Recruitment and Radicalization: The Role of Social Media and New Technology

Maeghin Alarid

As parts of the Middle East imploded following the euphoria of the Arab Spring, some Americans shocked friends, family, policymakers, and pundits alike by leaving home to join the Islamic State of Iraq and the Levant (ISIL) and other terrorist organizations operating in the chaos of Syria, Iraq, and Libya. By May 2015, hundreds of U.S. citizens had joined the fight on the side of the extremists, and many others had been apprehended in the attempt. Even greater numbers of recruits left Europe, making their way across the Mediterranean, or overland through Turkey, to join the self-declared caliphate in its latest call to jihad. In 2014 in the UK alone, conservative estimates pegged the numbers of radicalized individuals leaving to join ISIL at five per week.[1] By 2015, the numbers were generally believed to have climbed significantly.

In their efforts at both radicalization and recruitment, terrorists, militias, and other illicit organizations have used social media in a calculated strategy that confounds many in the West. As a CNN article recently concluded, "Violent extremists like the self-proclaimed Islamic State of Iraq and Syria, or ISIS, have become increasingly sophisticated at creating dense, global networks of support online, networks that are helping these groups run virtual circles around governments and communities."[2]

Terrorist groups have good reason to use social media, whose popularity suits them in many ways. In 2015, the Internet is fast overtaking conventional forms of media such as books, magazines, and television to become the leading research and entertainment platform.[3] Social media outlets allow them to present themselves as just another part of mainstream news. Most social media platforms are easy to use and cost little or nothing. With them, terrorists can tailor their message to narrow audience niches, enlisting the help of the virtual world to enter the homes of millions of people.[4]

This chapter details how illicit organizations, including international terrorist groups, use the Internet and social media to radicalize and recruit individuals online and carry out attacks. Focusing specifically on al-Qaeda and the Islamic State of Iraq and the Levant (ISIL), we also examine how and why terrorists target women for recruitment—a particularly disturbing trend. Finally, we discuss how the West can turn the tables on the terrorists, and outline a basic approach to deterrence, using the same social media platforms and techniques as those favored by the terrorists themselves.

---

[1] Ben Brumfield, "Officials: 3 Denver Girls Played Hooky from School and Tried to Join ISIS," CNN News, Oct. 22, 2014, www.cnn.com/2014/10/22/us/colorado-teens-syria-odyssey/.

[2] Quintan Wiktorowicz and Shahed Amanullah, "How Tech Can Fight Extremism," CNN News, Feb. 17, 2015, www.cnn.com/2015/02/16/opinion/wiktorowicz-tech-fighting-extremism/.

[3] Gabriel Weimann, "Social Media's Appeal to Terrorists," *Insite Blog on Terrorism and Extremism*, Oct, 3, 2014, http://news.siteintelgroup.com/blog/index.php/entry/295-social-media's-appeal-to-terrorists.

[4] Ibid.

How Online Radicalization Happens

Contrary to popular belief, many people who are radicalized online are not devout Muslims. Quite the contrary; some do not consider themselves very religious at all. It is also easy to categorize anyone recruited online as gullible, but this is simply not the case. In fact, many people who become caught up in online propaganda did not seek it out—it found them. The demographics vary widely. They may be barely or highly educated, young or old, male or female. Even financial status is no indicator. Online radicalization occurs in all economic classes. It reaches those of lower economic means and those who are financially stable.

The common denominator seems to be that everyone who is radicalized and recruited online feels sympathetic toward that group's cause, and people who feel there is "something missing" from their lives appear to be more susceptible than others. Radicalization is more widespread where conditions of inequality and political frustration prevail. It often takes root in people who sympathize with the plight of the oppressed and wish to show their solidarity. Radicalized men and women alike often feel despair, humiliation, and outrage over injustice and perceive few options for influencing change.[5] One brief moment of intense emotion evoked in them while they watch a YouTube video of innocent victims in Africa or the Middle East can be all it takes to spark their interest.

Once someone is mobilized, next steps vary. Some begin to research the causes that various extremist groups are fighting for. This leads to their discovery of the radical groups—and, more troublingly, to the groups' discovery of *them.* The Internet makes it easy to be found. A candidate for recruitment may come to the group's attention by making a financial donation, downloading extremist propaganda, entering a jihadi chat room, or visiting radical pages on Facebook. In today's environment, we see numerous examples of the radicalization process, from interest to recruitment, through execution of an actual mission, happening entirely online.

Radicalizing and recruiting online has great advantages over the traditional (and riskier) public communications. Terrorist groups can reach out to an incalculably vast audience. With no travel required, cost is minimal, no logistics or transportation support is needed, and the odds of detection are low. And the newly radicalized need not necessarily pack up and head for the Middle East—jihadi groups encourage attacks at home to avoid the risk of infiltration while traveling.

The threshold for engaging in cyber jihad is markedly lower than for someone who gives up a familiar, comfortable life to travel to an actual battle zone and risk death or capture. If the notion of online activism as a proper, respectable, and sufficient form of jihad wins wide acceptance within radical circles, we can expect ever-increasing efforts in online propaganda and cyber attacks. This could further inspire yet more individuals, facilitating both radicalization and recruitment, and lead to a new cycle of attacks.

From al-Qaeda to ISIL: An Increasingly Sophisticated Approach

The use of social media for recruitment and radicalization did not just suddenly emerge with ISIL. Even before 9/11, al-Qaeda recognized the value in harnessing the "new" media. It used the Internet to broadcast its message worldwide and prospect for recruits.

---

[5] Ibid.

It used the Internet for operational purposes, too. Much of the planning for the 9/11 attacks happened using online platforms. The attackers communicated with one another through the Internet and researched their targets online.[6]

Over time, terrorist groups have adapted their efforts with the changing battlefield landscape. In an undated letter to Taliban leader Mullah Omar that was quoted in a 2014 *International Security* article, al-Qaeda's leader, Osama bin Laden, observed that "90 percent of the preparation for war is effective use of the media." Al-Qaeda has long advocated *ghazwa ma'lumatiyya* ("information operations") and *harb electroniyya* ("electronic warfare").

The article's authors pointed out that bin Laden's successor, Ayman al-Zawahiri, shared this view. He spoke of the "jihad of the spear" and the "jihad of the *bayan*" (message, declaration). He considered the latter more important and praised the "knights of the media jihad," the "clandestine mujahideen," who are conducting it.[7] Al-Zawahiri practiced what he preached, making his declarations known in several videos and magazines posted online.

Social Media Platforms: Recruiting and Building Communities of Terrorist Practice

Social media differ from traditional media in several fundamental ways. They enable any terrorist group to reach a huge audience and circulate its message worldwide, and they provide a way to ensure that the group's propaganda lives forever online. And social media are democratic in the sense that they enable anyone to publish or access information online.[8] Social media are often used to incite fear in the general public and deliver threats (using tweets as one method), create a sense of community, radicalize others, romanticize Sharia law and the Islamic State, and offer travel advice and logistics for recruits.

As the Critical Incident Analysis Group (CIAG) points out, the Internet allows for vital dialogue between extremist ideas and inquisitive minds to take place in a virtual setting where infiltration is difficult: "For the post-Iraq (post-2003) generation especially, Internet chat rooms are now supplementing and replacing mosques, community centres and coffee shops as venues for recruitment."[9]

Nearly everyone in business today, licit or illicit, understands the importance of creating online communities. Even small mom-and-pop shops that were reluctant to provide Wi-Fi to their customers or build a website to market their business know that if they want to succeed and grow their customer base, an online community is a great way to start. And higher educational institutions realize that to stay relevant, they must routinely offer online courses and degree programs. According to Don Hinchcliffe of ZDNet, "Online communities are seen as a way to organize people and accomplish work

---

[6] Critical Incident Analysis Group (CIAG), "NETworked Radicalization: A Counter-Strategy," 2007, http://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/HSPI_Report_11.pdf.

[7] Jerry Mark Long and Alex Wilner, "Delegitimizing al-Qaida: Defeating an 'Army Whose Men Love Death,'" *International Security* 39, no. 1 (Summer 2014).

[8] Gabriel Weimann, "New Terrorism and New Media," Wilson Center, 2014, www.wilsoncenter.org/sites/default/files/STIP_140501_new_terrorism_F.pdf.

[9] CIAG, "NETworked Radicalization."

in a collaborative manner, across geographic and demographic boundaries. The world is beginning to understand that online communities aren't just for socializing; they are also for getting things done."[10]

Illicit power structures, and terrorist organizations in particular, understand this as well as anyone. As this study of al-Qaeda and ISIL shows, such groups have adapted the same platforms that we all commonly use and rely on. They use them to foster intraorganizational communication, radicalize the vulnerable, mobilize supporters, and recruit people from all over the world. And over time, they have become increasingly effective and increasingly efficient. Here are some key ways that they are leveraging the cyber universe to their own ends.

Open Source Journals and Publications

Cyber magazines have become a signature communications platform for both al-Qaeda and the Islamic State. *Inspire,* the al-Qaeda in the Arabian Peninsula (AQAP) online magazine, widely available on the Internet as early as 2010, was published in English to reach a vast Western audience. True to its name, the magazine succeeded in inspiring others to take up the cause. Several editions of *Inspire* provided lengthy, detailed instructions on how to plan and execute bomb attacks, and lone individuals and groups acting on behalf of AQAP made or attempted terrorist attacks after downloading its material. Most notably, Tamerlan and Dzhokhar Tsarnaev, the brothers who committed the terrorist bombings at the 2013 Boston Marathon, used homemade bombs made from ordinary pressure cookers, using a recipe they obtained from *Inspire*.[11]

The magazine also routinely uses past terrorist attacks to illustrate which methods work well against Western forces, and warns followers about which methods to avoid. Articles detail specific attacks, such as Umar Farouk Abdulmutallab's unsuccessful Christmas Day bombing attempt aboard a transatlantic flight bound for Detroit. The magazine uses such examples to help future jihadists accomplish their objective while avoiding capture and incarceration.

Like AQAP, ISIL publishes an online magazine: *Dabiq.* The magazine's name was carefully chosen. Dabiq is a small Syrian town close to the Turkish border, and the prophetic location where Muslims battle infidels.[12] The production quality is impressive, and the articles contain adroitly wrought arguments legitimizing ISIL's actions against the West. It is illustrated with skillfully edited images of world leaders and regional events, depicting the Islamic State as rational and moral, and anyone who disagrees with its philosophy as venal and self-serving.

As of March 2015, at least nine issues of *Dabiq* had been published online.[13] The mag-

---

[10] Dion Hinchcliffe, "Ten Leading Platforms for Creating Online Communities," Sept. 4, 2008, www.zdnet.com/article/ten-leading-platforms-for-creating-online-communities/.

[11] Azmat Khan, "The Magazine that 'Inspired' the Boston Bombers," *Frontline*, Apr. 30, 2013. www.pbs.org/wgbh/pages/frontline/iraq-war-on-terror/topsecretamerica/the-magazine-that-inspired-the-boston-bombers/.

[12] *BBC News*, "Why Islamic State Chose Town of Dabiq for Propaganda," Nov. 17, 2014, www.bbc.com/news/world-middle-east-30083303.

[13] Clarion Project, "The Islamic State's (ISIS, ISIL) Magazine," Sept. 10, 2014, www.clarionproject.org/news/islamic-state-isis-isil-propaganda-magazine-dabiq#.

azine, printed in English and several other languages, features articles on such topics as holy war, the importance of community, and unity within the ranks. And, of course, no issue would be complete without several colorfully written articles boasting of ISIL victories on the battlefield.[14] The National Consortium for the Study of Terrorism and Responses to Terrorism (START) compared the AQAP and ISIL publications. It found *Dabiq* notable "because the emphasis is on maintaining a strong media brand and disseminating highly ideologically-congruent propaganda to promote radicalism among distant operatives, sympathizers, and foreign fighters whereas *Inspire* had a strong focus on training."[15]

ISIL's online recruitment tactics do not rely solely on *Dabiq.* The magazine is only one method the group uses to reach its wide audience. Early in its existence, ISIL understood the value of using social media and video game technology to radicalize as many individuals as possible, specifically targeting those who are young and computer savvy. ISIL's aim is to reach every corner of the earth and gain recruits to expand the self-declared caliphate. Its use of new technology and social media is unprecedented and unlike anything seen before in a terrorist group. Its marketing campaign is truly impressive, and it is happening on a massive scale.

"Liking" Jihad

By January 2014, the average age of Facebook users was 30 years, with almost half of all users logging in daily. As of April 2015, the online social network had roughly 1.3 billion active accounts every month, and 54.2 million individual and group pages.[16] Terrorist groups understand that if they want to reach out to the younger generation, this is an excellent vehicle. A 2010 report by the Department of Homeland Security listed several ways that terrorist groups use Facebook, and we have seen both al-Qaeda and ISIL use them all:

- "as a way to share operational and tactical information, such as bomb recipes, AK-47 maintenance and use, tactical shooting, etc.;

- as a gateway to extremist sites and other online radical content by linking on Facebook group pages and in discussion forums;

- as a media outlet for terrorist propaganda and extremist ideological messaging;

- as a wealth of information for remote reconnaissance for targeting purposes."[17]

---

[14] *Counter Jihad Report*, "Islamic State Magazine Asks, 'Did You Think We Were Joking?'" May 26, 2015, http://counterjihadreport.com/tag/they-plot-and-allah-plots/.

[15] START, "The Islamic State of Iraq and the Levant: Branding, Leadership Culture and Lethal Attraction," report, Univ. of Maryland, Nov. 2014, www.start.umd.edu/pubs/START_ISIL%20Branding%20 Leadership%20Culture%20and%20Lethal%20Attraction_Ligon_Nov2014.pdf.

[16] Statistic Brain Research Institute, "Facebook Statistics," Apr. 14, 2015, www.statisticbrain.com/facebook-statistics/.

[17] Jana Winter, "Al Qaeda Looks to Make New 'Friends' — on Facebook," *Fox News*, Jan. 9, 2010, www.foxnews.com/tech/2010/12/09/facebook-friends-terror.

This list will not remain static. As Facebook and similar online social networks evolve, seemingly infinite avenues for promoting jihadist messages, disseminating threats to enemies, and infiltrating homes, families, and safe havens will emerge. The only limits on terrorists' use of this popular social media site are the bounds of human imagination.

Tweeting Terrorism

Twitter is another Internet social network that terrorist groups are using to their advantage. With it, they can get their propaganda out in almost real time. But the real targets of the tweets are not necessarily the recruiting base. Rather, the targets increasingly are Western institutions, news media, and anyone else who will react to a well-timed terrorist tweet. Terrorist groups use Twitter to put out fake news stories, entice followers, and win sympathy. There have been many instances of mainstream media mistaking terrorist-originated tweets as legitimate sources of breaking news. One particularly notable incident occurred in April 2013, when the Associated Press Twitter account was hacked and an ominous message posted: "Breaking: Two Explosions in the White House and Barack Obama Is Injured."[18] Within minutes of this false Twitter report, stocks on Wall Street plummeted.

In an effort to prevent itself from becoming a platform of choice for illicit goals and objectives, Twitter has suspended many accounts, but to no avail. The terrorists have proved nimbler than the administrators, and their sites generate an almost immediate response as soon as they appear. For example, when the Syrian extremist organization al-Nusra Front's Twitter accounts were shut down, the group had opened up a new account that had more than 20,000 followers within 24 hours.[19]

Getting It on Video

YouTube is another social medium that terrorists are using effectively. Their online recruitment videos even have sound tracks of slickly produced hip-hop music. According to a 2007 Associated Press article, this immensely popular platform receives "tens of thousands of new videos daily, and users watch over a hundred million per day, making content difficult to monitor."[20] According to statistics provided by YouTube, 300 hours of videos are uploaded to the site *every minute.*[21] Because of the sheer volume of videos added to the site each day, YouTube struggles with the Herculean task of filtering terrorist content. The site displays a "promotes terrorism" tag underneath all videos and relies on viewers to use this tag to flag inappropriate content for removal. Even so, the site cannot keep up with the onslaught of new content.[22] "Though authorities have identified

[18] Adam Shell, "Stocks Gyrate Wildly after Fake Terror Tweet," *USA Today*, Apr. 23, 2013, www.usatoday.com/story/money/markets/2013/04/23/stocks-gyrate-wildly-after-fake-terror-tweet/2107089/.

[19] Weimann, "New Terrorism and New Media."

[20] Tariq Panja, "Militant Islamic Groups Turn to YouTube," Associated Press, Feb. 11, 2007, http://www.nbcnews.com/id/17107489/#.VYr-FE3JCUk.

[21] YouTube, "Statistics," Oct. 10, 2014, www.youtube.com/yt/press/statistics.html.

[22] *NBC News*, "Ads Shown Before YouTube ISIS Videos Catch Companies Off-Guard," Mar. 10, 2015, www.nbcnews.com/storyline/isis-terror/ads-shown-isis-videos-youtube-catch-companies-guard-n320946.

a number of jihadist propaganda pieces—some of them viewed by thousands—these are often replaced almost as soon as they are removed."[23]

Removal comes at a cost, however, for those who are trying to counter radicalization and recruitment. For the intelligence community in particular, it is vitally important to analyze the tradeoff between the damage that jihadist videos can do and the potential intelligence that they may divulge. The complex debate whether to let these terrorist groups have a voice online is ongoing.[24] It may be possible for companies such as YouTube (as well as Google, Twitter, and Facebook) to use algorithms to detect violent language and content, much as they use them to ferret out illegal content involving children, and prevent these videos from being posted. This would deny the jihadists a useful medium, but what impact will it have on the intelligence community, which has gotten valuable inside information from such videos? To further complicate the dilemma, terrorists are keenly aware that their postings and videos are being monitored; thus, the actual intelligence value to be gained from their YouTube activity is questionable.

Radicalization and Video Game Technology

Terrorist groups worldwide have made no secret of their attempts to appeal to a younger generation. Various articles written as early as 2006 discuss how websites created by terrorist groups were meant to draw in "a computer savvy, media-saturated, video game-addicted generation."[25] One early jihadist website featured a video game titled "Quest for Bush," in which players "fight Americans and proceed to different levels including 'Jihad Growing Up' and 'Americans' Hell.'"[26] The game was released in 2006 by the Global Islamic Media Front, a radical organization with ties to al-Qaeda. According to one article, its "players are prompted to advance through six missions against soldiers who look like Bush, followed by a seventh mission against a character that looks like the president that takes place in a desert-like region. During the game, jihadist songs are played in the background."[27]

Quest for Bush was not the first, and certainly not the last, of its genre. But in 2006, it was the most extreme addition to a small but growing list of Islamic extremist video games, monitored by the Defense Department and much blogged about in gaming circles. Some are free, others not. But as the *Washington Post* describes them, they all champion issues "from an Islamic perspective, in stark contrast to many Western-made games that generally cast Muslims and Arabs as the bad guys. Furthermore, they underscore a brewing game-design war between East and West, a simmering tension over who is writing (and rewriting) history."[28]

---

[23] Tariq Panja, "Militant Islamic Groups Turn to YouTube," *Washington Post*, Feb. 11, 2007.

[24] Yigal Carmon and Steven Stalinsky, "Terrorist Use of U.S. Social Media Is a National Security Threat," *Forbes*, Jan. 30, 2015, www.forbes.com/sites/realspin/2015/01/30/terrorist-use-of-u-s-social-media-is-a-national-security-threat/2/.

[25] Bruce Hoffman, "The Use of the Internet by Islamic Extremists," Testimony before the House Permanent Select Committee on Intelligence, May 4, 2006, RAND, www.rand.org/content/dam/rand/pubs/testimonies/2006/RAND_CT262-1.pdf.

[26] Jose Antonio Vargas, "Way Radical, Dude," *Washington Post*, Oct. 9, 2006, www.washingtonpost.com/wp-dyn/content/article/2006/10/08/AR2006100800931.html.

[27] CNN, "Web Video Game Aim: 'Kill' Bush Characters," *CNN World News*, Sept. 18, 2006, www.cnn.com/2006/WORLD/meast/09/18/bush.game/index.html.

[28] Vargas, "Way Radical, Dude."

Terrorist groups have been using video game technology in their recruitment efforts since early in the first decade of this century. Recently, though, ISIL's efforts have reached unprecedented levels in scale and capabilities. Adapting the most popular video game of 2012, Grand Theft Auto, it created its own modifications so that players can role-play as members of ISIL engaged in combat.[29] Specific modifications made to the game include ISIL militants killing law enforcement officers and attacking military convoys with explosives, and ISIL snipers shooting American soldiers.[30]

Perhaps, in using video game development as a recruiting tactic, ISIL has taken a page from the U.S. military playbook. The U.S. Army published the video game America's Army in 2002, to be used as a recruitment video to reach the younger generation.[31] America's Army has been wildly successful and was listed as one of the top ten video games in the world in 2002-8.[32] Although a direct link has not been established, it is certainly in the realm of possibility that ISIL was aware of this marketing campaign by the U.S. Army, saw how successful the video game was at gaining recruits, and appropriated the idea to increase its own ranks.

Terrorist groups worldwide learn tactics from one another as well as from their sworn enemies. Video game technology is just one more way for them to reach a large audience. If militaries have been using video games not only to recruit soldiers but also to train them, as Professor Corey Mead's book *War Play* suggests, then why would adversarial groups not use this technology in the same way?[33] And indeed, they are.

Using Specialized Technology to Increase Reach and Effectiveness

Terrorists use many innovative methods to communicate online. The CIAG report states:

- Terrorists can draft an email message and save it as a draft rather than sending it, so that anyone with access to that email account can log in and read the message. Known as "dead drops," these communications are less subject to interception [than an email that has been sent].

- Terrorists can post training manuals online or even hack into a legitimate website and hide training materials "deep in seemingly innocuous subdirectories of the legitimate site," a process known as "parasiting."[34]

- Terrorists can conduct research on potential targets online, where both text and imagery, including satellite photography, is frequently available. Google Earth, for instance, has been used to target British soldiers in Iraq with increasing accuracy.

---

[29] START, "The Islamic State of Iraq and the Levant."

[30] *INQUISITR*, "ISIS Uses 'Grand Theft Auto' Mock Up to Recruit and Boost Morale," Sept. 19, 2014, www.inquisitr.com/1486558/isis-uses-grand-theft-auto-mock-up-to-recruit-and-boost-morale/.

[31] Brian Kennedy, "Uncle Sam Wants You (To Play This Game)," *New York Times*, July 11, 2002.

[32] Corey Mead, "Military Recruiters Have Gone Too Far," *TIME*, Sept. 17, 2013.

[33] Corey Mead, *War Play: Video Games and the Future of Armed Conflict* (Boston: Houghton Mifflin Harcourt, 2013).

[34] Technical Analysis Group, "Examining the Cyber Capabilities of Islamic Terrorist Groups," Dartmouth College, Nov. 2003, www.ists.dartmouth.edu/library/164.pdf, quoted in CIAG, "NETworked Radicalization."

- Terrorists can appeal anonymously for donations of financial or other support via websites.[35]

Another way that terrorists use social networking sites is with a method known as *narrowcasting.* According to Gabriel Weimann, "Narrowcasting aims messages at specific segments of the public defined by values, preferences, demographic attributes, or subscription. An online page, video, or chat's name, images, appeals, and information are tailored to match the profile of a particular social group."[36] Terrorist groups view online profiles and even user history and then target online pages, videos, or extremist chat rooms to match a particular individual. Using these methods of deduction, terrorist groups winnow their target audience by age, gender, and historical preferences. This technique is a classic Marketing 101 tool, revealing which sites users visit most often and what kinds of products they view online, and thus guiding marketers in what products to promote to them. Terrorist groups view people's profiles and decide whom to target and how best to approach each individual. "An online page, video, or chat's name, images, appeals, and information are tailored to match the profile of a particular social group. These methods enable terrorists to target youth especially."[37]

Understanding the many ways that the Internet can be used to their advantage is vital for terrorist organizations. "Social media also has numerous technical advantages for terrorists: sharing, uploading or downloading files and videos no longer requires access to computers or cyber-savvy members capable of using sophisticated computers and advanced programs. Using smart phones and social media platforms allows simple, free and fast access to all."[38]

It is vital that policymakers monitor the various methods by which terrorist groups use the Internet—and specifically social media. These groups are constantly trying to keep a step ahead of the game in their radicalization and recruitment efforts, while contriving new ways to attack their enemies.

Using Social Media to Launch Cyber Attacks

Although this analysis focuses on the various methods of online recruitment and radicalization by terrorist groups, no discussion of Internet terrorist activity would be complete if it failed to mention incidents of previous cyber attacks and the threat of possible cyber attacks to come. Says Weimann, "The online platforms used to promote electronic jihad are also used for operational purposes such as instruction and training, data mining, coordination, and psychological warfare."[39]

A 2008 article in the *Forensic Examiner* discussed another form of cyber warfare favored by terrorist groups. These attacks, known as "denial of service," work by impeding a cyber network's abilities and inundating the system with an enormous number of "pings" to create *message flooding.* The author explains: "A ping is a [data] packet that allows an attacker to determine whether a given system is active on a network. A flood of pings is transmitted to a targeted site. The pings saturate the victim's bandwidth and

---

[35] CIAG, "NETworked Radicalization."
[36] Weimann, "New Terrorism and New Media."
[37] Ibid.
[38] Ibid.
[39] Ibid.

fill up the system's buffer (memory space), causing network performance to deteriorate and the system to hang, crash, or reboot."[40]

To pull off cyber attacks such as these, ISIL and other terrorist groups rely increasingly on technologically savvy younger recruits. With their young recruits' hacking skills, they can penetrate critical infrastructure systems such as electrical grids and the financial sector. For example, in 1997 in Massachusetts, a hacker disabled a computer system that operated the local airport control tower.[41] And in 2000, hackers infiltrated the computer systems controlling the flow of natural gas through Russian pipelines.[42]

This much is certain: if we have seen these attacks before, we will see them again. Terrorist groups are constantly watching the behavior of other groups, learning which kinds of attacks are successful and which to avoid. Thus, they grow ever more sophisticated, with shorter learning curves.

Online Radicalization of Women

As of this writing in 2015, the world is late on the scene in examining the Islamic State's strategies for recruiting and radicalizing women. Terrorist groups have always recruited both males and females, but ISIL has made clear a specific agenda of enlisting women in its cause. In June 2014, ISIL declared itself a caliphate, and since then it has ramped up its efforts to gain both recruits and territory across Iraq and Syria. Its recruitment of women has turned into a massive endeavor that caught the West flat-footed, and we are only beginning to understand the implications. Throughout 2014, scarcely a week passed without news articles about young women in the West leaving home and fleeing to Syria. The stories left us perplexed and infuriated. Our emotional response to the ongoing news has been warranted, certainly, though it has been largely unhelpful. We have paid attention to the pattern of female recruitment, but we have not stopped to question the logic of this particular pattern.

Why ISIL Recruits Women

ISIL understood that to grow its ranks in the long-term and not just in the present, it needed a cadre of women to give birth to the next generation of fighters. Women living in Europe and countries outside the Middle East are among the least likely people to be suspected of Islamist extremism, which makes them prime targets for recruitment. Also, women are not often seen as posing an imminent threat and may be able to travel more freely than men without arousing suspicion. Interestingly, the ISIL campaign to recruit females was carried out primarily by European women who left their home countries, joined ISIL, and relocated to Syria. The recruitment campaign consists of ISIL propaganda, instruction on how women can communicate with ISIL members, and logistics on how Muslim women (of all ages) can travel to Syria and join the cause.[43]

---

[40] Marie Wright, "Technology and Terrorism: How the Internet Facilitates Radicalization," Forensic Examiner, Winter 2008.

[41] Mudawi Mukhtar Elmusharaf, "Cyber Terrorism: The New Kind of Terrorism," Computer Crime Research Center, Apr. 8, 2004, www.crime-research.org/articles/cyber_terrorism_new_kind_terrorism/.

[42] Ibid.

[43] Rita Katz, "From Teenage Colorado Girls to Islamic State Recruits: A Case Study in Radicalization

Researcher Rita Katz reports, "IS women recruiters created dozens of social media accounts, urging women to move to the 'Land of the Caliphate.'"[44] Travel manuals can be found online giving logistics for travel to Syria, where to cross borders undetected, and what to pack for a new life in ISIL. Photos have been posted online showing Western women who have fled their homes and traveled to Syria to join the caliphate. These photos depict young women carrying weapons and surrounded by ammunition. Tweets from women who have joined ISIL include flowery descriptions of a positive environment where they have been embraced in the prophesied land of the new Islamic State.[45]

In February 2014, the United States and its European allies learned that ISIL had formed Umm al-Rayan, "a female brigade, with the purpose of exposing male activists who disguise in women's clothing to avoid detention when stopping at the ISIL checkpoints."[46] According to Islamic custom, men cannot physically touch women on the streets. But the women of Umm al-Rayan can stop anyone dressed in hijab. Each woman receives "a monthly salary of 25,000 Syrian liras (less than $200) and is only allowed to be employed within the brigade."[47] As of this writing, the brigade had not yet taken part in acts of terrorism, but its existence, coupled with ISIL's demonstrated willingness to commit violence and murder against women in the territories it controls, is causing concern.

Why Women Join

It is perhaps puzzling why women might be willing to support a group that oppresses females, or that they would choose to support bombings that kill innocent women and children. But women have indeed shown repeatedly that they are willing to take up arms for extremist organizations and violent causes. They have been on the front lines of battle in extremist groups the world over, including Peru's Shining Path, Chechen rebel groups, and the Sri Lankan Tamil Tigers, and their participation, during the 1970s and 1980s, in terrorist organizations such as the Weather Underground in the United States, and the Red Army Brigades and the Red Army Faction in Europe, is well known.[48] Hence, it should come as no surprise that they are participants in ISIL's particularly brutal extremist violence.

The possibility also exists that despite the terrible oppression of women in many terrorist groups, women join to prove the worth of their gender in the hope of making strides toward women's rights. But while this might cross the minds of some, it is not the force driving their loyalty to the group. Far more commonly, women decide to leave their families, friends, and lives behind and join extremist groups for the same reason as

---

via Social Media," *Insite Blog on Terrorism and Extremism*, Nov. 11, 2014, http://news.siteintelgroup.com/blog/index.php/entry/309-from-teenage-colorado-girls-to-islamic-state-recruits-a-case-study-in-radicalization-via-social-media.

[44] Ibid.

[45] Ibid.

[46] TRAC, "Umm al-Rayan," TRAC report summary, 2014, www.trackingterrorism.org/group/umm-al-rayan.

[47] Ibid.

[48] Nimmi Gowrinathan, "The Women of ISIS: Understanding and Combating Female Extremism," *Foreign Affairs*, Aug. 21, 2014, www.foreignaffairs.com/articles/middle-east/2014-08-21/women-isis.

men: they believe in the cause. If policymakers ever hope to understand the prevalence of female radicalization and recruitment, they must first put the stereotypes to rest.

What, then, is the apparent particular vulnerability of Muslim women to radicalization and recruitment? It may stem from deep feelings of marginalization. These women may be attracted to the idea of belonging to something greater than themselves, and to the elevated status that they expect to achieve by joining ISIL. When women feel they are seen as the "other" in the country where they live, and their religious ideology tells them they have a greater purpose and duty as a Muslim, these are prime conditions for recruitment. Online interactions encourage these feelings because they can foster a sense of community and belonging in a virtual world, which may not exist in the real world. And just as online social media are used to generate fear and spread terror, they are also used to create relationships and feelings of closeness and fitting in with a group.

Fighting Fire with Fire: How to Deter Online Radicalization

The obvious question arises: how to deter this growing threat of recruitment and radicalization using online social media and other new technology? The 2014 analysis by Jerry Mark Long and Alex Wilner, examining al-Qaeda's perspective on social media and the Internet, also suggested a number of practicable ways to diminish the appeal of radical messages online. The authors suggest that the process may begin with depriving extremist groups of their socioreligious appeal. If the very message that the group promotes can be debunked as a false teaching and an obscene misinterpretation of Islam, the very rationale for joining the group vanishes. Stripping away the group's legitimacy will diminish both its community of support and its target pool of recruits. For instance, by challenging al-Qaeda's religious appeal, one may debunk the very way the group legitimizes its acts of terrorism.[49]

An apt example of challenging the jihadists' religious appeal is the campaign to deradicalize inmates in Saudi Arabia's prisons. This program places radicalized individuals with religious scholars who educate them in the teachings of the Quran. According to a PAK Institute report, in 2004 the religious counseling program had some 2,000 prisoners enrolled. By 2007, about 700 had been released upon completing the program.[50] The program has achieved a high success rate through (a) helping individuals learn the true teachings of the Quran and thus avoid buying into the extremist message; (b) rehabilitating former jihadists; and (c) reintegrating them back into their communities.[51] The report attributes much of the program's success to the social support that the prisoners receive after completing the rehabilitation program—for example, assistance in finding employment and living arrangements.

Exploiting the Narrative

As Long and Wilner point out, all extremist groups have a narrative, and it is within the West's power to turn that narrative on its head and use it against them. If the group's manifesto appears questionable, the group will lose sympathizers and, with them, re-

---

[49] Long and Wilner, "Delegitimizing al-Qaida.

[50] Saba Noor and Shagufta Hayat, "Deradicalization: Approaches and Models," PAK Institute for Peace Studies, Apr. 2009, http://san-pips.com/download.php?f=116.pdf.

[51] Ibid.

cruits and revenue. Thus, the West can and must deter potential sympathizers by manipulating the group's message. According to the PAK Institute, "In strategic terms, if we can target a message, we thereby deter/compel those who would have adopted it, along with those who currently employ it. And the degree to which al-Qaida's message loses traction with Arab and Islamic publics is the degree to which deterrence by delegitimization will have succeeded."[52]

Sometimes, the terrorist group itself, through its actions, inadvertently delegitimizes its own message. For example, al-Shabaab lost support after employing cruel tactics, such as suicide bombings that caused the death of many civilians. The group also withheld goods and services from the people of Somalia, causing many civilians to starve.[53] Whenever a terrorist group incurs such a loss of confidence, this creates a golden opportunity for Western news media and intelligence agencies to highlight that group's brutality, thus deterring potential new recruits.

A terrorist group can survive only when it has a following of people who support its cause. History has shown us that without a critical mass of supporters, the group will shrink in size and eventually become irrelevant. Men and women contemplating joining an extremist group will not do so if they feel that the group's belief system is flawed or disingenuous. An examination of past and present terrorist groups shows that when the recruitment pool deems the group's behavior offensive and illegitimate, the group will soon become obsolete.[54]

The International Centre for the Study of Radicalisation and Political Violence (ICSR) has discovered numerous online messages revealing that many of the women married off to jihadi fighters in Syria are mourning husbands who have died fighting for ISIL. And the ICSR has seen several online posts from British women describing the harsh living conditions in Syria, including the lack of hot water for bathing, and the high incidence of illness from the cold.[55] Such online social media posts, painting life within ISIL in a negative light, can be an effective tool in counterradicalization efforts. Intelligence agencies can and should take advantage of social media to routinely monitor what is going on within the ranks of groups such as ISIL. Online social media posts from members themselves provide an excellent opportunity to infiltrate the group.

Understanding Cultural Implications and Shifting the Cultural Identity

It is crucial for policymakers to understand how these groups grow their community of support and portray themselves to the world as a force to be reckoned with. And it is equally important to understand how the extremists' narrative "guides its interpretation of history and of contemporary Western policies"—for example, al-Qaeda's narrative that the actions of the West are monolithic and that they are aimed entirely at expanding

---

[52] Long and Wilner, "Delegitimizing al-Qaida."

[53] Armin Rosen, "How Africa's Most Threatening Terrorist Group Lost Control of Somalia," *Atlantic*, Sept. 21, 2012, www.theatlantic.com/international/archive/2012/09/how-africas-most-threatening-terrorist-group-lost-control-of-somalia/262655/.

[54] Long and Wilner, "Delegitimizing al-Qaida."

[55] Mark Townsend, "How a Team of Social Media Experts Is Able to Keep Track of the UK Jihadis," *Guardian*, Jan. 17, 2015, www.theguardian.com/world/2015/jan/17/social-media-british-jihadists-islamic-state-facebook-twitter.

Western policies and advancing the West's economic stance in the world.[56] This understanding is essential to deterring the threat that extremist groups pose online.

The CIAG report mentioned earlier discusses another key factor in deterring radicalization: understanding the link between how a group thinks and how it acts, based on its cultural identity. Not so long ago, geography played a much greater role in determining an individual's worldview.[57] In today's virtual world, this is often no longer the case.

"Whether contained within a country of origin or within ethnic or immigrant communities, spread of large group identities was only as effective as the limited transportation possibilities at the time. . . . It may be that the Internet is transforming large group identity formation from a lateral, physical process to a metastatic, technological process. Previous boundaries have little relevance."[58]

In short, a successful counterterrorist message must include these elements:

- Be easily accessible.
- Be able to reach the masses.
- Reach out to women.
- Be as globally pervasive and ubiquitous in countering the terrorist message as ISIL is in promoting it.

A surprising example of a counterterrorist message that had a significant impact online originated with the hacker group known as Anonymous. In early 2015, in response to the January 2015 terrorist attack on the satirical Parisian newspaper *Charlie Hebdo,* Anonymous hacked into a large number of ISIL Twitter and Facebook accounts, shutting them down and also sending this message: "You [ISIL] will be treated like a virus, and we are the cure."[59] Hacker attacks such as this against ISIL and other terrorist groups will not prevent the spread of extremism online. But they certainly can present a strong counter message, and a reminder to the online community that illicit power structures do not own the space unimpeded, but are as vulnerable as any other entity that depends on cyberspace to further its objectives.

How to Deter Women from Online Radicalization and Recruitment

As Badran points out, even in patriarchal societies, women often have a solid and powerful network of connections to their surrounding community. This allows them to exert influence in their neighborhoods, towns, villages, and universities. This connection to community is vitally important when studying female recruitment efforts by jihadist groups because, across most cultures, women connect with other local women. Women can provide a powerful voice that should not be discounted in the effort to prevent other women from becoming radicalized.[60]

Counterterrorism officials need to recognize that women's roles within a community can be a key source of intelligence about existing radicalization in their neighborhoods.

---

[56] Long and Wilner, "Delegitimizing al-Qaida."

[57] CIAG, "NETworked Radicalization."

[58] Ibid.

[59] Chris Perez, "Anonymous Attacks ISIS Supporters Online," *New York Post*, Feb. 10, 2015, http://nypost.com/2015/02/10/hacking-group-anonymous-attacks-isis-supporters-online/.

[60] Badran, "Women and Radicalization."

Women are often quite savvy about what goes on in their community. Despite their status as second-class citizens in many cultures, women are predominantly the ones raising the next generation. Their children will grow up, perhaps to become extremists, but perhaps instead to be the first in their family to graduate from college.[61]

The Organization for Security and Cooperation in Europe (OSCE) has consistently stressed the importance of reaching out to women in communities vulnerable to extremism. Stressing best practices in security and development, the OSCE emphasizes gender inclusion as a cornerstone of effective security sector reform, security force development, and community stabilization and resilience:

"Women can have special potential in countering VERLT (violent extremism and radicalization that lead to terrorism). The involvement of women as policy shapers, educators, community members and activists is essential to address the conditions conducive to terrorism and effectively prevent terrorism. Women can provide crucial feedback on the current counter-terrorism efforts of the international community and can point out when preventive policies and practices are having counterproductive impacts on their communities."[62]

The ideal target audience for helping with efforts to deradicalize women is also the same target audience that jihadi groups hope to recruit: modern, young, second generation, perhaps studying abroad. Terrorist groups understand, however, that targeting women from this particular demographic is risky because they may already believe in and support gender equality and, in fact, are *not* prone to radicalization. For feminist transnational networking organizations, this same demographic comprises a whole new generation of Muslim women who have grown up exposed to new Islam-grounded gender-egalitarian ideas. When properly empowered, these women can reach out to other women and play a vital role in deterring their online radicalization and recruitment.[63]

It is not enough to focus on the straightforward technical solution of removing or blocking radical material online. This strategy will not stop terrorist groups from gaining recruits. Indeed, a purely technical solution will probably not be cost effective and may, in fact, work in the terrorists' favor. The independent research organization ICSR, which concluded to help policymakers and practitioners find more intelligent solutions in dealing with radicalization and political violence, concluded that a successful strategy to dissuade the recruitment of women must include the following:

- Dissuade people from posting extremist messages online, by removing such websites and prosecuting the owners. This will send a strong message that those involved in online extremism are within the reach of the law and will be penalized.

- Help online communities take matters into their own hands and vet all material posted to their group pages. They can do this through creation of an *Internet users panel* that would provide a way for members of the online community to report complaints.

---

[61] OSCE, "Women and Terrorist Radicalization Final Report," Mar. 13, 2012, www.osce.org/atu/99919?download=true.
[62] Ibid.
[63] Badran, "Women and Radicalization."

- Diminish the terrorist message by having a larger "counter message" online.[64] For example, develop more websites (largely for women) that spread an antiviolence message of Islam as a peaceful religion that supports women's rights.

- Encourage the publication of progressive messages online, thus discouraging extremist propaganda. Efforts to counter online radicalization of women through social media must include using precisely this technology, not shying away from online social media methods but using those same sites to counter radicalization messages.[65]

Conclusion

Illicit power is not new. Illicit power structures' use of the Internet is not new. Illicit power structures' use of social media and video game technology, to the extent that ISIL is using them, *is* new. And it is dangerous. ISIL's radicalization and recruitment efforts via social media and cyber technology have been very successful in gaining sympathizers worldwide. Terrorists and other illicit organizations understand that the young generation spends a huge amount of its time online, and they target that population for this reason. They realize how vitally important it is to have the young generation in their ranks.

These young people have tremendous cyber capabilities, which can help the terrorists not only radicalize and recruit new blood but also conduct cyber attacks on their enemies. Attacks on electrical systems, transportation systems, and the financial sector can be devastating. We have seen such attacks in the past, and we will continue to see this method of warfare in the future. Extremist groups know that they must adapt and change to survive on the changing landscape of war. They will continue to use the Internet to maintain their current methods and will also try to eclipse those methods with new, more effective ones.

Illicit power structures will continue to use the Internet and new technology—to spread their extremist message, to execute attacks, and to recruit women to their cause. The importance of women within these groups worldwide must not be discounted. If counterterrorism officials can work with other women and focus on changing the hearts and minds of females within these groups, perhaps these mothers at home will begin to teach their sons and daughters to fight with their words and counter the extremists' distortion of the Quran, instead of taking up arms.

The situation is by no means hopeless, nor is it a one-way street. In 2012, the NGO Invisible Children launched its KONY 2012 campaign as "an experiment." "Could an online video [take on an illicit power structure by making its leader,] an obscure war criminal, famous? And if he was famous, would the world work together to stop him?"[66] According to Invisible Children's website, "the experiment yielded the fastest growing viral video of all time. The KONY 2012 film reached 100 million views in 6 days, and 3.7

---

[64] ICSR, "Countering Online Radicalisation: A Strategy for Action," Jan. 28, 2009, http://icsr.info/projects/the-challenge-of-online-radicalisation/.

[65] Ibid.

[66] Invisible Children, "Kony 2012," 2012, http://invisiblechildren.com/kony-2012/.

million people pledged their support for efforts to arrest Joseph Kony." [67] Few outsiders dispute Invisible Children's numbers, and even though the campaign failed to lead to Kony's capture, it riveted world attention and began the conversation on how we can use the Internet and social media to counter extreme cases of impunity when the nation state where it resides is either unwilling or unable to take action.

Three years later, following the massacres in Paris of *Charlie Hebdo* leaders and staff, online counter messaging triumphed with the launch of the *Charlie Hebdo* app. This app was approved by Apple's App Store and made available for users to download less than two hours after developers contacted the Apple CEO. This is highly unusual in that it typically takes a week and a half for an app to get approval and become available for users.[68] The app allowed the user to support the Charlie Hebdo cause of free speech, subscribe to the magazine, and also acquire the issue that was published after the attack.[69] By downloading this app, the user simultaneously supports the Charlie Hebdo creed: "Because a pencil will always be better than barbarity . . . because freedom is a universal right," and demonstrates how technology and social media can be turned against those who would use them to kill and enslave others.[70] Or, as Weimann points out, "Online social media is not only a potent way to promote terrorism, but also a necessary tool in preventing it. . . . This is the emerging challenge for the West: to regain the cyber territory it has long ceded to extremists."[71]

---

[67] Ibid.

[68] Alyssa Newcomb, "Charlie Hebdo Launches App Version of Latest Issue," *ABC News*, Jan. 20, 2015, http://abcnews.go.com/Technology/charlie-hebdo-launches-app-version-latest-issue/print?id=28345203.

[69] *Charlie Hebdo*, "Charlie Hebdo," app, Apple iTunes Preview, Jan. 2015, https://itunes.apple.com/us/app/charlie-hebdo./id957966299?mt=8.

[70] Ibid.

[71] Weimann, "Social Media's Appeal to Terrorists."