facebook page—maximizing the efficiency of a real-time communication platform.

During Phase III, English-language users continued to drop off, while fans who used SETimes target-country languages continued to increase at a rapid pace (see Figure 8). While our advertising doubled, there was, surprisingly, an increase of only four more fans per day compared to our daily average in Phase II—a trend that has not changed. In fact, the return on investment dropped off very rapidly as daily advertising levels increased. For example, if a Facebook page gets twenty new fans per day for $10, it does not necessarily mean that investing $50 per day will bring in one hundred fans.

Fans by...

Country		Language	
1,648	Bosnia	1,087	Turkish
1,296	Macedonia	882	Croatian
1,080	Turkey	873	English (US)
802	Bulgaria	843	Macedonian
670	Albania	789	Albanian
475	Serbia	734	Bulgarian
245	Romania	633	Bosnian

Figure 8. Phase III Results

Phase IV: Shift Focus to Established Social Networks (January 2011–ongoing)

At the beginning of 2011, we initiated Phase IV, which involved increasing the advertising budget to $100/day and focusing our efforts on increasing four measurable Facebook page user actions: 1) page visits; 2) page "likes"; 3) fan interaction; and 4) referrals to SETimes.com (i.e., reads of SETimes.com

content). In order to promote an increase in the above actions, we recognized the need to leverage the power of social comparison that is inherent in the Facebook platform. Social Comparison Theory postulates that people evaluate their opinions and actions based on their peer group. When one's own opinions or beliefs are in contradiction to the comparison group, there is a tendency to either change one's own opinions or attempt to convince others that your beliefs are correct in order to re-establish group cohesion. Typically, when encountering content on a traditional website, the reader does not know what other friends have read the same article, who liked it, or what they thought about the content they read. Social media platforms, however, are by definition built on social connections, and thus are formatted to allow the reader or fan to engage in social comparison.[5]

We recognized the need to leverage the power of social comparison that is inherent in the Facebook platform.

In previous phases, we advertised to all Facebook users within SETimes' established target audience (over 30 million Facebook users, and growing). This all-encompassing approach established nodes in existing social networks in every corner of our focus countries; however, the majority of our fans were not connected in any meaningful way. To rectify this, we expanded established nodes (existing SETimes Facebook fans) and began advertising only to their Facebook "friends." Currently, a tag at the bottom of every SETimes Facebook ad might say something like, "Joe Smith likes this." As more "friends" within a circle "liked" the ad, it might say "Joe Smith and 5 of your friends like this"—increasing the power of social comparison with every new fan. These newly formed pockets of SETimes fans not only increased the effectiveness of our advertising, but also increased the potential of both online and offline conversations with friends surrounding the content of the Facebook posts. Figure 9 illustrates that previously observed trends continued, with a marked increase in the growth of fans from the target audience.

Fans by...

Country		Language	
3,208	Bosnia	2,201	Turkish
2,174	Turkey	1,848	Croatian
2,061	Macedonia	1,380	Albanian
1,052	Bulgaria	1,268	Bosnian
987	Albania	1,252	Macedonian
800	Serbia	1,242	English (US)
539	Romania	986	Serbian

Figure 9. Phase IV Results

A tag might say, "Joe Smith and 5 of your friends like this."

Once a social media user joins the site or page, social comparison continues to have an influence. When readers interact with content on Facebook, they immediately know how many other total users have "liked" the content, but more importantly, they know how many and which of their own friends (their comparison group) "liked" it (they do not see which of their friends do *not* like an article). Additionally, they can see any comments made about the content and make comments of their own in real-time. Whether the reader tries to change the opinion of friends or changes his or her own to match theirs, either outcome could be useful for the influencer if properly managed.

Lessons Learned and Difficulties

Over the last eighteen months we have identified several advantages, difficulties, and lessons learned while using Facebook, many of which already

have been discussed above. The following section offers nine broad topics we consider principles for getting started.

1. Research and listen.

Where are the conversations among your target population taking place? On what platforms? What are the advantages and disadvantages of the different social media platforms for reaching your audience? Answer these basic questions before launching a social media effort.

Where are the conversations among your target population taking place?

2. Have a plan, but experiment. Be deliberate, expect failures, and be flexible.

Before starting, have a plan and be deliberate in your method, but also leave room to experiment. The same principles that worked for us will not necessarily work for everyone. As you experiment, start small, expect failures, and be prepared to make adjustments. This will ensure you have the flexibility to make required changes while minimizing the negative effects of failures and growing pains.

3. Provide fans with experiences. Make interaction easy. But do not saturate!

We found that to get fans involved with our content, we needed to provide online "experiences" that invited them to interact. An activity that encourages engagement, participation, and conversation, yet remains easy and quick for the reader, is ideal. In the social media world, more is not always better. A user typically is not going to join in an in-depth erudite dialogue, but most will likely vote in a poll, complete a sentence, or "like" a quote. Too much information (i.e., too many posts) hinders your effort. At best you run the risk of being ignored, and at worst, annoying the individuals you want to influence.

To get fans involved with our content, we needed to provide online "experiences."

4. Benchmark your efforts and progress.

Benchmarks help you see progress toward your goal. If you do not establish a reliable baseline from the outset of your activity, it is impossible to show how far you've come at subsequent benchmarks, or at the end of your effort. In March of 2010, SETimes' Facebook page had 306 fans and was ranked in the bottom 15% when compared to similar DoS Facebook pages. Less than a year later, we had over 17,300 fans and it was ranked in the top 6% compared to similar pages. Other aspects can be benchmarked as well. Our Phase IV measurable actions provide a good starting point: 1) page visits; 2) page "likes;" 3) fan interaction; and 4) referrals to an external website (i.e., reads).

This was a welcome indication that our page's fans were taking "ownership."

5. Add a Terms of Service policy.

A Terms of Service policy outlines acceptable and unacceptable user behavior on the site. By stating policies upfront, you have de facto authority to delete inappropriate posts and ban disruptive users from the site. On several occasions, this policy enabled our fans to regulate each other and make sure that

fellow fans abided by the spirit and the letter of the policy. This was also a welcome indication to us that our page's fans were taking "ownership" of the page and regarded it as theirs to monitor.

6. Educate the organization.

Find senior leaders in your organization who "get it" and who will act as advocates.

Much can be written about educating your organization. Be aware that some individuals will never understand, or desire to understand, what you're doing and how you're doing it. However, there are others who are willing to learn. Help these people set up an account and show them how social media work, then encourage them to experiment from their personal computers. Ensure you are an available resource to answer questions, but be careful to do it without making anyone feel stupid. Locate and mobilize key personnel in your organization. If possible, find senior leaders in your organization who "get it" and who will act as advocates when needed. Similar to the "start small and expect failures" discussion above, do not make unreasonable or unrealistic promises to your bosses. We kept our developmental phases pretty quiet until we were able to demonstrate some solid metrics. Furthermore, because we started small, there was no need or requirement to report setbacks.

7. Real-time interactions.

Real-time interactions are both Facebook's greatest advantage and its greatest challenge. The challenge lies in the fact that these interactions require constant monitoring in order to respond appropriately. Social media encourage conversation, which assumes timely responses. Failure in this area alienates fans and discourages future participation. A unique advantage of real-time interaction on Facebook, however, is that every time a fan comments on a discussion thread, the comment is sent out to everyone who has previously taken part in that thread, as well as all of the friends of the commenters. This feature continues to draw people back into the dialogue.

8. Translation and the use of an official language.

It is important to be aware that social media tools are ideally suited for campaigns focused on a single audience with a common language and problem set. Our audience, in contrast, spans twelve countries and ten spoken languages. Regardless of language(s) used, there are two translation management issues: 1) fan comments submitted in a language other than the page's official language(s); and 2) the general difficulty of maintaining oversight on a second-language (for the manager) fan page. For the first issue, on-call translators are required; this, however, can take time. While waiting for full translation, we have found the Google Translate and Live Translate applications to be useful for an immediate base-line understanding. To maintain oversight of a second-language Facebook page requires a minimum of one full-time, native speaking-level employee.

9. Leadership's lack of understanding.

There are many people who view Facebook as an invasive site that reveals far too much information about its users. Although mistrust was a more

common problem three to four years ago, it still is an identifiable generational issue and a recognizable hindrance to social media initiatives within an organization.[6] While many senior-level leaders still do not fully understand social media, most at least understand its importance. Basic understanding and acceptance is all one needs to move forward.

Social media tools are ideally suited for a single audience with a common language and problem set.

Summary and Conclusion

When we look back at the original four goals we set for getting involved in Facebook, we are gratified to see that we achieved each of them.

Leverage the existing social media community to introduce and draw them to SETimes.com.

By the middle of 2012, we will have accumulated nearly 400,000 SETimes Facebook fans. Nearly all of these members of our target audience are individuals who had never heard of SETimes.com, nor been exposed to the website's themes and messages prior to the launch of our Facebook page. Additionally, in 2011, we recorded over 120,000 visits to SETimes.com from readers who came directly from our Facebook page; in other words, they were on the SETimes' Facebook page, clicked on a hyperlinked headline that interested them, and then read the full article on SETimes.com.

By the middle of 2012, we will have nearly 400,000 SETimes Facebook fans.

Provide an additional forum that exposes our target audience to our themes and messages.

If a fan never clicked on one of the Facebook-posted links taking them to the SETimes.com content, they would still be exposed, three times a day, seven days a week, to its themes and messages via postings and interactive features on the SETimes' Facebook wall.

Provide a convenient place for the SETimes community to discuss regional topics of interest, and interact in an environment where they are comfortable and familiar.

We assessed our achievement of this goal by asking our fans, in a Facebook poll on January 23, 2012, what they liked most about the SETimes' Facebook page. The great majority (72%; 1720 of 2390) of respondents acknowledged that the feature they appreciated most was that the page provided "a forum for an exchange of opinions and dialogues with others in the region" (see Figure 10).

Figure 10. Poll Question: What do you like about SETimes?

Establish a trusted communication platform that can be leveraged during a crisis, humanitarian assistance, or disaster relief operation.

This function was validated on several different occasions. A good example occurred in September 2011 during a flare-up of tensions at the

Appropriately designed content prompts the target audience to share the message with others.

Serbia-Kosovo border. Utilizing the SETimes' Facebook page, we were able, first, to inform the target audience of the actual situation on the ground, thereby discrediting rumors and disinformation. As a result of this effort, combined with our Google advertising, SETimes' coverage of the event was the #1 overall search result in Google news. Second, by utilizing the Facebook polling option, we were able to quickly gauge sentiment among the target audience, and provide that information to commanders and decision-makers. The fact that our audience trusted the integrity of our information was key to our success on these occasions.

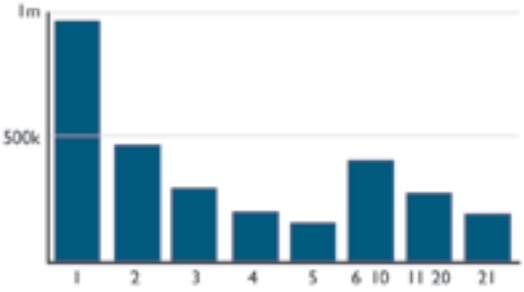


Figure 11. Total Views x Frequencies of Views from 1–7 January 2012

The question posed in the first paragraph of this article, you may recall, was: "Can an information operator use social media to exert influence and if so, how?" After two and a half years of daily experience with the SETimes platform, it is evident to us that Facebook and other social media sites are valid influence tools. First, social media allow an influencer to expose the target audience multiple times to the crafted content. As one can observe in Figure 11, over one million Facebook users were exposed to (had read or viewed) SETimes Facebook content more than five times in a seven-day period.

One reason this statistic is encouraging is that users not only saw SETimes content several times, but they chose to have our content delivered to them or they actively sought it out.

Figure 12. Sharing with Others Poll Question

Second, we discovered that appropriately designed content prompts the target audience to share the message with others. Participation in a dialogue or a conversation about a topic encourages an individual to think deeply about the topic. To see how often this was occurring, in December 2011, we asked the poll question: "How often have you had a discussion with someone about a topic/issue you read about on SETimes?" (see Figure 12). Eighty-nine percent (2099/2365) of respondents acknowledged that they had had conversations about SETimes' content either daily or weekly.

An impressive 93 percent of fans who responded acknowledged they had been affected by our product.

These results confirmed that our target audience is thoughtfully considering the material presented by SETimes. The results also indicate that the online target audience is expanding the reach of the SETimes' message by having conversations with their off-line, real-world social network, thus expanding SETimes' sphere of influence.

Lastly, while we have illustrated that well-designed social media offer the tools to deliver a message and encourage dialogue, measuring influence (effectiveness) still remains difficult. Besides observing a change in the behavior of members, self-reporting (polling) is often the only method for

determining effectiveness. To this end, we asked our Facebook fans: "Has anything you have read on SETimes.com caused you to think differently about an issue?" (see Figure 13). Although people are often reluctant to admit they have been influenced, an impressive 93 percent (2693/2916) of SETimes' Facebook fans who responded acknowledged they had been affected by our product.

Figure 13. Influence Indicator Poll Question

As one can gather from our experiences, social media initiatives require constant attention; the good news is that they require only limited personnel and funding to have an impact. No matter how enticing this high return on investment may sound, however, it is essential to keep in mind that Facebook, or any social media platform, is not a stand-alone tool. In fact, it will always work best in concert with traditional communication tools supporting a larger effort, event, or cause, such as, in our case, the SETimes news and information website. Used properly, this rapidly evolving capability is proving itself a tremendous addition to the communication toolbox. ❖

ABOUT THE AUTHORS

LTC Jamie Efaw serves as the Fort Story ASA Commander and Deputy Commander for Joint Expeditionary Base Little Creek-Fort Story in Virginia Beach. He was commissioned into the Corp of Engineers by the United States Military Academy at West Point in 1993 with a degree in Psychology. After receiving his Master's Degree in Social Psychology, LTC Efaw went on to teach in the Behavioral Science and Leadership Department at West Point, and branch transferred to Psychological Operations. After serving in the 4th Psychological Operations Group at Fort Bragg, North Carolina, LTC Efaw served as the United States European Command's Military Information Support Operation officer.

From 2009–2012, SFC Chris Heidger was the Senior Enlisted Military Information Support Advisor at the U.S. European Command in Stuttgart, Germany, where he and LTC Efaw managed Southeast European Times. A nine-year PSYOPS veteran, Chris has spent five years overseas with tours in Iraq, Afghanistan, Africa, and, most recently, Europe. Chris earned a BA in Political Science from American Military University, and recently finished the coursework for a Master's of Professional Studies in Strategic Public Relations at George Washington University.

NOTES

1 James M. Efaw, "Social Networking Services: The New Influence Frontier," *IO Sphere* (Winter 2008): 4-7; http://www.au.af.mil/info-ops/iosphere/09winter/iosphere_win09_efaw.pdf; accessed on September 27, 2012.

2 The Southeast European Times website is a central source of news and information about Southeastern Europe, offered in ten languages: Albanian, Bosnian, Bulgarian, Croatian, English, Greek, Macedonian, Romanian, Serbian, and Turkish.

3 Natasa Radic, "Facebook has a friend in Southeast Europe," *SETimes.com*, March 8, 2010; http://www.setimes.com/cocoon/setimes/xhtml/en_GB/features/setimes/articles/2010/03/08/reportage-01; accessed on October 1, 2012.

4 View the SETimes' Facebook terms of usage at http://www.facebook.com/SETimes#!/SETimes?v=info

5 Leon Festinger, "A theory of social comparison processes," *Human Relations* vol. 7, no. 2 (1954): 117-140.

6 Meagan Johnson and Larry Johnson, *Generations, Inc.: From Boomers to Linksters—Managing the Friction Between Generations at Work* (New York: AMACOM, 2010).

Mining Twitter Data from the Arab Spring

Rob Schroeder, Sean Everton, and Russell Shepherd

In this article we draw on social movement theory to help explain how the use of social media, in particular Twitter feeds, may have played a role in the emergence of the Egyptian Arab Spring revolution. More precisely, we suggest that activists' uses of Twitter may have facilitated the framing of grievances in ways that resonated with their target audience. In an examination of a subgroup of primarily Arab-speaking Twitter users, we found that not only did traditional media and activists appear to play a large role in framing the events in Egypt, but so did a fake Twitter account impersonating Egyptian President Hosni Mubarak. This account's tweets attracted a large audience, and may have helped disseminate a portrayal of Mubarak as a corrupt leader who should resign, both of which were goals of the Egyptian revolution.

While grievances are certainly necessary for sustained collective action, they alone are not enough.

People often assume that all that is needed for a social movement, an insurgency, or other form of collective action to emerge is for enough individuals to become sufficiently angry about a particular social condition. While grievances are certainly necessary for sustained collective action, they alone are not enough. As social movement scholars have noted, in most societies there are plenty of individuals who are angry with the status quo, but few become activists or engage in contentious politics.[1] For a social movement or insurgency to gain traction, other factors need to fall into place.[2] In particular, not only do individuals need to harbor grievances of some kind, but: 1) the grievances have to be framed in such a way that people recognize they share them with others, and believe that together they can do something about them (i.e., *insurgent consciousness*); 2) the aggrieved population needs to have access to and be able to appropriate sufficient resources so they do not have to rely on external support (i.e., *sufficient mobilizing resources*); and 3) they need to perceive (whether correctly or incorrectly) that the broader socio-political environment is either vulnerable to collective action, or that it represents a significant threat to the group's interests or survival (i.e., *expanding opportunities or increased threats*). In isolation, none of these factors is sufficient to generate and sustain an insurgency. When they converge and interact, however, collective action becomes a possibility although, we should emphasize, not a certainty.

Grievances have to be framed in such a way that people believe they can do something about them.

In this paper we explore how the use of social media, in particular Twitter feeds, may have played a key role during the Egyptian Arab Spring of 2011. We focus on Twitter's role in the framing of grievances, but along the way we also note how it may have been used to attack some of the Egyptian government's vulnerabilities and as a communication network among activists. We begin with an overview of social movement theory, and explain the process of framing.[3] We next consider how Twitter functions, and how activists and others used it during the Egyptian Arab Spring. We then examine Twitter data gleaned from the Arab Spring and what it possibly tells

us about its role in the framing process. We conclude with a few thoughts on the role that social media could play in facilitating the development of social movements, insurgencies, and other forms of collective action.

Social Movement Theory

The question of why populations that had appeared quiescent will suddenly rise up against their leaders in protest, riot, and full-blown revolt has intrigued and confounded rulers and researchers alike since long before Niccolò Machiavelli wrote his treatises on benevolent tyranny in the early 16th century. Social movement theory suggests three interrelated causes, each of which is insufficient by itself, but which in combination can fan smoldering resentment into mass revolt: a perceived threat and the opportunity to act, access to resources, and a unifying message. As this section notes, access to new social media may be helping bring these three factors together more quickly and efficiently than ever.

Access to new social media may be helping bring the three factors for revolt together more quickly and efficiently than ever.

Opportunity and Threat

Disaffected populations generally face numerous obstacles in attempting to mobilize, while opportunities to overcome those obstacles are rare and tend to fluctuate over time. Doug McAdam has suggested that the socio-political environment becomes vulnerable to collective action in three different and interrelated ways: 1) political instability; 2) an enhanced political position for the aggrieved population; and 3) ideological openness.[4] Political instability occurs when elite control of the political status quo is weakened by events such as economic crises, armed conflict, large-scale natural disaster, and so on. An increase in the political position (i.e., power) of aggrieved populations can result from broad social changes that occur over extended periods. Finally, social change can lead the wider population to tolerate alternative and sometimes even subversive ideas championed by the aggrieved population.[5]

Social change can lead the wider population to tolerate alternative and even subversive ideas championed by the aggrieved population.

More recently, scholars have noted that expanding political opportunities are more likely to be a factor in democratic societies, while in autocratic societies it is often substantial threats to a group's interests or survival that matter.[6] Drawing on Daniel Kahneman and Amos Tversky's observation that individuals are especially adverse to loss,[7] many scholars argue that groups will risk far more to preserve what they have than on what they might gain.[8]

Whether it is the expansion of opportunities or an increase in threats, neither will lead to collective action unless groups perceive them as such.[9] An established political order can be reeling, but if no group notices this, it is unlikely that any will take advantage of the situation to bring about change. Similarly, if a group does not recognize that its interests or its very existence are threatened, then it may not act in time to avert its own destruction.

Many scholars argue that groups will risk far more to preserve what they have than on what they might gain.

Mobilizing Resources

Favorable and/or threatening changes in the political environment only increase the probability that nascent insurgencies will mobilize. Whether

they actually do also depends on whether they have access to and are able to appropriate the resources necessary to mobilize and sustain their cause.[10] Another enabling factor is access to a network of pre-existing organizations (formal and informal) that can provide the institutional foundation on which to build a movement. These also help link people to activists, form and sustain the moral outrage that feeds insurgencies, and facilitate mobilization and deployment for insurgent activities.[11] Along with fostering a sense of solidarity, networks can also contribute other key resources, such as the ability to monitor participants (the latter is especially important when defection poses serious security issues to insurgencies), leaders, and communications.[12] One other resource that incipient movements often need is "free spaces" (e.g., coffee houses, religious institutions, neighborhood bars, ungoverned spaces) that are beyond the surveillance and control of authorities, and where groups can frame the narratives (e.g., "We shall overcome.") that accompany successful mobilization efforts.[13]

Favorable or threatening changes in the political environment only increase the probability that nascent insurgencies will mobilize.

Insurgent Consciousness

As noted at the outset, discontent by itself does not produce social movements and insurgencies; there needs to be what Christian Smith calls "the development of an insurgent consciousness," which occurs when the social situation is framed in such a way that people feel compelled to mobilize.[14] A budding social movement, however, cannot expect that all potential members will be able to grasp fully the group's ideology. Thus, movement elites generally frame their group's core message in generalized ideological snippets, much like bumper stickers,[15] that are easily communicated to their target audience.[16] Given the 140-character limitation of Twitter messages (see discussion below), Twitter appears to be an ideal tool for broadcasting ideological snippets and framing grievances for delivery to a social movement's target audience.

Twitter appears to be an ideal tool for broadcasting ideological snippets and framing grievances for a social movement's target audience.

Twitter and the Arab Spring

Twitter is a micro-blogging tool that enables users to send and receive text-based, publicly available posts of up to 140 characters known as "tweets," which can contain messages, images, and links to internet sites. In addition to broadcasting tweets to others, users can choose to follow other users, so that they are constantly updated with new information when those they follow "tweet." They can also describe the topic of their tweet by placing a "#" before a word. If they want to pass on another person's message, they can "retweet" that message to their own followers or other users. Retweets contain the original message along with the original tweeter's name, but they can be passed on to other users with additional content if the retweeting user so desires.

During the 2011 Egyptian protests, many users posted messages, images, and links to other web pages about what was occurring through Twitter. These helped to create a global conversation about events in Egypt. Some struck a chord and were retweeted thousands of times, while others did not reach large audiences.

During the 2011 Egyptian protests, Twitter users helped to create a global conversation about events in Egypt.

In order to understand which users were significant conduits of information during this time, we analyzed over one million tweets about Egypt from two days, January 28 and February 4, 2011, that we downloaded using a research tool on the Twitter API (Application Programming Interface).[17] The Twitter API offers various tools that allow other programs to receive data from and send data to Twitter. We used a program to request from Twitter all publicly available data it could find in regards to users tweeting about Egypt; the program then organized and stored that data. The key aspects of the data that were stored included the user's Twitter name, the content of each tweet, and a description of each user (from the user's public profile). Using these data, we generated a user-by-user network where a direct tie was drawn between two users if one of the users sent a message to the other, or a user retweeted the message of another. In the case of the latter, we drew a tie from the author of the original message to the user who "retweeted" the message. In the end, our user-by-user network included 196,670 users with 526,976 ties between them. Figure 1 presents a visualization of the network.

We analyzed over one million tweets about Egypt from two days, January 28 and February 4, 2011.

The size of the network we traced makes the application of some standard social network-analysis algorithms difficult to implement (because many are computer intensive) and the results of others potentially open to misinterpretation. For example, in terms of degree centrality, which is a count of each user's ties, the celebrity singer Katy Perry ranks in the top ten in our database. While it is possible that Perry's tweets helped frame the grievances of Egyptians, it is unlikely that they did.

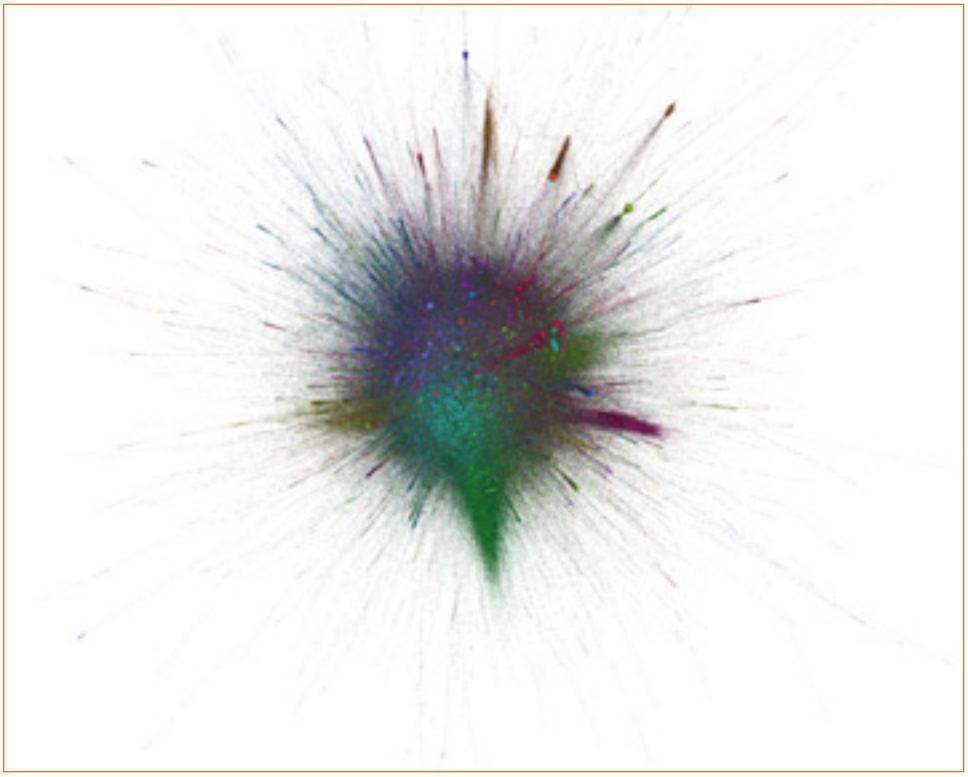


Figure 1: Visualization of Entire Twitter Network on Egypt (nodes colored by community)[18]

In order to filter out noise such as this, we used an algorithm developed by a group of statisticians to identify distinct clusters (or communities) within the network.[19] This algorithm assigns users to different clusters based on a partition of users that yields the highest modularity score. Modularity is a measure of fit that compares the ties within and across clusters to what one would expect in a random graph of the same size and having the same number of ties.[20] Formally, it is the fraction of internal ties in each cluster less the expected fraction if they were distributed at random across the network. The higher the net fraction, the better the fit. The algorithm identified a number of distinct clusters in our data. Here, we focus on the cluster that included Al Arabiya and Al-Jazeera Arabic, because most of the users speak Arabic and are probably geographically close to the events in Egypt.

Analysis and Findings

The Al Arabiya and Al-Jazeera Arabic cluster is a far smaller subset (8,460 users, 14,391 ties—see Figure 2) of our entire database, and thus more amenable to the use of most social network analysis algorithms. We began by estimating "betweenness centrality,"[21] which measures the extent to which each actor in a network lies on the shortest paths (i.e., geodesics) connecting all pairs of actors in the network. It is often used as a measure of brokerage; here we use it to identify users who are potential conduits of information in the network. In Figure 2, the size of each node reflects that user's betweenness centrality score.

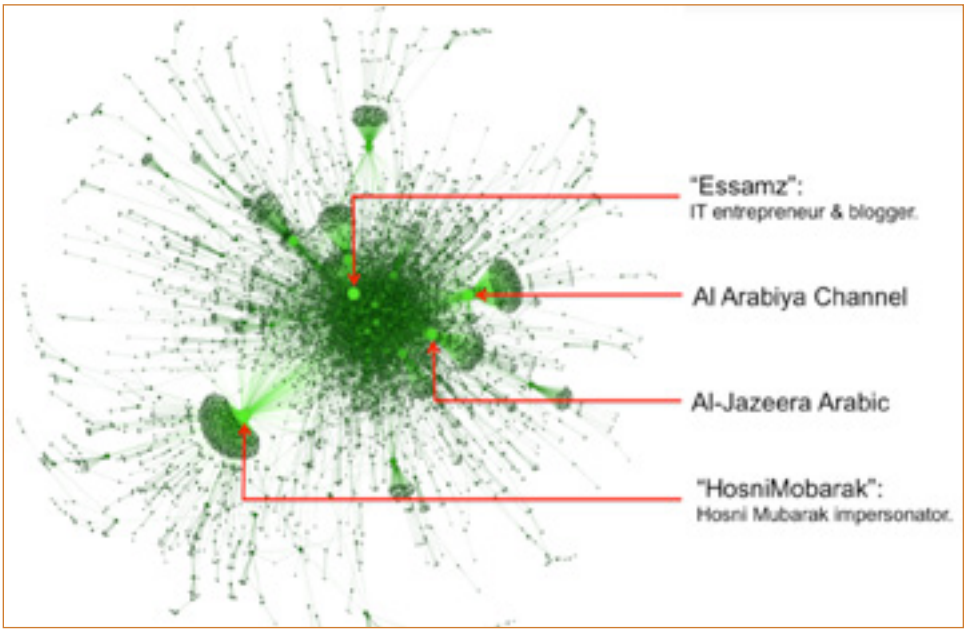


Figure 2: Network Cluster Containing Al Arabiya and Al-Jazeera Arabic (nodes sized by betweenness)

Al Arabiya and Al-Jazeera Arabic rank third and fourth respectively in terms of betweenness centrality. This is unsurprising since both are traditional "go to" sources of news and information, and we would expect them to be conduits of information about the Egyptian revolution. The Saudi user "Essamz" ranks second highest in betweenness centrality. This also was not a surprise

to us because he (Essam Al-Zamil) portrays himself as an activist who uses Twitter to start open conversations. Al-Zamil in fact recently created a new Twitter venture called Radwitter, which is a radio show that broadcasts about Saudi events and issues brought up on Twitter. The program's goal is to facilitate discussion on the radio between activists and others who use Twitter.[22]

Interestingly, the user who ranks highest in terms of betweenness centrality is a parody account, "HosniMobarak."

Interestingly, the user who ranks highest in terms of betweenness centrality is a parody account ("HosniMobarak") where the user poses as Hosni Mubarak, the president of Egypt who was overthrown in the course of the revolution. According to the user's profile, he (or she) is located somewhere near or in Cairo, and the majority of the account's tweets during the two days we studied were in English. A few examples appear below:

> "I'll be on TV soon to announce the new changes. First thing will be the replacement of the current people of #Egypt."
>
> "I survived 83 years, 6 assassination attempts, 2 major wars, and 2 major revolutions. What makes you think I won't survive this? #Egypt"
>
> "Fool you once, shame on me. Fool you for 30 years, shame on you, your children, and your grandchildren. #Egypt"
>
> "#Irony: Using the Internet, that I blocked earlier, I hereby announce my resignation as "President" of #Egypt."
>
> "Like I said in my TV statement, I will deliver the reforms I promised, I just didn't say when. #Egypt"
>
> "They say that what goes up must come down. But then again, I've defied every law there is. #Egypt"

It is interesting that while most of the fake Hosni Mubarak's tweets were in English, the clustering algorithm we used still assigned him to a predominantly Arab-speaking cluster, indicating that in spite of the potential language barrier, his tweets received substantial airplay within a largely Arabic-speaking community. This suggests that his parody of the Egyptian president may have helped frame Mubarak as a corrupt and incompetent leader. This portrayal, conveyed with sharp humor, spread widely across the "Twitterverse," with individuals from the Arabic-speaking community, the Netherlands, and elsewhere around the world retweeting his messages. The active spread of this negative imaging from individual to individual fits with social movement theory's requirement for social consciousness to embrace common grievances. Of course, it is possible that many Egyptians already perceived their president in this way. If that was the case, then the fake account's tweets would likely have reinforced the public's perception of Mubarak, and were taking advantage of an existing political opportunity by attacking one of the regime's vulnerabilities. In addition, when individuals posted tweets about the real Hosni Mubarak, they often included a link to the parody account, thereby directing even more attention to it. In either case, theory suggests that the widespread sharing of a common viewpoint

The widespread sharing of a common viewpoint may have contributed to people's sense that the moment for change had come.

among a largely educated, middle-class population with access to resources may have contributed to people's sense that the moment for change (opportunity) had come.

To be clear, we are not suggesting that the fake Hosni Mubarak caused the events in Egypt to occur. As our earlier discussion of social movement theory should have made clear, a number of factors need to fall into place in order for a group of aggrieved individuals to mobilize, and even then there is no guarantee that they will. Nevertheless, our analysis does suggest that the parody's tweets *may* have played a role in influencing the public's perception of the president and thus given a boost to the movement. Without additional data we cannot prove that this in fact happened. The results of our analysis, however, are consistent with such a deduction.

Conclusion

In this article, we have examined how social movements may be able to use Twitter to frame grievances in ways that resonate with their target audience. We saw how during the Egyptian Revolution, thousands of people used Twitter to discuss the events that were taking place. Using a clustering algorithm, we identified and focused on a particular cluster of Twitter users, the one that included the news organizations Al Jazeera Arabic and Al Arabiya. Using betweenness centrality to identify potentially influential nodes within this cluster, we discovered that a Hosni Mubarak parody account was quite central, and speculated that its tweets may have been influential in the framing of grievances during the Egyptian Revolution. By portraying the real Hosni Mubarak as corrupt and unwilling to give up power, it may have helped create or further a negative public perception of the Egyptian president.

A fake Henry Kissinger account had to remove all of its tweets because it was deemed an impersonation rather than a parody account.

This is not the only example of fake accounts that apparently tried to influence unfolding events during the Egyptian Revolution or elsewhere in the world. For example, during the Egyptian Revolution a fake Henry Kissinger (the former U.S. secretary of state) tweeted regularly, and attempted to portray Kissinger as a war criminal (e.g., his profile location displayed as "Anywhere but the Hague," a reference to the location of the International Criminal Court and the International Court of Justice). Interestingly, this fake account often retweeted messages from the fake "HosniMobarak" account. Another example is the fake FARC (Revolutionary Armed Forces of Colombia) account ("FARC"). The FARC is a Colombian guerilla movement that was originally founded in 1964 to protect rural peasants against the harsh policies of large landowners, and provide the poor with education in exchange for food and supplies. It has since devolved into an international organization that now controls Colombia's drug trade and often wreaks violence against the peasants it claims to protect.[23] While the FARC has its own Twitter account ("FARC_Colombia"), the fake FARC account tweets about government victories against the FARC and atrocities committed by the FARC.

We should note that Twitter has a policy regarding parody accounts and impersonation accounts. It allows parody accounts as long as they make clear that they are a parody. Impersonation accounts, however, are not allowed. In fact, the "Henry_Kissinger" account discussed above has had to remove all of its tweets because it was deemed an impersonation rather than a parody account.[24] While this policy will place limits on the long-term viability of impersonation accounts, they will most likely continue to spring up, and along with parody accounts, will help frame how others perceive various events around the world. Moreover, social movements, insurgencies, and other forms of collective action will almost certainly continue to use Twitter as a means of communicating with the faithful. ❖

ABOUT THE AUTHORS

Rob Schroeder is a Research Associate in the Department of Defense Analysis (DA) CORE Lab at the U.S. Naval Postgraduate School (NPS). He earned a M.A. in International Policy with a focus on Conflict Resolution at the Monterey Institute of International Studies (MIIS, 2011) and a B.A. in International Relations at Boston University (2008). He is researching how to use open source information to understand and map the Syrian opposition, and how different types of external support to insurgencies relate to length of conflicts and the ways they end. Rob also helped train members of the Joint Special Operations Task Force—Philippines to collect and analyze relational information using social network analysis.

Sean Everton is an Assistant Professor in the DA Dept. and the co-Director of the NPS CORE Lab. Prior to joining NPS in 2007 he was an adjunct professor at both Santa Clara University and Stanford University. Professor Everton earned his M.A. and Ph.D. in Sociology at Stanford University (2007). He has published articles in the areas of social network analysis, sociology of religion, economic sociology, and political sociology. He recently published a monograph for Cambridge University Press on using social network analysis for the crafting of strategies for the disruption of dark (i.e., criminal and terrorist) networks.

Cairo, Egypt–February 9, 2011: A Muslim demonstrator in crowded Tahrir Square, holding her national flag and gesturing with a victory symbol.

Russell Shepherd graduated with a M.A. degree in International Policy Studies from MIIS (2012), where he focused on economic and public policy analysis. His research used open-source technology to create innovative approaches to modern data analysis, including social networks, statistics and economics. While working at the NPS CORE Lab (2011–2012), Russ developed methods for the analysis of unconventional data, including generating social networks from Twitter.

PHOTO CREDIT

Photo page 63 via iStockPhoto.com

NOTES

1 John D. McCarthy and Mayer N. Zald, "Resource Mobilization and Social Movements: A Partial Theory," *American Journal of Sociology* 82 (1977): 1212–41.

2 Doug McAdam, Sidney Tarrow, and Charles Tilly, *Dynamics of Contention* (New York and Cambridge: Cambridge University Press, 2001).

3 David A. Snow and Robert D. Benford, "Ideology, Frame Resonance, and Participant Mobilization," *International Social Movement Research* 1 (1988): 197–217.

4 Doug McAdam, *Political Process and the Development of Black Insurgency,* 1930–1970 (Chicago: University of Chicago Press, 1982).

5 Christian S. Smith, *The Emergence of Liberation Theology: Radical Religion and Social Movement Theory* (Chicago: University of Chicago Press, 1991), 59.

6 David A. Snow, Daniel M. Cress, Liam Downey, and Andrew W. Jones, "Disrupting the 'Quotidian:' Reconceptualizing the Relationship between Breakdown and the Emergence of Collective Action," *Mobilization: An International Journal* 3 (1998): 1–22.

7 See Daniel Kahneman and Amos Tversky, "Prospect Theory: An Analysis of Decision under Risk," *Econometrica* 47 (1979): 263–91; and Amos Tversky and Daniel Kahneman, "The Framing of Decisions and the Psychology of Choice," *Science* 211 (1981): 453–58.

8 Jack A. Goldstone and Charles Tilly, "Threat (and Opportunity): Popular Action and State Response in the Dynamics of Contentious Action," in *Silence and Voice in the Study of Contentious Politics,* Ronald R. Aminzade, Jack A. Goldstone, Doug McAdam, Elizabeth J. Perry, William H. Sewell, Jr., Sidnew Tarrow, and Charles Tilly, eds. (New York and Cambridge: Cambridge University Press, 2001), 179–94.

9 McAdam, Tarrow, and Tilly, *Dynamics of Contention.*

10 McCarthy and Zald, "Resource Mobilization and Social Movements:" 1212–41.

11 Christian S. Smith, *Resisting Reagan: The U.S. Central America Peace Movement* (Chicago: University of Chicago Press, 1996).

12 See McAdam, *Political Process;* and Smith, *The Emergence of Liberation Theology.* Social media such as Facebook and Twitter can obviously facilitate communication between activists. This aspect of social media's role in helping give birth to various forms of collective action, however, is not the focus of this paper.

13 Doug McAdam and David A. Snow, "Facilitative Spaces and Contexts," in *Readings on Social Movements: Origins, Dynamics, and Outcomes,* Doug McAdam and David A. Snow, eds. (New York and Oxford: Oxford University Press, 2010), 187–88.

14 Smith, *The Emergence of Liberation Theology,* 61.

15 Glenn E. Robinson, "Hamas as Social Movement," in *Islamic Activism: A Social Movement Theory Approach,* Quintan Wiktorowicz, ed. (Bloomington: Indiana University Press, 2004), 129.

16 David A. Snow, E. Burke Rochford, Jr., Steven K. Worden, and Robert D. Benford, "Frame Alignment Processes, Micromobilization, and Movement Participation," *American Sociological Review* 51 (1986): 464–81.

17 For information about Twitter API, see https://dev.twitter.com/

18 The green community at the bottom of the graph is the one we focus on. Another community of interest centered around a language is the purplish-pink community that extends from the center of the graph to the 4 o'clock position. This one is largely made up of Chinese speakers with some individuals speaking about a possible "jade" revolution. This does not, however, mean that each community is based around languages. Other communities tend to be focused around certain news organizations, such as CNN, or those following a celebrity.

19 Vincent D. Blondel, Jean-Loup Guillaume, Renaud Lambiotte, and Etienne Lefebvre, "Fast Unfolding of Communities in Large Networks," *Journal of Statistical Mechanics* P10008 (2008).

20 Mark E. J. Newman, "Modularity and Community Structure in Networks," *Proceedings of the National Academy of Sciences* 103 (2006): 8577–82.

21 Linton C. Freeman, "Centrality in Social Networks I: Conceptual Clarification," *Social Networks* 1 (1979): 215–39.

22 Mariam Abdallah, "Saudi Arabia: Boycotting Twitter to Save It," *Al Akhbar English,* January 31, 2012: http://english.al-akhbar.com/content/saudi-arabia-boycotting-twitter-save-it; accessed on October 5, 2012.

23 Claire Metelits, *Inside Insurgency: Violence, Civilians, and Revolutionary Group Behavior* (New York and London: New York University Press, 2010).

24 For more information on Twitter's parody and impersonation policies see: https://support.twitter.com/articles/106373#

ETHICS AND INSIGHTS

Should Military Members Really Call Themselves "Professionals"?

Bradley Jay Strawser

Dr. Bradley J. Strawser is an assistant professor in the Defense Analysis Department at the Naval Postgraduate School. He is also a Research Associate at Oxford University's Institute for Ethics, Law, and Armed Conflict. Strawser is a philosopher who specializes in moral and political philosophy, with an emphasis on applied ethics. He has published on issues in just war theory, military ethics, and the ethics of newly emerging military technology, as well as in subfields such as metaphysics, human rights, and ancient philosophy. His work has appeared in the journals *Analysis, Philosophia, Journal of Military Ethics, Journal of Human Rights, Epoché,* and others. Strawser's newest book is *Killing By Remote Control: The Ethics of an Unmanned Military* (forthcoming from Oxford University Press).

In today's military, the word "professional" has become a catch-all for anything good or worthy of praise. You'll hear it used by a commander who, one suspects, is simply reaching for something—anything—positive to say. "Very professionally handled," the commander may intone with the utmost gravity, or, "Tom is a real professional in everything he does," for want of a more artful compliment. Conversely, "unprofessional" has become the go-to term for any negative appraisal of, well, just about anything for any reason at all.

That's not to say the term is meaningless. The idea of being a "professional" certainly gets at something in the collective consciousness of the military. But if, like me, you've noticed that it has become overused to the point of banality, you probably aren't interested in thinking seriously about the term. If you are in the military, the concept may have had little direct impact on how you think of your military duties and service, despite the fact that most training or education you'll undertake throughout your career will be what we call "professional military education."

Humor me then on a modest proposal. I think a better understanding of what the concept "professional" and its derivatives actually mean could affect our thinking on military service in a real and substantive way. Moreover, I think that the notion of being a professional—when properly understood—can provide some level of normative guidance on the ethical challenges facing military operators.

Classically, there were only three vocations that were considered professions. I used to tell my students this when I taught at the Air Force Academy, and then have the cadets guess what the three occupations were. For some reason they would at first invariably guess "blacksmith" or some other antiquated vocation. But eventually they'd hit upon the three "original" professions: medicine, law, and clergy. It's worth exploring why this was the



Society trusts each sub-group [of professionals] to act on behalf of everyone else in the society.

case. Why were only doctors, lawyers, and "men of the cloth" traditionally called professionals?

To begin, notice that each of these activities does something very important for an individual's well-being. Doctors are entrusted by society to take care of physical health; lawyers are entrusted to uphold rights and legal standing; priests, rabbis, or pastors, and the like are entrusted with our spiritual well-being. Imagine you are an average person living several hundred years ago. You have a tremendous self-interest in assuring that these three critical aspects of life—your physical, legal, and spiritual health—are in good condition. Yet, the average human being, then or now, has no time to master the requisite specialized knowledge and skills that are needed to properly care for each of these aspects of life.

We see the idea of a profession born out of this societal need for some members to take on these particular, specialized roles that are necessary for the well-being of all. Society trusts each of these sub-groups to be the guardian of its particular domain of expertise, and then to act on behalf of everyone else in the society. With that societal trust comes a heightened respect and dignity for these classic professions. But each also comes with special obligations and correlating special permissions.

For each of the three classic professions, there is a special kind of bargain between its members and the society they serve.

For example, since I am not a medical doctor, I am not entrusted by society to prescribe medications. That's a unique permission that we give to doctors who have met specified standards of training and expertise. Similarly, lawyers are trusted with the special permission of lawyer-client privilege. They can also argue in a court of law before a judge "past the bar"—that is, in the front portion of a courtroom past the small fence or piece of furniture (the bar) that traditionally divides the court between its working areas and areas where the public can sit and observe. (Hence, the term still used for admission into the profession of law is to "pass the bar.") Clergy are given special permission to perform a wide variety of important rites according to their faith, that an average citizen generally cannot, such as marriages and funerals.

Each bargain comes with special privileges that only the members of the given profession enjoy, and each also brings distinct duties that hold only for them.

These permissions are granted to each profession for the purpose of carrying out that specific area of human activity with which that given profession is entrusted. But with each of these permissions also come distinct duties and obligations. If a doctor fails to meet the standard expected of her in carrying out her professional duties, she can be held liable for malpractice. If a lawyer is negligent in his counsel, he can be disbarred and himself prosecuted. Clergy take on a wide range of special restrictions depending on the particulars of each religion, but they are almost always expected to put the well-being of their lay adherents ahead of their own. So we see that for each of the three classic professions, there is a special kind of bargain between its members and the society they serve. Each bargain comes with these special privileges that only the members of the given profession enjoy, and each also brings with it distinct duties that hold only for them.

As we look closer, we discover other similar characteristics between the three classic professions. For example, notice that each is, in some sense, internally

self-regulated. They have their own unique ethical codes and sets of rules that society trusts them to enforce upon themselves. Doctors in some countries, including the United States, are "board certified" by an association made up of other doctors. Clergy members are typically ordained in some manner by their respective faith. U.S. lawyers, as noted, must pass a bar examination, which is administered by other attorneys in the state where they wish to practice. In all cases, this certification can be revoked by their peers within the profession. We also expect the three professions to continually improve the knowledge of their particular profession and to use it responsibly for the benefit of the society. We all rightly presume, for example, that our family physician is at least reasonably up-to-date on the latest medical studies as they relate to our care.

Most vocations, while valuable in their own right, don't carry these distinctive features of the three classic professions.

These days it seems we wish to call just about every occupation imaginable a "profession." But I think that's ungrounded. Most vocations, while valuable to society in their own right, don't carry these distinctive features of the three classic professions. That is, while being a baker or a carpenter or a used car salesman may be indispensable to the functioning of society, none of those jobs should properly be characterized as a profession according to the classic criteria we just reviewed. So while it would perhaps not sound odd to our modern ears, it would technically be incorrect to call someone a "professional baker" or a "professional salesman."

Does the term "military professional" fit with the concept's classic meaning?

So, then, let's ask ourselves: should serving in the military be considered a profession? By listening to the language of the modern military, one would certainly think that is the default view. But is it an accurate claim based on what military servicemen and women actually do? Does the term "military professional" have the right fit with the concept's classic meaning the way it does for a doctor?

There are many ways that military service appears to have the right fit. The military is entrusted by society to carry out a particular highly skilled and specialized activity for the benefit of all: national defense. Just as with the three classic professions, the job the military is entrusted with generates its own peculiar duties and special permissions. The most striking special permission is obvious: the permission to kill in war. The unique duties military members take on are also clear: to bear the largest burden of risk in war, and to accept a wide-range of restrictions placed on their personal liberty when they join.

The most striking special permission is obvious: the permission to kill in war.

Looking closer, we see other parallels (and some points of disconnect) with the three original professions. Just like doctors, lawyers, and clergy, the U.S. military, for example, has its own set of unique rules (the Uniform Code of Military Justice) and its own ethical code. The UCMJ is internally enforced by the military hierarchy but, interestingly, it is imposed upon the military by an external body: the U.S. Congress. Notice as well that the military has its own unique process for bringing members into its body, just like the classic three professions do. Commissioning (or enlistment) has a parallel with ordination or passing the bar. But, again, it is the U.S. Congress that holds the final decision over who is commissioned as a military officer. So there are points of similarity with the classic professions, but also points of

dissimilarity in which the military's autonomy over its own regulation is restricted.

The final commonality I noted was an expectation that members continually improve the knowledge of their particular profession and to use it responsibly for the benefit of the society. This brings us back to that tired military idiom: professional military education. It seems there is good reason to interpret this as consistent with the demand on the classic professions for on-going competence in their given field. And, moreover, I think today there is an expectation from society that its military will be as up-to-date as possible not only on the knowledge of how best to wage war, but also how to conduct it justly.

The society one serves is counting on its military personnel to be competent, skilled experts carrying out their end of the noble bargain.

Do all of these points of commonality with the classic professions mean that military service is properly a "profession"? I'll leave that to the reader to decide. But if we take seriously the notion of military professionalism, then we would do right to remember what that actually means. "Professionalism" is not some catch-all synonym for praise or a job well done, as it is so often used in the military today. Rather, to be a professional means to take the trust that society has given you for this very particular (yet critically important) vocation, and give that trust the proper weight and respect it deserves.

If we do this, we might just return to things like "professional military education" with a new appreciation for the fact that the society one serves is counting on its military personnel to be competent, skilled experts carrying out their end of the noble bargain that being a member of a profession entails. Part of that bargain means our military members bear exceptional hardships. But it also includes being granted the unique and unsettling permission to kill and destroy. That is no small thing with which to be trusted. Society today respects military professionals to a striking degree; one that at times borders on reverence. With that honor comes the responsibility for military members to properly value the trust society gives to the profession of arms. ❖

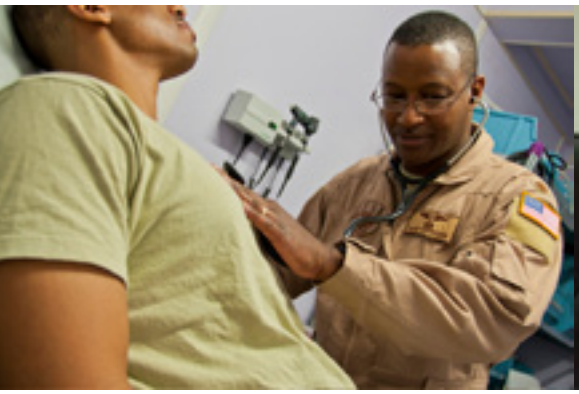


PHOTO CREDITS

Photos page 65:
Mary Edwards Walker, Civil War Surgeon: Wikimedia Commons
Judge Learned Hand: Wikimedia Commons
Soldiers receiving communion, Iwo Jima battlefield: from http://forums.catholic.com/index.php

Photos page 68 courtesy DefenseImagery.mil:
U.S. Air Force Maj. David Simmons: by SSgt David Carbajal
U.S. Army Capt. Velma C. Gay: by Sgt. A. M. LaVey
U.S. Navy Lt. Cmdr. Joselito Tiongson: by MCSN Benjamin T. Liston

STATE OF THE ART

Contemplating the Future of Social Media, Dark Networks, and Counterinsurgency[1]

> "We use Facebook to schedule the protests, Twitter to coordinate, and YouTube to tell the world."
>
> —Cairo activist, Egyptian Arab Spring[2]

Sean Everton

Sean Everton is an assistant professor in the DA Dept. and the co-Director of the NPS CORE Lab. Prior to joining NPS in 2007 he was an adjunct professor at both Santa Clara University and Stanford University. Professor Everton earned his M.A. and Ph.D. in Sociology at Stanford University (2007). He has published articles in the areas of social network analysis, sociology of religion, economic sociology, and political sociology. He recently published a monograph for Cambridge University Press on using social network analysis for the crafting of strategies for the disruption of dark (i.e., criminal and terrorist) networks.

The spectacular growth in social media over the last decade, led by Facebook, YouTube, and Twitter, and their potential usefulness have not been lost on insurgents and others using what we call dark networks.[3] Over the last few years, such groups have increasingly turned to social media to communicate with and motivate their followers and supporters. For example, the use of social media by Egyptian insurgents during the Arab Spring is well documented,[4] and other dark networks, such as the FARC (*Fuerzas Armadas Revolucionarias de Colombia*—Revolutionary Armed Forces of Colombia) and the Free Syrian Army (FSA), have attempted to exploit their functionality as well. At the same time, authorities have been seeking ways to capture the information that dark networks share through social media. To date their efforts have yielded minimal returns, but there is good reason to believe that this could change in the future.

Speculating about the future is almost always a tenuous endeavor, and contemplating the interplay of social media, dark networks, and counterinsurgents is no exception. I'll limit myself here to discussing three of many possible scenarios: the use of social media by insurgents to communicate and disseminate information; social media's value for authorities who track and disrupt dark networks; and the ways both insurgents and authorities use social media to frame and reframe discontent.

Communication and Diffusion

Scholars have long highlighted the importance that communication networks play in the mobilization of insurgencies and other social movements. "For example, the communication channels that were long embedded in African American churches and historically black colleges were employed to help coordinate communications in the black civil rights movement of the 1950s and '60s;" more recently scholars have noted that the internet, satellite broadcasting, and cell phone technologies "have helped to mobilize and sustain various uprisings, protests, and insurgencies since the 1990s."[5] Thus, it is not surprising that contemporary insurgencies, such as the FARC and the FSA, have turned to social media to help mobilize members and supporters. The FARC and some individual members have their own websites, while the group's commander, Timoleon Jimenez, a relative newcomer to the world of social media, recently issued a series of tweets attacking the Colombian government, less than two weeks before peace talks were to begin.[6] Similarly,

Authorities have been seeking ways to capture the information that dark networks share through social media.

Contemporary insurgencies such as the FARC and the FSA have turned to social media to help mobilize members and supporters.

the FSA operates two Facebook accounts on which it posts information concerning its military operations; it also uses Twitter and YouTube to communicate with and disseminate videos to its followers.[7]

How insurgents and other groups use these media in the future will hinge, of course, on how social media evolve. It is a reasonable assumption that the platforms will only get faster, easier, and less expensive, making them even more attractive to insurgents. We can also be reasonably confident that insurgencies and other dark networks will attempt to remain on or close to the technological cutting edge.

Insurgencies and other dark networks will attempt to remain on or close to the technological cutting edge.

That said, given how easy it is to track the posts, tweets, and video uploads of insurgent groups, it is surprising that they are so open about what they are doing and with whom they communicate. Moreover, one would expect that counterinsurgents would attempt to use such information to their advantage. For example, it seems logical that the Assad regime would regularly monitor the FSA's online activity, since the information contained therein might offer them a strategic advantage in their efforts to better counter the FSA's operations. It appears, however, that either the regime is unaware of the FSA's use of social media, or it lacks the technological sophistication needed for monitoring the FSA's activities in a timely manner. What this suggests is that until counterinsurgents develop the tools necessary to track how insurgents use social media, dark networks will continue to have the advantage.

Tracking and Disrupting

That the Assad regime appears unable to track the FSA's on-line activities does not mean that others cannot or are not doing so, however. For example, the New York Police Department (NYPD) became aware that newer gangs are using social media to boast of their exploits and taunt rival gangs, and therefore have been able to monitor the gangs' activities. "By capitalizing on the irresistible urge of these suspects to brag about their murderous exploits on Facebook, detectives used social media to draw a virtual map of their criminal activity over the last three years."[8] In fact, by monitoring the conversations and trash talk between two rival gangs on Facebook, the NYPD was able to arrest 49 gang members on homicide and other criminal charges.[9]

By tracking social media posts and uploads, authorities can identify key members through analytical methods such as social network analysis.

What this suggests is that by tracking social media posts and uploads, not only can authorities be alerted to significant events and uncover self-identified perpetrators, but they can also identify key members through the use of analytical methods such as social network analysis.[10] For example, as my colleagues and I discuss in our article "Mining Twitter Data from the Arab Spring" (in this issue), network data culled from publicly available micro-blogging tools such as Twitter can help analysts and operators identify individuals worth tracking, and ideally improve knowledge of the network. This kind of knowledge is essential to improve the crafting of disruption strategies over time:

> In the successful strikes against al Qaeda affiliates in Singapore, Morocco, and Saharan Africa, the key doctrinal approach was to

> wait and watch for a considerable period, then to swarm the targets simultaneously at their moment of maximum illumination. This strategic patience grew out of the understanding that striking at nodes as they were identified might actually reduce the ability to detect and track other cells in the networks in question. It is a curious fact [that]… the more that is disrupted, the less may be known.[11]

Using social media to track and ultimately disrupt dark networks will, of course, turn on the ability to scrape social media data in near real-time. While techniques for doing so are in their infancy, analysts, for example, recently developed a program (NodeXL) designed for pulling network data from social media sites such as Facebook, Twitter, Wikipedia, YouTube, and so on.[12] More recently, Russell Shepherd and Patrick Dudas helped the Defense Analysis Department's CORE Lab at the Naval Postgraduate School create a tool for gathering publicly available Twitter posts in near real-time. The Lab recently used this tool to track the social media use of the FARC, the FSA, the Taliban, the Omari Battalion, and others dark networks, as well as anti-regime protesters in Egypt.

Using social media to track and ultimately disrupt dark networks will turn on the ability to scrape social media data in near real-time.

It is hard to imagine that insurgencies and other clandestine actors would continue to use social media if counterinsurgent analysts become increasingly adept at tracking their movements and mapping their interactions. We can be sure, however, that the social media market will continue to evolve, and that current major players such as Facebook, Twitter, and YouTube may give way in turn to new sites that are easier and more convenient to use. It is also highly likely that insurgencies will turn to these newer media as counterinsurgents get a handle on older ones. Thus, it is possible to imagine a scenario where insurgents, or at least the successful ones, will stay one step ahead in the exploitation of social media functionality.

Framing and Reframing

Scholars have noted that discontent by itself does not produce insurgencies. To take action, people must believe that change is not only necessary but also possible. They need to be able to perceive, interpret, and explain a situation in such a way that compels them to mobilize.[13] This is most effectively accomplished by budding insurgencies when they frame their core message in ideological snippets that resonate with their target audience.[14] As we describe in our article on Egypt's Arab Spring, it is easy to see the potential role that tools such as Twitter, with its 140-character limit on tweets, can play in the framing of grievances by insurgencies. A report published by the Project on Information Technology and Political Islam at the University of Washington concluded that social media played a role in framing the Arab Spring in three major ways: by shaping political debates, by spreading democratic ideas, and by facilitating online "revolutionary conversations" that often preceded major events on the ground.[15]

It is easy to see the potential role that Twitter can play in the framing of grievances.

What has received less attention is the ways in which authorities can use social media to reframe discontent so that it is redirected in more benign directions. An example of the potential for reframing was recently illustrated

by a Twitter conversation in response to a Newsweek cover that featured two men with fists in the air under the headline, "Muslim Rage."[16] In an effort to promote a conversation about the cover story, which concerned riots that broke out in response to a film clip posted to YouTube lampooning Islam, Newsweek asked its readers to tweet their thoughts. What it got in response was an onslaught of comments that mocked both the Newsweek story and the Islamic rioters in the Middle East. One reader captured the general sentiment:

> I think it was this unspoken communal desire to reclaim the initiative, not just from what was regarded as kind of a cynical and inflammatory cover from Newsweek, but also just from a terrible, terrible week. I mean, it had been a really disillusioning week, seeing the way that this movie was responded to in Muslim countries in the Middle East. Even if it was only a thousand people here and a thousand people there, seeing people take the bait so easily was depressing … I think for a lot of people it sort of restored their faith in the community, because, honestly, this should have been the response to this movie from the very start. *It should have been mocked and then ignored* (emphasis added).[17]

The dampening effect, if any, that these tweets may have had on the riots in the Middle East is difficult to determine, but they illustrate the potential of how social media tools, such as Twitter, can be harnessed to reframe discontent, so that rather than resorting to violence, people can express their anger in public dialogue.[18]

Not only can social media be used to reframe discontent, however, they can be used to turn public opinion against popular insurgent movements as well. For example, Óscar Morales, a Colombian civil engineer, grew increasingly frustrated by the FARC's human-rights abuses, so in 2008 he set up a Facebook page called "One Million Voices Against the FARC," whose motto was "No more kidnappings, No more lies, No more killings, No more FARC."[19] His campaign not only helped attract attention to the insurgents' indiscriminate use of violence, but it led to worldwide protests against the FARC.[20] Some analysts are beginning to imagine how social media can be used to alienate insurgent groups and other dark networks from the wider population, a key aspect of counterinsurgency theory.[21]

Some analysts imagine how social media can be used to alienate dark networks from the wider population.

Whither the Future?

So what can we say about how insurgents and authorities will attempt to capitalize on social media tools to further their goals? I think it is relatively safe to conclude that insurgents will continue to turn to social media to communicate and frame grievances, and if the past is any indication of the future, they will become increasingly sophisticated in doing so. This will place a heavy burden on those of us who seek to disrupt dark networks, to keep abreast of the latest social media developments. It is fairly certain that as we become more adept at tracking the movements of insurgents, terrorists, criminals, and others from information gleaned from social media outlets,

As we become more adept at tracking insurgents, terrorists, and criminals, these actors will abandon old technologies in favor of new ones.

these actors will abandon old technologies in favor of new ones. The rewards for attaining and maintaining a high level of technological sophistication in the use of social media are high. The costs for not doing so may be even higher. ❖

NOTES

1 I'd like to thank my colleagues Rob Schroeder and Seth Lucente for their cogent comments and suggestions for improving this article.

2 Quoted in Nadine Kassem Chebib and Rabia Miatullah Sohail, "The Reason Social Media Contributed to the 2011 Egyptian Revolution," *International Journal of Business Research and Management* 2 (2011): 139.

3 Dark networks are those groups that actively seek to hide their activity from existing authorities. They are typically defined as "covert and illegal" networks and are often assumed to be malicious. See Jörg Raab and H. Brinton Milward, "Dark Networks as Problems," *Journal of Public Administration Research and Theory* 13 (2003): 413–39. They can, however, be forces for good, such as the World War II Polish resistance group Żegota illustrates (see Irene Tomaszewski, and Tecia Webowski, Żegota, *The Council for Aid to Jews in Occupied Poland, 1942-45,* rev. ed. (Montreal: Price-Patterson, Ltd., 1999), or, as some may argue, in several countries during the Arab Spring uprisings.

4 See, for example, Chebib and Sohail, "The Reason Social Media Contributed," 139–62; Philip N. Howard, Aiden Duffy, Deen Freelon, Muzammil Hassain, Will Mari, and Marwa Mazaid, "Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring," Working Paper 2011.1, Project on Information Technology and Political Islam, University of Washington-Seattle, 2011, 1–30.

5 Christian S. Smith, *What Is a Person? Rethinking Humanity, Social Life, and the Moral Good from the Person Up* (Chicago and London: The University of Chicago Press, 2010), 375–376.

6 Esteban Manriquez, "FARC Leader Rallies Base on Twitter," Colombia Reports, Medellín, Colombia, 2012: http://colombiareports.com/colombia-news/news/26216-farc-leader-rallies-base-on-twitter.html; accessed on October 16, 2012. The FARC's Facebook page is located at http://www.facebook.com/pages/FARC-FUERZAS-ARMADAS-REVOLUCIONARIAS-DE-COLOMBIA/151722051581104; accessed on October 16, 2012. FARC member Mojuluna Alberti's Facebook page notes that he is a product manager for the FARC and that he is from Cairo, Egypt but currently living in Guadalupe, Nuevo León, Mexico. The NPS CORE Lab followed the original FARC Twitter account (@FARC_COLOMBIA) and discovered that it was simply taking long statements and cutting them up into a series of 140-character (or less) tweets. In short, it was an unsophisticated use of Twitter.

7 Seth Lucente, Robert Schroeder, and Gregory Freeman, "Syria: Crossing the Red Line," an unpublished report from the CORE Lab, Defense Analysis Department, Naval Postgraduate School, 2012.

8 Quoted in Tom Hays, "NYPD Is Watching Facebook to Fight Gang Bloodshed," *Associated Press,* October 2, 2012: http://hosted.ap.org/dynamic/stories/U/US_GANG_CRACKDOWN_NYC?SITE=AP&SECTION=HOME&TEMPLATE=DEFAULT; accessed October 16, 2012.

9 Ibid. Also see Maria Ressa ("The New Battlefield: The Internet and Social Media") and Peter Kent Forster ("Countering Individual Jihad: Perspectives on Nidal Hasan and Colleen LaRose"), in this issue, both of whom describe uses of network tracking to identify terrorists.

10 See Aaron Weisburd ("Artisanal Intelligence and Information Triage") in this issue for more on cyber forensics.

11 John Arquilla, "Aspects of Netwar & the Conflict with Al Qaeda," Information Operations Center, Naval Postgraduate School, Monterey, California, 2009, 34.

12 Derek Hansen, Ben Shneiderman, and Marc A. Smith, *Analyzing Social Media Networks with NodeXL: Insights from a Connected World* (Burlington, Mass.: Morgan Kaufmann, 2010).

13 Christian S. Smith, *The Emergence of Liberation Theology: Radical Religion and Social Movement Theory* (Chicago: University of Chicago Press, 1991), 61.

14 Glenn E. Robinson, "Hamas as Social Movement," in *Islamic Activism: A Social Movement Theory Approach,* Quintan Wiktorowicz, ed. (Bloomington: Indiana University Press, 2004), 129.

15 Howard, et al., "Opening Closed Regimes," 1–4.

16 The cover can be seen at: http://www.magazine-agent.com/newsweek/magazine

17 Ashraf Khalil, interviewed by Audie Cornish, "Newsweek's 'Muslim Rage' Cover Mocked on Twitter," *All Things Considered,* National Public Radio, September 18, 2012: http://www.npr.org/2012/09/18/161369296/newsweeks-muslim-rage-cover-mocked-on-twitter; accessed on October 16, 2012.

18 James Efaw and Chris Heidger describe their success using Facebook to influence an online community ("Another Tool in the Influencer's Toolbox: A Case Study") in this issue.

19 See the site at: http://www.facebook.com/pages/One-million-voices-against-FARC/10780185890

20 David Kirkpatrick, "The 'Facebook Effect': Standing up against the FARC," Facebook blog post, Menlo Park, California, June 8, 2010): http://blog.facebook.com/blog.php?post=397218557130; accessed on October 16, 2012.

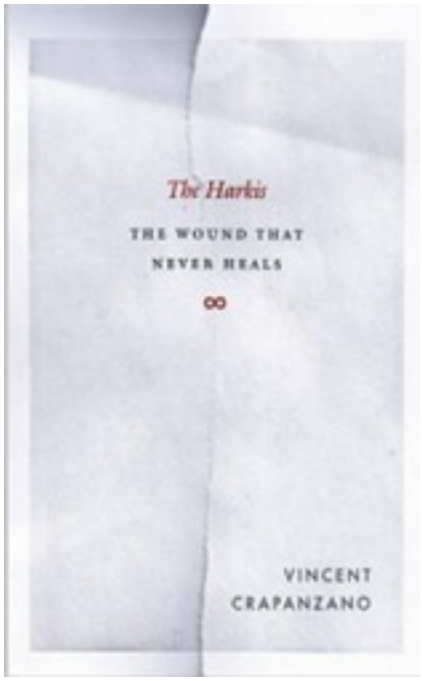
21 David Galula, *Counterinsurgency Warfare: Theory and Practice* (Westport, Conn.: Praeger Security International, 2006, originally published in 1964); David Kilcullen, Counterinsurgency (Oxford and New York: Oxford University Press, 2010); Eric P. Wendt, "Strategic Counterinsurgency Modeling," *Special Warfare* (September 2005): 1–13; available at: http://www.highbeam.com/doc/1P3-913087021.html; accessed October 16, 2012.

THE WRITTEN WORD

The Harkis: The Wound that Never Heals

Joey Wang

Author: Vincent Crapanzano
University of Chicago Press
ISBN-10: 9780226118765
Hardcover: $35.00 USD
248 pages



In the 2007 movie, L'ennemi Intime (Intimate Enemies), a cinematic tour de force of the French-Algerian War, some soldiers in a French company are ordered to take a *fellagha*, a captured insurgent out for a "walk in the woods" and dispose of him. During this walk, Saïd, a Harki (an Algerian fighting on the French side) in the company strikes up a conversation with the *fellagha*. Saïd discovers that the *fellagha*'s name is Idir Danoun, and that they both had fought at the battle of Monte Cassino. When the company stops for a rest, Saïd shares a cigarette with Danoun and asks him why he had joined the FLN guerrillas. Danoun silently takes the cigarette that he has just lit and, while Saïd watches curiously, lights the other end. Danoun then says, "Look at this cigarette. This is you. On one end is the French Army, on the other, the FLN. Either way, you lose. You don't know who you are anymore. You're no longer an Algerian. You'll never be a Frenchman."

We know the fate of Danoun, who had chosen to side with the FLN. But the movie never reveals the ultimate fate of Saïd, who sided with the French Army. Was he killed in the war? Did he survive? We never know. Saïd's role ends thus perfectly, neatly swept off the stage.

Harkis like Saïd have remained a vestige of the brutal French-Algerian War that all the protagonists sought to ignore, forget, or exterminate. Unlike Saïd, however, history and historiography do not always allow uncomfortable truths to be neatly swept off of the stage. It is in this context that the fate of the Harkis and the impact on their descendants are explored, in Vincent Crapanzano's latest work, *The Harkis: The Wound that Never Heals*.

Based on a combination of archival research and face-to-face interviews, Crapazano's results are riveting. In a typical scene, Crapanzano observes that the father of a man named Boussad "speaks to no one. He just sits at home and stares into space." (p. 116) This silence in Crapanzano's interviews is pervasive. It speaks to the presence of memories that have nowhere to go. Crapanzano inquires if perhaps Boussad's paternal uncle, who is often drunk, might be a willing interlocutor. Also to no avail: "What the use? The past is the past." (p. 116)

This silence is pervasive. It speaks to the presence of memories that have nowhere to go.

Throughout his work, Crapanzano makes extraordinary efforts to engage the old Harkis and record their stories to ensure that they do not simply vanish from the stage like Saïd. But, like the other protagonists in this war, these men would rather forget: "What's the point? ... It's over. It's best forgotten." (p. 9) Crapanzano, however, recognizes that it is often far harder to forget than to remember. Indeed, the lifeless stares into space, the depression, the drunken stupors, the psychoses, the apathy, the suicides, the violence, all suggest that, in fact, nothing has been forgotten. It is evidence that demands a verdict.

During the French-Algerian War, the Muslim community was faced with a choice: join either the FLN insurgency, or the French Army as an auxiliary. As all students of insurgencies know, the only neutrals are dead ones. Indeed, Muslims often joined the French Army only after being forced to witness the slaughter of their family members en masse. All told, approximately 260,000 Algerians of Arab or Berber descent served in various capacities in the French Army as Harkis.

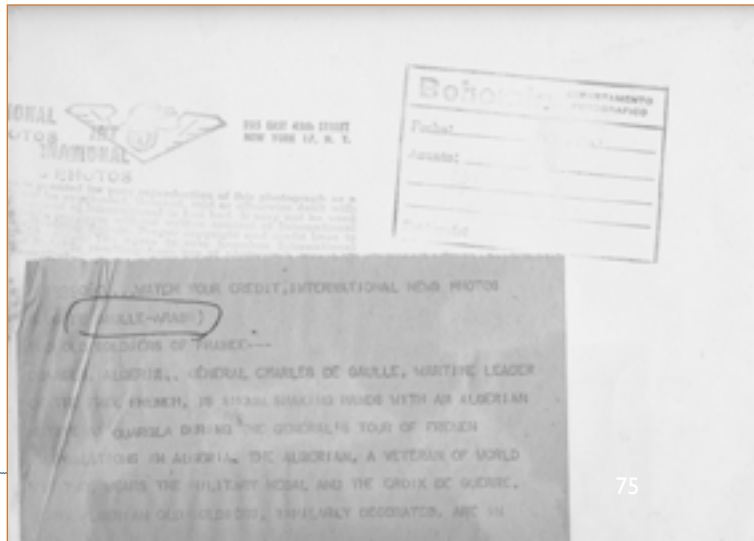
Approximately 260,000 Algerians of Arab or Berber descent served in various capacities in the French Army as Harkis.

As the war drew to a close, the period leading up to the ratification of the Treaty of Evian (July 3, 1962) was a defining period for the Harkis. With *Algérie Francaise* quickly slipping away, the French Army was losing its ability to maintain order. In the midst of the transition's chaos and confusion, the Harkis were told to return to their villages. Crapanzano recalls a conversation with Hacène, whose father, a Harki, was told by the French to turn in his weapon because he was going to be issued a more sophisticated one. Once he had done so, his father and the entire attachment were sent back to their village unarmed, with the understanding that with the Treaty signed, they would be protected. As the men had feared, this provision, however well intended, was totally unenforceable and proved to be an outright death sentence. Indeed, "some of the Harkis were sacrificed as soon as they entered the village."

Betrayal and abandonment run throughout the Harkis' story. As with so much in Algeria, though, there was another side to it. Crapanzano reminds his readers that the French army did not always stand by in abject obsequiousness while this murderous rampage took place. Some, in fact, made heroic attempts to spirit their Harkis back to France. While one officer with whom the author spoke "simply denied knowing anything about it," he found many more who, disgusted and dispirited, lamented their powerlessness in the face of negotiated defeat.

Many [French soldiers], disgusted and dispirited, lamented their powerlessness in the face of negotiated defeat.

For those Harkis who were fortunate enough to escape, life was anything but predictable. For most, however, emigration—which began in the summer of 1962—began with a harrowing ride in the cargo hold of a ship to Marseille. Most had never even seen the ocean, let alone been on a ship. Upon arrival, the families were transferred by rail to military camps that had been hastily erected to accommodate the surge of refugees. Those unheated and rodent-infested camps, according to Crapanzano, were representative of the deplorable conditions that most would endure for years. They were overseen by poorly trained, often unsympathetic and resentful administrators who thought their own careers had been brought to a dead-end by the assignment. Even once in France, the war's dangers never subsided completely for the refugees, who were viewed with suspicion by the French even as they were pursued by the FLN with revenge in mind.



Whether or not one ever found his way out of these camps depended upon skills, qualifications, connections, and often a bit of luck. As Crapanzano explains, this reflected the dichotomy between French assimilationists, who advocated settling Harki families throughout

France, and the isolationists who advocated keeping them separate from French society. Put another way, "The assimilationists wanted to make them French; the isolationists wanted them to disappear."

The camps have long been closed and abandoned, but they serve as constant reminders of France's imperial past and its consequences. Crapanzano, in his final reflections, addresses the monumental challenges in achieving forgiveness and reconciliation; from France, the Harkis' adopted country, and from Algeria, their native country. In both countries they exist at best as pariahs, at worst as traitors. Most of his interviews were with the children of the Harkis, many of whom experienced both the deprivations of the camps and the excesses of the camp administrators. Consequently, they also bear the scars of their parents.

"The assimilationists wanted to make them French; the isolationists wanted them to disappear."

Some have moved on with their lives, becoming writers, businessmen, doctors, or lawyers. Others have become activists fighting for recognition of the sacrifices their parents made for the *tricolore*. But many, if not most, of the grandchildren are unemployed and living on welfare in subsidized housing. Tragically, today, this world is becoming more isolated, and its inhabitants are undergoing an "intensification of Muslim identity," according to a report for the Institut Montaigne.

Crapanzano has chronicled the story of the Harkis with a well-researched and heartfelt, deeply disturbing personal journey. He illuminates not only the immediate costs of the Algerian rearguard action, but the less known collateral damage visited upon those forced to make choices that meant only preserving one's life for the moment. Insightfully written, this work skillfully shifts our focus in one of the great geopolitical conflicts of the twentieth century to the most elemental level, that of the individual. ❖

ABOUT THE REVIEWER

Joey Wang is an analyst with the U.S. Department of Defense. He received a M.A. in National Security and Strategic Studies from the U.S. Naval War College, and a M.A in Strategic Security Studies from the College of International Security Affairs, National Defense University. He has also completed the National and International Security program for senior executives at Harvard's John F. Kennedy School of Government. His essays on international security and insurgency have received international recognition.

PHOTO CREDITS

1 All photos courtesy of the author.

NOTES

1 In pages 66-80, Crapanzano discusses in depth not only the decisions that led some to join the FLN and others the French Army, but also the rationales for switching sides.

2 Available at http://www.banlieue-de-la-republique.fr/

RESOURCES: PUBLICATIONS

The following publications are available electronically from the publications section of the JSOU (Joint Special Operations University) public web site: https://jsou.socom.mil

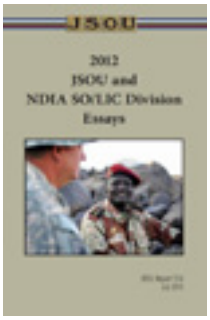
USSOCOM Research Topics 2013

Issue Date: July 2012

The USSOCOM Research Topics 2013 list identifies and categorizes suggested SOF-related topics for research by PME students, JSOU Senior Fellows, and other SOF researchers who want to make timely and meaningful contributions to issues of concern to SOF. Each year representatives from USSOCOM, the Theater Special Operations Commands (TSOCs), SOF chairs from the war colleges, and JSOU senior fellows develop a list of issues salient for SOF in the near term. The resulting topics are vetted through the components and TSOCs to ensure that research will advance SOF missions and support SOF interests. The final recommendations for research topics are approved by the USSOCOM commander. Ultimately, the research, study, and debate of these topics will inform decision makers and better prepare SOF for our current conflicts and future challenges. ❖

2012 JSOU and NDIA SOLIC Division Essays

Issue Date: July 2012



Each year, JSOU partners with the Special Operations and Low Intensity Conflict (SO/LIC) chapter of the National Defense Industrial Association (NDIA) to sponsor this annual essay contest. The first-place winner is recognized at the NDIA SO/LIC Symposium, held each February, and awarded a $1,000 cash prize. The first runner-up receives a $500 prize. The competition is open to resident and nonresident students attending Professional Military Education (PME) institutions, and regularly produces outstanding works on special operations issues. These essays provide current insights on what our PME students see as priority national security issues affecting special operations. JSOU is pleased to offer this selection of the top five essays from the 2012 contest, in the hope that they may benefit the reader professionally and encourage future PME students to write on special operations issues. ❖

Knowing Your Partner: The Evolution of Brazilian Special Operations Forces

by Alvaro de Souza Pinheiro

Issue Date: August 2012

In this monograph, retired Brazilian Army Major General Alvaro de Souza Pinheiro highlights the importance of knowing our partners. Beginning with a look at the post-9/11 world from the Brazilian point of view, General Pinheiro presents the history and a current overview of Brazilian SOF units from the Army, Navy, Marine Corps, and Air Force. The pioneers of Brazilian Army SOF, educated and trained at U.S. Army schools, founded Brazil's Special Operations Course in 1958, which was later expanded to include Commando Actions, Special Forces, and Jungle Operations qualifications courses. In 2002 the Brazilian Special Operations Brigade was created by presidential decree. As U.S. Special Operations Command looks to strengthen the global SOF network, General Pinhiero's monograph is a must-read for the American SOF operator who seeks to better know our partners. ❖

CALL FOR SUBMISSIONS

The Combating Terrorism Exchange (CTX) is a quarterly peer-reviewed journal. We accepts submissions of nearly any type, from anyone; however, submission does not guarantee publication. Our aim is to distribute high quality analyses, opinions, and studies to military officers, government officials, and security and academic professionals in the counterterrorism community. We give priority to non-typical, insightful work, and to topics concerning countries with the most pressing terrorism and CT issues.

Submission Guidelines

CTX accepts the following types of submissions. Please observe the following length guidelines:

- **academic analyses** (5,000–7,000 words)
- **reports or insightful stories from the field** (2,000–3,000 words)
- **photographic essays**
- **video clips** with explanation or narration
- **interviews** with relevant figures (no longer than 15 minutes)
- **book reviews** (500–1,000 words); review essays (1,000–3,000 words); or lists of books of interest (which may include books in other languages)
- reports on any **special projects**

Submission Requirements

Submissions to CTX **must** adhere to the following:

- the work must be copyedited for basic errors *prior to* submission;
- citations should adhere to the *Chicago Manual of Style*, available online;
- the work submitted may not be plagiarized in part or in whole;
- you must have consent from anyone whose pictures, videos, or statements you include in your work;
- you must agree to our Terms of Copyright;
- include a byline as you would like it to appear and a short bio as you would like it to appear (we may use either, or both);
- Any kind of submission can be multimedia.

Submissions should be sent in original, workable format (in other words, we must be able to edit your work in the format in which you send it to us: no PDFs please!)

Submissions should be in English. Because we seek submissions from the global CT community, and especially look forward to work which will stir debate, WE WILL NOT REJECT submissions outright simply because of poorly written English. However, we may ask you to have your submission re-edited before submitting again.

Ready to Submit?

By making a submission to CTX you are acknowledging that your submission adheres to all of the Submission Requirements listed above, and that you agree to the CTX Terms of Copyright, so read them carefully.

Submit to:
CTXSubmit@GlobalECCO.org

If you have questions about submissions, or anything else, contact:
CTXEditor@GlobalECCO.org

Terms of Copyright

CTX is now online at globalecco.org/journal

CONTRIBUTE TO CTX:
CTXEditor@GlobalECCO.org