Cyber Jihad in the Service of the Islamic State (ISIS)

Adam Hoffman and Yoram Schweitzer

In early 2015 US President Barack Obama stated that terrorist organizations such as al-Qaeda and the Islamic State (hereafter ISIS) use the internet and social media to recruit young Muslim operatives to their ranks by radicalizing their views: "The high quality videos, the online magazines, the use of social media, terrorist Twitter accounts – it's all designed to target today's young people online, in cyberspace."[1] The President's statement helped position the use of cyberspace by terrorist organizations at the center of the struggle against terrorism in the current age in general and against the ISIS phenomenon in particular.

The use of communications media by terrorist organizations is not new, but the technological tools available in recent years has affected the nature of their activities and thereby changed the nature of the perceived threat they pose. As part of these changes, cyber jihad has begun to occupy a central place in the discussion on how to contend with ISIS. This article defines cyber jihad, surveys its characteristics, examines its central influence in establishing the ISIS image, and probes ways of contending with this challenge. The intensive use that ISIS makes of cyber jihad as a tool for recruitment, radicalization, and dissemination of propaganda makes the struggle against this element no less important than the physical engagement with its forces and the prevention of its geographic expansion.

What is Cyber Jihad?

The term "cyber jihad" refers to use of 21st century technological tools and cyberspace (the environment in which communication between computer

Adam Hoffman is a Neubauer research associate in the Terrorism and Low Intensity Conflict Program at INSS. Yoram Schweitzer is a senior research fellow and head of the Terrorism and Low Intensity Conflict Program at INSS.

networks occurs) in order to promote the notion of a violent jihad against those classified by its followers as enemies of Islam. While the concept of cyber jihad has evolved over the years, the use of online space by jihad organizations per se is not a new phenomenon: a popular manual published already in 2003 extolled the "electronic jihad," which includes participating in forums and hacking websites with the aim of participating in the media battle against the West and the perceived enemies of Islam in the Arab world.[2] This manual and others attest to the tremendous importance that Salafi-jihadi organizations attribute to online space, which enables them to circumvent the barriers placed before them by various state institutions and security organizations and disseminate the message calling for a violent struggle against the West and the "infidel" Arab regimes without interruption and faster and more easily than ever before.

The internet, which was the main online communications medium in the late 1990s and early 2000s, initially served as the primary platform for cyber jihad by Islamic terrorist organizations. However, recent years have seen far reaching technological developments, particularly the rise of social media, which facilitate the use of cyberspace by terrorist entities and allow additional courses of action, especially internet-based services and applications that enable users to share content. Currently, the cyber jihad concept refers mainly to the use of online social networks such as Facebook, Twitter, YouTube, and Tumblr.[3] Yet while social media has evolved a great deal, some basic properties characterizing this type of communications media remain: the content in social media is user-based, enables and encourages sharing and interactivity, and is characterized by a rapid flow of information between people. As such, the communication on social media is fundamentally different from the internet, which is hierarchical in nature and based on fixed sites and closed forums.

Cyber Jihad in the Service of ISIS

Although the use of cyberspace by jihad organizations is not new, ISIS uses the internet, and primarily social media, more than any other terrorist organization before it. In addition to the organization's technological capabilities, it appears that its primary innovation in its use of cyber jihad is its role in transforming ISIS from yet another Islamic fundamentalist terrorist organization into a global brand name that features prominently in the public discourse in the West, as well as in the Muslim world. As part of its efforts to influence Middle East and global public opinion and brand itself, ISIS disseminates propaganda materials using a well-designed online magazine in English called *Dabiq* and produces high quality movies that are disseminated on YouTube, Twitter, and various websites affiliated with the organization.

Furthermore, the organization targets and exploits online social networks for its own needs on an unprecedented scale. ISIS makes extensive use of Twitter, Facebook, Tumblr, and Instagram, and according to senior American officials, operatives and supporters of the organization produce up to 90,000 tweets every day. [4] A recent extensive study found that ISIS supporters operate at least 46,000 independent Twitter accounts, with 200-500 of these accounts active all day, thereby helping to disseminate the organization's propaganda.[5] In addition, the organization developed an application for mobile devices called "Dawn of Glad Tidings," which for a while was available for download in Google and Apple app stores and enabled its supporters to follow the organization's activities in real time. Downloading the application allowed ISIS to take temporary control of the Twitter account of the said user and publish messages in his/her name. In this way, ISIS, as part of its social media strategy, managed to generate a significant volume of activity on Twitter and exploit the accounts of the application users to raise the online profile of the organization in a coordinated campaign.[6]

In addition to the extensive use of social media by the organization's operatives and supporters, ISIS' cyber jihad includes offensive use of online space for attacks on websites. Jihad organizations often refer to this offensive activity as a *ghazwa* (raid/attack, in Arabic), in the spirit of the raids in which the Prophet Muhammad participated in the seventh century against the infidels. This was how the September 11 attack was referred to by its planners,[7] and various jihad organizations in Syria use this term to describe their military operations against the Assad regime. Similarly, ISIS supporters characterize the digital attacks as an "electronic raid (*ghazwa*)."

Prominent examples of this type of cyber jihad are the ISIS takeover of the social media accounts of the US Central Command and of French websites following the terrorist attack on the *Charlie Hebdo* magazine. In the first case, ISIS supporters hacked into the Twitter and YouTube accounts of the United States Central Command (CENTCOM), which is responsible for US military activity in the Middle East and for coordinating the international coalition attacks against ISIS. After taking over these accounts, hackers replaced the official American emblems with the ISIS black flag and broadcast from these accounts messages supporting the organization that announced its presence on US military bases – ironically, at the same time that President Obama was delivering a speech in Washington on cyber security.[8] In the second case, hacker groups affiliated with ISIS attacked more than 19,000 French websites in the week following the terrorist attack on *Charlie Hebdo* in Paris, and the servers of these sites collapsed because of the attacks. This cyber attack was described by a senior French official as "unprecedented," and the first time that a country has dealt with a cyber attack on such an extensive scale. [9]

The Role of ISIS Cyber Jihad

ISIS perceives the cyber jihad as an integral part of its overall strategy, alongside its military combat and takeover of territories, and as serving several functions. First, the use of social media – and particularly the manipulation of online social networks, such as by using the Dawn of Glad Tidings application – enables ISIS to generate a volume of activity in social media greatly exceeding the organization's true dimensions, and thus serves as a force multiplier and an effective medium for psychological warfare. The combination of a high noise level in social media with images and video clips of atrocities creates a deterring and frightening effect, which succeeds in influencing the morale of ISIS' adversaries. A clear example of this can be seen prior to ISIS' takeover of Mosul, the second largest city in Iraq, in early June 2014. The organization's takeover of the city was considered by most analysts to be impossible, as the ISIS fighters who took part in the fighting numbered roughly 1,500, against thousands of Iraqi soldiers armed with American weapons and equipment defending Mosul, at a ratio of 1:15.[10] However, to the surprise of many (including, apparently, ISIS itself), the militants managed to take over the city after four days of fighting, while many Iraqi soldiers shed their uniforms and tried to assimilate into the civilian population in an attempt to evade their attackers.[11] Alongside the structural weaknesses of the Iraqi military, the use that ISIS made of social media apparently had a significant role in this move. Commanders and fighters in the Kurdish Peshmerga forces attested that ISIS had begun a social media campaign nearly a year before the conquest of the city "in order to show how they kill people and even take their children and kill them. This is truly psychological warfare and I can testify that it is successful."[12] In this manner ISIS manages to use cyber capabilities to enhance its image as a powerful and unstoppable force, much beyond the actual number of fighters that are at its disposal.

Second, in order to leverage opportunities for recruitment, ISIS uses social media as a marketing tool, and for this purpose implements a strategy tailored to individual target audiences. John Horgan, a forensic psychologist who specializes in the psychology of terrorism, noted that the opportunities currently available to recruiters for terrorist organizations for communicating with young people in the wake of the popularity of social media are "unique" and "bigger than ever in the history of terrorism."[13] The message that is disseminated differs between men and women and uses symbols and images that are tailored to the respective target audiences. For young men, ISIS uses images from the days of early Islam of knights on horses, epic battles, and glory on the battlefield, which are displayed in the publications of the organization and on high quality video clips. For women, on the other hand, the marketing of the message uses "softer" images, such as pictures of kittens (such as the Twitter account @ISILCats) and Tumblr, which is more popular among women.[14] Alongside the "softer" images, ISIS also disseminates messages of female empowerment with photos of armed operatives in the al-Khansaa Brigade (the women's unit of ISIS named after a female Muslim poet from the time of the Prophet Muhammad), which conveys the message that "in ISIS, women carry weapons and are capable of defending themselves." The message is that in a fundamentalist organization such as ISIS women can gain protection, status, and empowerment that they could not attain in the traditional society in the Arab world or even in the liberal West. In this manner ISIS "sews" different marketing suits, depending on the target audience – male or female, Muslim or Western – and communicates with a global audience using social media.

Foreign Fighters and "Lone Wolf" Terrorist Attacks

ISIS cyber jihad is conducted on nearly every possible channel, and thereby maximizes the possibilities inherent in online space for disseminating its messages. The two principal effects of this effort are the accelerated recruitment of foreign fighters joining the organization and the encouragement of terrorist attacks in the West perpetrated by "lone wolves." The precise number of foreign fighters who have joined the organization is unknown, but according to various estimates, it currently stands at more than 20,000, of whom some 4,000 are Western volunteers. This number exceeds the number of those volunteering to fight against the Soviet Army in Afghanistan from 1979 to 1989, which is considered the conflict that had drawn the largest number of foreign fighters in the second half of the twentieth century.[15] ISIS activity on social media is ascribed a key role in this trend and many organizational recruits (as well as people who attempted to join the organization but were arrested by the security agencies of the various countries prior to enlisting) attest that the content on social media affected their decision to join its ranks.

Some researchers have noted that social media should not be credited with an exclusive role in this process of radicalization and recruitment. Max Abrahms argues that the battlefield successes of ISIS constitute a more significant factor in the decision to join its ranks than the organization's effective use of social media, and Thomas Hegghammer attributes the flow of foreign fighters to poorly policed borders and the ease of travel to Syria.[16] Nonetheless, it seems that social media indeed plays a key role in this phenomenon, since it presents ISIS as a winning brand, encourages volunteers to join, and even instructs how this can be done. An e-book published by ISIS, titled *Hijrah* (migration/journey, in Arabic) *to the Islamic State*, details how to reach the caliphate territories and what the prospective traveler should pack.[17]

In addition to facilitating the flow of foreign fighters, ISIS cyber jihad strategy encourages the phenomenon of "lone wolves," who, inspired by the organization but with no official connection to it, perpetrate terrorist attacks in the West. For instance, the terrorist attacks in Sydney, Paris, and Copenhagen were perpetrated by individuals who were influenced by ISIS and used its flag, but were not formally affiliated with the organization. ISIS saw these terrorist attacks as a success and appropriated them for itself. The organization also released video clips praising Omar el-Hussein, the terrorist from Copenhagen, and called for additional terrorist attacks by lone wolves.[18] Lone wolf attacks, which are for the most part perpetrated with no early warning, allow ISIS to operate outside the Middle East through sympathetic operatives and supporters. The message to Muslims in the West is thus that even if they cannot immigrate to the territory of the Islamic State and join its ranks, perpetrating terrorist attacks and attacking Western symbols in their countries constitutes a worthy alternative. The use by ISIS of social media inspires such acts, conveys remote instructions with respect to the preferred targets without the need for physical communication between the perpetrators and ISIS members, and confers the official blessing of the organization subsequent to the attack on the perpetrator. The lone wolf phenomenon, which has already materialized several times, currently poses a significant threat to Western countries, particularly in face of what is disseminated through social media.

Contending with the Cyber Jihad Challenge

Cyber jihad poses a significant challenge to the countries contending with ISIS in two principal respects. First, ISIS' use of cyberspace has dramatically lowered the obstacles to participation in the organization's activities and thereby eased the recruitment of additional operatives and the ideological support of its actions. A clear example of this is the case of Mehdi Masroor Biswas, an Indian hi-tech executive who operated the popular Twitter account @ShamiWitness. This account, which has more than 17,000 followers, openly supported ISIS and praised the foreign fighters who were killed in its ranks. After his exposure, Biswas said that he would have been glad to join ISIS himself, but since his family needs him, he did not leave his home and travel to Syria or Iraq.[19] In the current age of communication, anyone can support ISIS from a distance and thereby provide ideological support and public legitimacy to the organization – and ISIS thoroughly exploits this possibility.

Second, ISIS makes extensive and effective use of various social media platforms and optimally exploits the extensive decentralization in the current age of communication and the difficulty in preventing the circulation of information. Since ISIS messages spread through thousands of different accounts of individual users and not through one central website, it is nearly impossible to curb the dissemination of its contents. This understanding of the technological possibilities inherent in cyberspace allows ISIS significant freedom of action in disseminating propaganda, recruiting, and making contact with operatives and supporters, and complicates contending with the organization's message online. ISIS' extensive use of social media has led Robert Hannigan, head of the British intelligence organization GCHQ, to assert that this poses a tremendous challenge to government and intelligence agencies responsible for thwarting and fighting terrorism. Hannigan even described the internet and social networks as "the command and control network of choice for terrorists."[20]

In order to contend with the challenge of cyber jihad, different countries opt for one of two principal approaches: a technological battle against the online presence of ISIS, and the use of social media to disseminate counter-propaganda. According to proponents of the technological approach, in order to stem the use of social media by terrorist organizations, it is necessary to block access to online space by these organizations: close their Twitter and Facebook accounts, block users affiliated with terrorist organizations, and thereby deny ISIS and other terror organizations the option of exploiting these communication channels for their own purposes. As part of this effort, the French Minister of the Interior, Bernard Cazeneuve, visited Silicon Valley in February 2015 and met with representatives of technology companies to obtain their cooperation in combating ISIS's use of the internet.[21] This move was designed to allow governments to change the status quo, in which cyberspace constitutes an open and unregulated field.

While the desire to deny terrorist organizations the freedom of action on social media is understandable, the effectiveness of this solution is limited. Although social networks have recently adopted a censorship policy designed to prevent the dissemination of violent contents that encourage terrorism,[22] this censorship takes place only after the contents have been uploaded onto the various websites and social media accounts – and in many cases their removal occurs after hundreds of thousands of people have already viewed them. Therefore, this measure has an important but limited effect. Moreover, for every account that is closed, a number of new accounts are immediately opened in its place, so that it is impossible to completely prevent users from using social media for purposes of terrorism over time – unlike forums and websites, which can more readily be closed and disabled.

In contrast to the approach that advocates the suspension of accounts of users affiliated with terrorist organizations and thereby limit their influence on social media, another approach recognizes the influence of social media and seeks to take a more proactive line that would exploit this influence in favor of the struggle against these same terrorist organizations. This approach seeks to exploit cyber activity against ISIS, with the aim of influencing potential supporters of the organizations who are exposed to its content on social media. A prominent example of this approach is the US State Department's social media campaign, "ThinkAgainTurnAway." Through an official English-language campaign that began in December 2013[23] under the hashtag #ThinkAgainTurnAway,[24] the State Department is attempting to engage with the recruitment and propaganda efforts of ISIS on these channels and influence potential recruits and supporters of the organization. The campaign includes video clips, text messages, and images, and is active on the same platforms that ISIS uses to disseminate its content, i.e., YouTube, Facebook, Twitter, and Tumblr.[25] The campaign's content includes images of ISIS atrocities and testimonies of operatives who were active in the organization and were disillusioned by its extremism and brutal activities. The campaign thus attempts to counter the narrative that ISIS and other organizations promote online, and by that turn social media against them.

In conclusion, ISIS' cyber jihad activity has managed to create a powerful image for the organization in global public opinion, which has also affected the forces actually engaged in the fight against it. However, it appears that in recent months, the combined struggle against ISIS is managing to halt the momentum of its territorial conquests, primarily in Iraq and partially also in Syria. The organization lost its control of the city of Kobani in Syria and in Tikrit in Iraq, while in other areas its forces have been curbed by the Western-backed Kurds and by the Shiite militias. These physical achievements in the campaign against ISIS are vital to defeating the organization, but the struggle against ISIS must also take place online, where its cyber jihad activity continues in full force and extends its influence to regions outside the Middle East. This activity lures potential supporters to travel to the Islamic State territories in Iraq and especially Syria. This being the case, it is clear that the extensive and potent use that ISIS makes of cyberspace requires a widespread and targeted confrontation with the challenge, comprising an ideological response to its messages and a struggle to reduce its massive and effective presence on online social networks. Only such a combined confrontation, in addition to the targeted use of military force and an effort to discredit ISIS' ideological message and its methods of circulation together with technology companies, may help curb the ISIS phenomenon. Containing the territorial conquests of ISIS and reducing the appeal of the ideological message that it offers potential supporters are vital to curbing ISIS, both in cyberspace and in the "real," offline world.

Notes

[1] Office of the Press Secretary, "Remarks by the President in Closing of the Summit on Countering Violent Extremism," The White House, February 18, 2015.

[2] Muhammad bin Ahmad al-Salim, "39 Ways to Serve and Participate in Jihad," 2003, http://www.archive.org/stream/39WaysToServeAndParticipate/39WaysToServeAndParticipateInJihad_djvu.txt.

[3] Tumblr is a microblogging platform and social network that allows users to upload and share texts, images, and video files. The platform is particularly popular among young people and according to the site figures for February 2015, hosts 224.5 million blogs (personal online journals of users). See https://www.tumblr.com/about.

[4] Eric Schmitt, "U.S. Intensifies Effort to Blunt ISIS' Message," *New York Times*, February 16, 2015.

[5] J. M. Berger and Jonathan Morgan, "The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter," Brookings Project on U.S. Relations with the Islamic World, Analysis Paper No. 20, March 2015, http://www.brookings.edu/~/media/research/files/papers/2015/03/isis-twitter-census-berger-morgan/isis_twitter_census_berger_morgan.pdf.

[6] J. M. Berger, "How ISIS Games Twitter,*" The Atlantic*, June 16, 2014, http://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/.

[7] Hassan Mneimneh and Kanan Makiya, "Manual for a 'Raid,'" *New York Review of Books*, January 17, 2002.

[8] Spencer Ackerman, "US Central Command Twitter Account Hacked to Read 'I Love You Isis,'" *The Guardian*, January 12, 2015, http://www.theguardian.com/us-news/2015/jan/12/us-central-command-twitter-account-hacked-isis-cyber-attack; Russell Berman, "The Hacking of Central Command," *The Atlantic*, January 12, 2015, http://www.theatlantic.com/politics/archive/2015/01/central-command-accounts-are-hacked-centcom-isis-soldiers-obama-cybersecurity-cybercaliphate/384442/.

[9] "19,000 French Websites (and Counting) Hacked Since Charlie Hebdo Attack," *Newsweek*, January 15, 2015, http://www.newsweek.com/19000-french-websites-and-counting-hacked-charlie-hebdo-attack-299675.

[10] "Terror's New Headquarters: The Capture of Mosul," *The Economist*, June 14, 2014.

[11] Martin Chulov, "Isis Insurgents Seize Control of Iraqi City of Mosul," *The Guardian*, June 10, 2014, http://www.theguardian.com/world/2014/jun/10/iraq-sunni-insurgents-islamic-militants-seize-control-mosul.

[12] Jillian Kay Melchior, "Those Who Face Death," *National Review*, September 21, 2014, http://www.nationalreview.com/article/388505/those-who-face-death-jillian-kay-melchior; "ISIS Tactics Illustrate Social Media's New Place In Modern War," *TechCrunch*, October 15, 2014, http://techcrunch.com/2014/10/15/isis-tactics-illustrate-social-medias-new-place-in-modern-war/.

[13] Christine Petre, "The Jihadi Factory," *Foreign Policy*, March 20, 2015, http://foreignpolicy.com/2015/03/20/the-jihadi-factory-tunisia-isis-islamic-state-terrorism/.

[14] Examples of Tumblr pages of women who sympathize with ISIS are: http://Al-khanssa.tumblr.com; http://fa-tubalilghuraba.tumblr.com.

15 "Foreign Fighter Total in Syria/Iraq Now Exceeds 20,000; Surpasses Afghanistan Conflict in the 1980s," International Center for the Study of Radicalization and Political Violence (ICSR), January 26, 2015, http://icsr.info/2015/01/foreign-fighter-total-syriairaq-now-exceeds-20000-surpasses-afghanistan-conflict-1980s/.

16 Kathy Gilsinan, "Is ISIS's Social-Media Power Exaggerated?" *The Atlantic*, February 23, 2015, http://www.theatlantic.com/international/archive/2015/02/is-isiss-social-media-power-exaggerated/385726/.

17 *Hijrah to the Islamic Stat* , https://archive.org/stream/GuideBookHijrah2015-ToTheIslamicState/7-Hijrah2015-ToTheIslamicState_djvu.txt/.

18 "ISIS Produces a Promotional Video to Promote Lone Wolf Terrorist Attacks on the U.S., Canada and Europe," Shoebat Foundation, February 21, 2015, http://shoebat.com/2015/02/21/isis-produces-promotional-video-promote-lone-wolf-terrorist-attacks-u-s-canada-europe/.

19 "Unmasked: The Man behind Top Islamic State Twitter Account," *Channel 4*, December 11, 2014, http://www.channel4.com/news/unmasked-the-man-behind-top-islamic-state-twitter-account-shami-witness-mehdi.

20 Robert Hannigan, "The Web is a Terrorist's Command-and-Control Network of Choice," *Financial Times*, November 3, 2014, http://www.ft.com/intl/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3QhKyjb33.

21 "France Seeks Silicon Valley Allies in War on Terror," *France 24*, February 21, 2015, http://www.france24.com/en/20150221-france-seeks-silicon-valley-allies-war-terror/?aef_campaign_date=2015-02-21&aef_campaign_ref=partage_aef&dlvrit=66745&ns_campaign=reseaux_sociaux&ns_linkname=editorial&ns_mchannel=social&ns_source=twitter.

22 J. M. Berger, "The Evolution of Terrorist Propaganda: The Paris Attack and Social Media," Brookings, January 27, 2015, htt p://www.brookings.edu/research/testimony/2015/01/27-terrorist-propaganda-social-media-berger.

23 The English campaign was preceded by similar attempts in Arabic and in Urdu, which have been active since 2011. See Matt Hansen, "State Department Combats Islamic State Recruitment via Social Media," *Los Angeles Times*, September 6, 2014, http://www.latimes.com/nation/nationnow/la-na-state-department-islamic-social-media-20140906-story.html.

24 Eric Schmitt, "A U.S. Reply, in English, to Terrorists' Online Lure," *New York Times*, December 4, 2013, http://www.nytimes.com/2013/12/05/world/middleeast/us-aims-to-blunt-terrorist-recruiting-of-english-speakers.html.

25 See https://www.youtube.com/user/ThinkAgainTurnAway; https://twitter.com/thinkagain_dos; http://thinkagainturnaway.tumblr.com/; https://www.facebook.com/ThinkAgainTurnAway.