Butler Journal of Undergraduate Research

Volume 6

2020

Cyber Jihadism: An Analysis on How the Cyber Sphere Has Altered Islamic Terrorism

Simon Spangenberg
University of New Mexico

CYBER JIHADISM: AN ANALYSIS OF HOW THE CYBERSPHERE HAS ALTERED ISLAMIC TERRORISM

SIMON SPANGENBERG, UNIVERSITY OF NEW MEXICO
MENTOR: MARIE VASEK

Between 2011 and 2015, more than 30,000 foreigners, including more than 4,000 Westerners, have joined the ranks of ISIS in the Syrian conflict (Schmitt & Sengupta, 2015). Between 2000 and 2018, 91% of the total victims of terror attacks in Europe were accounted for by Islamic terrorists, causing a total of 753 fatalities in that time frame (Le Figaro, 2019). Numerous studies have statistically demonstrated a continuous surge of new recruits in Islamic terrorist groups such as ISIS since the beginning of the millennium. Carter, Maher, and Neumann (2014) attribute this trend to the expansion of technological possibilities in the cybersphere. They claim that the conflict in Syria is arguably one of the first live-documented conflicts on social media and video streaming platforms: "In the minds of the foreign fighters, social media is no longer virtual: it has become an essential facet of what happens on the ground" (Carter et al., 2014, p. 1). Propaganda and recruitment encompass only a portion of the online Islamic extremism threat, however. Training also represents a significant role that Islamic terrorism has on the cybersphere (Pawlak, 2015). Digital tools are increasingly used to train foreign recruits. This is most prominently illustrated by the Al-Qaeda-created online magazine *Inspire*, which led to the making of two bombs that killed three and injured approximately 300 in the Boston Marathon in April 2015 (Lemieux, Brachman, Levitt & Wood, 2014). In this paper, we review and analyze the three above-mentioned major components of online Jihad: propaganda, recruitment, and training. Through related work, we propose a formal description and explanation for the reasons of past superiority of online Islamic terrorism.

The fight against Islamic terrorism is extremely complex and requires historical understanding of the roots of current conflicts in the Middle East. Understanding why new recruits join the ranks of Islamic terrorist groups is crucial for efficiently fighting online terrorism (Rosenblatt, 2019); thus, we provide a brief historical review of ongoing conflicts in the Middle East and the emergence of radical groups.

Although fighting online terrorism is often neglected, the need to do so is at an all-time high. Overlooking this necessity has undeniably contributed to the

recent surge of attacks and has perpetuated the formation of powerful groups such as Al-Qaeda and ISIS (General Intelligence and Security Service, 2012). Although most nations, organizations, and even independent hacking groups called "hacktivists" have considerably increased their attention toward online terrorism, a significant amount still needs to be done to gain the upper hand in the online war of terror (Ghost Security, 2015). Brantly (2017) notices that a significant challenge faced by nation-states and governments lies in the innovation and adaptation of extremist groups' digital security. In this paper, we discuss several methods to surveil and fight online terrorism. We identify challenges and promising aspects concerning the future of the fight against online terrorism. Finally, we offer a model of potential future threat landscapes related to Islamic radicalization in the cybersphere.

Background and Definitions

Islamic Terrorism Terminology and Definitions

Terrorism can be defined as the systematic use of violence to achieve political objectives. It is a tactical asymmetric fight to compensate for the incapacity of the weak to win over a stronger state opponent. Islamic terrorism includes a strong religious component derived from an extreme interpretation of the Quran, Sharia law, and various Hadiths, in which Islamic supremacy (i.e., establishment of a new worldwide Islamic caliphate) is viewed as the ultimate goal.[1] This goal is attained by conducting a *Jihad* (literally translated as "struggle" or "striving"), or holy war, against unbelievers (*kafir*). Islamic terrorism takes different forms and has multiple roots and origins going as far back as the 11th century CE.

Historical Review

To gain support from Arabic movements during World War I and to help defeat the Ottoman Empire, France and the United Kingdom promised to support the creation of an Arabic state after the war ended. Simultaneously, the British government issued the so-called Balfour Declaration supporting the establishment of "a national home for Jewish people" in Palestine (Kepel, 2004). After the fall of the Ottoman Empire, France and the United Kingdom betrayed their promise by secretly agreeing to partition the Arabic territories of the former Ottoman Empire under their respective colonial control. The period between World Wars I and II is consequentially characterized by the emergence of an Arabic nationalism and Islamism as well as by the development of Zionism (via different waves of

migration of Jewish people in Palestine). After World War II, the important oil resources of the region became a major component of the subsequent Cold War between the Soviet Union and the United States. The creation of Israel in 1948 ignited the war between the new Jewish state and its Arabic neighbors in support of the Palestinian people. This period was dominated largely by Palestinian terrorism.

An important development is the change of power in Iran in 1979 with the arrival of Ayatollah Khomeini. For the first time in the region, an Islamic Shia state was created, which introduced a new form of Islamic terrorism against Western states. Concurrently, the Soviet invasion of Afghanistan constituted a turning point in the development of modern Islamic terrorism. Weakened by the fall of the Shah in Iran, the United States would not allow the creation of a USSR satellite state in the region. Together with Saudi Arabia, the United States started supporting Muslim opponents and Afghan mujahideen (Islamic fighters) factions. The withdrawal from Afghanistan in 1989 resulted in the fall of the Soviet Union and the end of the Cold War. During the following years of civil war in Afghanistan, different Islamic groups were trained with the intention of exporting their newly gained skills to other parts of the world (notably Algeria, Bosnia, and Chechnya). Not gaining enough recognition, some groups—Al-Qaeda in particular—turned to global terrorism, September 11 being the most representative moment of this evolution.

The succeeding "War on Terror" on countries associated with Al-Qaeda, along with the killing of Abu Abdallah Usama bin Laden, has reduced the influence of this movement but has also given rise to a new and more violent group called ISIS/ISIL. In 2014, ISIS/ISIL, led by Abu Bakr al-Baghdadi, established a caliphate over a significant part of Iraq and Syria. During this period, the Islamic group conducted terrorist attacks on numerous countries, particularly in Europe (Paris, Brussels, Nice, London, Stockholm, etc.).

Online Jihad

The use of the online sphere as a platform for Jihad is endemic to Islamic terrorism and has exponentially increased in the past decade (Brantly, 2017). In 2005, Ayman al-Zawahiri (2nd General Emir of Al-Qaeda) openly denoted the media to be an inclusive part of the battlefield (Carter et al., 2014). Terrorist groups have successfully learned to use complex online tools that ensure anonymity and protection to communicate and coordinate their affairs. We recognize the materialization of this development through three main fundamentals: propaganda,

recruitment, and training. For each of these points, we identify several attack vectors exploited by Islamic terrorists, which have contributed to their ascendance in the online war of terror.

Propaganda

Based on related work, we detect a number of tools used by jihadists as means for diffusing motivational material, such as social media, media centers, online magazines, and video games. From the infamous video of American hostage Nick Berg's beheading by Abu Musab al-Zarqawi in 2004, to the use of social media and the creation of online magazines, Islamic extremists have exploited many different techniques to rally individuals to their cause. For instance, as Pawlak (2015) notes, Al-Qaeda has "openly encouraged cyber Jihad as a sacred duty of every Muslim and called upon its followers to hack western websites" (p. 1). This call has quickly been answered by a prominent British-Islamic figure called Abu Hussain al-Britani, also known as "TriCk," most notorious for hacking Tony Blair's account and joining the ranks of ISIL in 2013. Jihadi groups have quickly understood the influence of social media. Platforms such as Twitter, Facebook, and Instagram have allowed jihadists to share and promote their views. Berger and Morgan (2015) estimate that in September 2014, between 46,000 and 70,000 Twitter accounts were linked to ISIS. Several of these profiles reached thousands of followers, one particular example being the ISIS-affiliated Twitter account @reyardiraq, with more than 90,000 followers (Brantly, 2017).

Social media is also used as an outlet for newly emerged centralized media centers such as "al-Hayat," "al-Sahab," and "al-Furquan." These media centers often exhibit well-edited Islamic propaganda videos, using advanced technological cameras and drones to depict often severely contrasted sceneries. For instance, amongst the shocking films of beheadings, ISIS has crafted impressive video series such as *Harvest of the Soldiers*, which include almost weekly releases and updates of pure military advertising material (Zelin, 2019). The Islamic State (ISIS/ISIL) often contrasts its videos of strength and violence with displays of peace, happiness, and prosperity in its controlled cities. ISIS's efforts to portray a form of utopia to undermine the humanitarian crisis occurring in its occupied cities is verified through a study led by Tarabay, Shiloach, Weiss, and Gilat (2015), in which the authors found that 45% of the Islamic State's propaganda focuses on its endeavors to build and sustain the caliphate by portraying hospitals, charity work, agricultural projects, and roadworks.

Media outlets and forums have also allowed terrorist groups to publish new types of propaganda material, such as online magazines and video games (Al-Rawi, 2016). One of the most notorious examples is Al-Qaeda's online magazine *Inspire*, thought to be the work of English-speaking jihadi Anwar al-Awlaki, also known as the "bin Laden of the Internet" ("Online Preachers," 2011). Figure 1 depicts instructions given in the magazine relating to propaganda and wide distribution of the media.

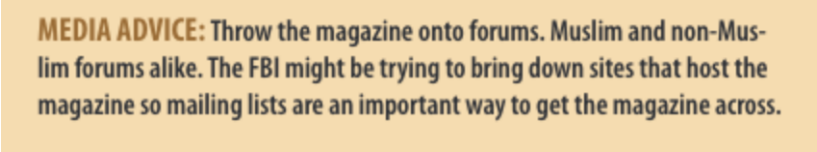

Figure 1. Propaganda message given in the eighth issue of Al-Qaeda's online magazine Inspire (Zelin, 2019).

For the first time, Islamic extremist groups have implemented impressive technological tools to modernize their propaganda campaigns. As established in a study led by Al-Rawi (2016), groups such as ISIS base most of their marketing strategies on emphasizing simple ideological appeals,[2] greatly facilitated through the use of the cybersphere. Islamic terrorists build their media strategies on three main traits, as explained by Haroro J. Ingram (2014): the use of multidimensional and multiplatform approaches to instantaneously target individuals and enhance the scope and importance of messaging; the organization of narratives and deeds to amplify operational and strategic outcomes in the field; and the centrality of the Islamic State brand.

Recruitment

Patryk Pawlak (2015) notes that "the internet has not only altered traditional channels for radicalization and facilitated a two-way communication between terrorist organizations and their supporters, but also allowed for a change in planning, coordination and execution of attacks" (p. 1). The distribution of propaganda through social media is only the first step toward successful radicalization and recruitment (Al-Rawi, 2016). Jihadists tend to distrust platforms for direct communication and rely on more developed digital operational security (OPSEC) techniques to target specific individuals (Brantly, 2017). As soon as the first contacts have been made, jihadists rely on mobile messaging applications like Viber, Telegram, and Redphone to directly communicate with their potential

targets. Brantly (2017) observes in his study that high levels of online "safeguarding" are required for a potential recruit to make his way into terrorist groups. Through the analysis of thousands of posts in forums and social media, Brantly establishes a list of communication tools that are either positively or negatively regarded by extremists. The list of applications that are considered "safe to use" by jihadists includes but is not restricted to Signal, Linphone, Vimeo, Gmail, and Telegram. Unsafe tools include Skype, iCloud, and Tor Mail. A strong recognition is made on the Silent Phase software, which is often considered to offer "secure solutions for voice, browsing and messaging" (p. 91).

ISIS also regularly uses video games as a measure to radicalize younger individuals. Shooting game *Arma 3* includes a specific ISIS mod,[3] easily accessible via online download (Scimeca, 2015). In addition, an adaptation of *Grand Theft Auto V* called "Salil al-Sawarem" (The Clanging of the Swords) was popularized in 2014. In this adaptation, the user takes control of a jihadist in his struggle to restore the caliphate and combat the infidels. Such means are clearly intended to target a younger set of individuals and idealize the daily life of an Islamic fighter. Al-Rawi (2016) notes that with high-definition video games and entertaining missions, the user is lured into believing that ISIS is a technologically advanced group fighting for genuine and authentic beliefs. Finally, ISIS also introduced a self-made Android application available for free download on the Google Store. "Dawn of the Glad Tidings" was a Twitter-based application that automatically posted ISIS-related tweets on the user's account. Although the lifetime of this application was quite limited, Berger and Morgan (2015) and Stern and Berger (2016) noted that the application reached a peak of 40,000 tweets a day.

Training

Through the expansion of the online sphere, jihadists have rapidly discovered that the Internet is not only a place for radicalization, recruitment, and propaganda but also for knowledge sharing. In this section, we recognize two main attack vectors used by Islamic groups to train recruits in the cybersphere: digital protection vectors and military threat vectors.

Digital Protection Vectors

Most of the general techniques required to maintain anonymity and privacy over the Internet are not generally known by the average user. Developing some techniques to preserve online security requires a minimum amount of training,

which, as Brantly (2017) notes, is often promoted by social media accounts linked to terrorist groups. For instance, the Telegram account @Software_ENG, also named Tiqani al-Dawlah al-Islamiyyah,[4] has been known to post hundreds of training documents on forums and websites linked to implementing strong digital OPSEC techniques. Another instance is depicted by Mula'ib al-Assina's response to a question related to the use of Skype through Tor on the Minbar forum: "Skype is insecure, and Americans are recording every single call since 2008" (Brantly, 2017, p. 86). It is important to note that most of the material covered and questions asked on such platforms are quite trivial and do not dig deep into digital operational security. Nevertheless, such activity clearly indicates a high interest and concern from jihadists about digital OPSEC and illustrates that the online sphere and cybersecurity techniques have become a crucial asset for their operations.

Military Threat Vectors

The emergence of certain media outlets and online document-sharing platforms has allowed the creation of so-called do-it-yourself terrorism (Pawlak, 2015). This modern practice of Jihad is most prominently illustrated through online journals and magazines released in several volumes by groups such as Al-Qaeda and ISIS. Al-Qaeda is one of the first groups to release easy-to-access online training documents, like the journal *al-Battar*,[5] which served predominantly as a virtual training camp, encouraging weapons of mass destruction and teaching explosive handling and kidnapping techniques, amongst many others (Cohen-Almagor, 2016). A more notorious example of Al-Qaeda's online training tools relates to the 17-volume online magazine *Inspire*. *Inspire* became influent throughout the world as it was fully aimed at English readership (i.e., Western recruits). Studying the influence of *Inspire*, Lemieux et al. (2014) note that the magazine seems to target a "less intellectually engaged audience" around the world, particularly in Australia, the United Kingdom, and the United States. Lemieux et al. (2014) also note that one of the reasons for the magazine's infamy relates to the "Open Source Jihad" section. This section of *Inspire* covers in great detail a variety of skills to learn—from weapon handling to bomb making—and was allegedly used by Dzhokhar Tsarnaev and his brother, Tamerlan, in the 2013 Boston Marathon bombings. Figure 2 illustrates an extract from the step-by-step process of making an acetone peroxide bomb in the "Open Source Jihad" section of *Inspire*'s sixth volume. The primary explosive material used in the Paris and Brussels bombings was triacetone triperoxide, a trimer form of the mixture of acetone and hydrogen peroxide (Alfred, 2016). The aforementioned arguments clearly illustrate the fact

that today, to pursue Jihad, modern terrorists require only a sufficient Internet connection.

FIGURE 1.0
All of the parts you will be required to have are shown. What is not shown here is that you can choose to have any kind of dropper for the experiment.

sodium carbonate solution
acetone
filter paper
sodium carbonate
sulfuric acid
jug
hydrogen peroxide
beaker
cold bath
thermometer
pH paper
FIGURE 1.0

REMEMBER
To make sodium carbonate solution, mix sodium carbonate with water as shown in step 7.

IMPORTANT
Make sure to wear your safety gear that includes gloves and goggles. If your hair is long, tie it back. If any of the chemicals get on your hands, make sure to wash it off immediately. After you're done with the experiment, wash the entire area and the items thoroughly.

HINT

For extra precaution, keep large chunks of ice in the cold bath so as to maintain the cold temperature.

TABLE 1.1
The rule is to use 6 times as much the quantity of pure acetone with its equivalent pure H_2O_2.

Preparation:

The rule is to use 6 times as much the quantity of pure acetone with its equivalent pure H_2O_2. So if you are using 20ml 100% H_2O_2, you would add to it 120ml 100% acetone. The acid is added to facilitate the reaction.

So for 3% H_2O_2: Use 50ml H_2O_2 + 9ml acetone + 10-20ml Sulfuric acid. See Table 1.1 below for details.

You will need a glass beaker, ice cold water (cold bath) and a thermometer.

1. Add the needed amount of acetone according to the concentration of the H_2O_2 as seen in Figure 1.1. Refer to Table 1.1 for the method of pouring.
2. Pour H_2O_2 into a beaker.

FIGURE 1.1

FIGURE 1.2

Ingredients in ml	3% H_2O_2	6% H_2O_2	18% H_2O_2	30% H_2O_2
H_2O_2	50ml	50ml	50ml	50ml
Acetone	9ml	18ml	54ml	90ml
Sulfuric acid*	10-20ml	20ml	20ml	20ml

Table 1.1

*The quantities above are for 98% sulfuric acid. If you are using a weaker concentration, increase the amount of acid. You may also substitute sulfuric acid for hydrochloric acid.

Inspire | Al-Malahem Media

42

Figure 2. Extract from the step-by-step procedure of the making of an acetone peroxide bomb. This figure appeared in the sixth issue of Al-Qaeda's online magazine Inspire and was part of the "Open Source Jihad" section (Zelin, 2019). For security purposes, the rest of the instructions have been omitted here.

The Fight against Online Islamic Terrorism

Since the early 2010s, the threat of online terrorism has become publicly acknowledged and many entities have significantly increased their digital counterterrorism measures. To analyze the fight against online Islamic terrorism, we focus our research on three main actors: governments and international organizations, companies, and independent groups. For each of these groups, we discuss policies and measures taken to tackle online terrorism. We also consider newly emerging groups that have considerably helped nation-states improve their trailing position in the online war of terror.

Governments and International Organizations

The international coalition against online terrorism is structured around three main pillars: "constraining the use of the internet by jihadi organizations," "strengthening de-radicalization efforts," and "limiting access to funding" (Pawlak, 2015, p. 2). Nation-states' efforts to combat online terrorism via several platforms have drastically amplified over past years. Initial government responses included social media campaigns[6] and unsuccessful countermessaging techniques ("Digital Counterterrorism," 2018). Although many of these attempts have been unable to compete against the propaganda tactics implemented by jihadists so far, international initiatives continue to grow and challenge the spread of online terrorism.

Many nation-states recognized that cutting Islamic extremist groups' financing would ultimately result in those groups' extinction. This led to the 2015 UN Resolution 2199, which condemns any form of trade associated with groups such as Al-Qaeda ("Unanimously Adopting," 2015). A few government initiatives and offensive responses to Islamic terrorism have proven successful, however. For instance, in 2016, the National Security Agency and the United States Cyber Command successfully conducted a joint offensive operation called Glowing Symphony, with the purpose to disrupt and deny ISIS's ability to coordinate and conduct attacks against the United States and its allies (Martelle, 2018). This operation is considered one of the most significant and successful cyber offensive operations undertaken by the United States.

Companies

A most recent initiative, called the Christchurch Call, led by New Zealand's prime minister Jacinda Ardern and French president Emmanuel Macron, aims to encourage all major tech companies to eliminate any form of terrorism and violent extremist content online (Roy, 2019). Major companies are playing a crucial role in the fight against cyber Jihad. As most of the propaganda content flows through social media, many of these companies recognize the fight against online extremism as a responsibility and a duty. In 2015, Twitter announced the suspension of 10,000 ISIS-linked accounts in one day (Gladstone, 2015). Two years later, YouTube announced the removal of the lectures and sermons of prominent Islamic preacher Anwar al-Awlaki (Wallace & Townsend, 2017). Furthermore, Google's recent Jigsaw Project presents a modern face in combatting Islamic propaganda and dismantling extremism networks. This project aims to be "a platform for former violent extremists to collaborate, in order to prevent young people from joining extremism groups" ("Jigsaw," n.d).

Independent Groups

The rise in online Islamic terrorism has also resulted in the enlisting of independent hacking groups, also called hacktivists. Following the Paris Charlie Hebdo attacks in 2015, hacktivist group Anonymous publicly declared war on ISIS through the #OpISIS campaign and removed 20,000 ISIS-related Twitter accounts (Rogers, 2015). Another prominent group engaged in the battle against cyberterrorism is Ghost Security Group. To date, Ghost Security Group claims to have identified more than 100,000 extremist social media accounts used primarily for recruitment, and to monitor more than 200 known violent extremist websites ("Ghost Security," n.d).

Ways Forward

Beyond a more stringent international and national legal order and the effective involvement of online platforms and social media, the increasing level of threat sophistication of the cybersphere and its mastering by terrorist groups require constant adaptation. Since the 2013 Snowden leaks, companies have significantly increased their use of robust encryption methods in their consumer-communication technologies, which has strongly challenged authorities to efficiently track terrorists online ("Digital Counterterrorism," 2018). Brantly (2017) described the necessity behind jihadists' adaptation and innovation on current online

technologies. Strong digital OPSEC has become a vital need for groups such as Al-Qaeda and ISIS to exist. It is therefore natural to assume that the future war on terror will occur mainly online. Social media and forums are only a small part of the danger that Islamic terrorist groups represent, and as technological means expand, so does the jihadi threat landscape.

Recent findings and developments seem to suggest that artificial intelligence will become a major asset for tracking, monitoring, and surveilling Islamic extremism activities on the Internet. According to a report published by the Capgemini Research Institute, 56% of 850 surveyed senior executives in cybersecurity claim that their security analysts are overwhelmed by the increasingly sophisticated threat levels (Tolido, Van Der Linden, Thieullent, & Frank, 2019). The need to further incorporate automation and artificial intelligence as tools for detection and response to cyber threats has become crucial. Through the development of machine learning and data-mining algorithms, companies and public authorities could potentially classify data collected from past attacks to model trends that would determine high-risk scenarios and prevent future attacks (Beuchelt, 2020). Beuchelt (2020) notes that, "using temporal analytics as well as structured and unstructured data analysis and integration, companies can build complex social media and other open source intelligence models to predict future attacks" (para. 10). Counter Extremism Project's eGlyph technology and Google's recent Jigsaw Project both illustrate new types of automated mass-tracking algorithms, which, if used properly, could lead to astonishing positive results ("How CEP's eGLYPH Technology Works," 2016).

Link analysis (defined as a method to evaluate relationships between nodes in a network) is an interesting technique used to study information surrounding high-stake targets (Carafano, 2005). This method could allow efficient large-scale analysis of a suspect's relationships as well as his or her links to a terrorist organization. All of the aforementioned implementations, however, require a significant dependence on available and structured data. Although the fields of machine learning, data mining, and data analysis are exponentially growing, they still face challenges when trying to process natural languages or when manipulating nonstructured data such as images, text mixtures, videos, and sensor information (Carafano, 2005).

Online security is often considered a "cat and mouse" game. As security strengthens, so do threats and attacks. Although artificial intelligence and data-analysis algorithms could be used to secure systems and fight online terrorism, these techniques could also be used by Islamic terrorists to widen their online range

and social-engineering techniques. For instance, artificial intelligence could be deployed to enhance terrorists' online propaganda campaigns by implementing an algorithm that sends tweets faster and with a higher success rate than a human could (Tolido et al., 2019). The need to recognize that the threat vectors of terrorist attacks will drastically change in the future is of paramount importance ("Cyberterrorism," 2009). Because of the interconnectivity revolution of the past few decades, critical infrastructures such as hospitals, power plants (specifically nuclear plants), transportation infrastructures, and banks are prone to becoming terrorists' next targets of value. There is no definite answer to ensure protection against terrorist threats in the cybersphere, but cooperation and intelligence sharing will be critical for the containment of such threats (Collins, n.d).

The need for public and law enforcement authorities to design adequate and reactive cross-border cooperation tools has been highlighted by the European Union after the series of terrorist attacks that hit a number of its member states in 2015 and 2016. In September 2018, the European Commission adopted a legislative proposal on "preventing the dissemination of terrorist content online" (European Commission, 2018). The regulation introduces a removal order that can be issued as an administrative or judicial decision by a competent authority in a member state. In such cases, the hosting service provider is obliged to remove the content or to disable access to the content within one hour. The regulation requires hosting service providers, where appropriate, to take proactive measures proportionate to the level of risk and to remove terrorist material from their services, including through the deployment of automated detection tools. Failure to act within an hour after a removal order has been placed by a member state could result in fines of up to 4% of the hosting service provider's annual revenue ("European Parliament," 2019).

Opponents of this proposal—such as Tim Berners-Lee, founder of the World Wide Web—claim that the proposed regulation is an attack on freedom of speech and would impair the Internet in Europe without strengthening the fight against online terrorism (Baker, Berners-Lee & Cerf, 2019). The proposal is still in discussion between the European Union's colegislators because of concerns expressed by the European Parliament about possible abuses of removal orders and restriction of freedom of speech (Creighton, 2019).

Despite these criticisms, adoption of the regulation could represent a major milestone in the fight against online Islamic terrorism. Lucinda Creighton (2019), Senior Advisor at the Counter Extremism Project, explained: "Of the 1.5 million videos of the attack in Christchurch, New Zealand, that were detected and

eventually removed by Facebook, only 1.2 million were screened and blocked by Facebook's software before being uploaded. This left 300,000 videos uploaded to the platform for users to see" (para. 2).

The way companies and public authorities shape new regulations and approach technical advancements will undoubtedly be crucial for the future of online counterterrorism. Collins (n.d) argues that the way we approach online counterterrorism must change, as we need to adapt to new rules, new technologies, and new players. Ultimately, technical developments and legal frameworks will need to properly balance public security needs with freedom of speech and individual data-protection requirements.

Conclusion

In this paper, we have provided a cohesive narrative of the way Islamic terrorists use the cybersphere to conduct their Jihad and how nation-states have reacted to the threat posed by such groups. We have selectively reviewed online methods used by Islamic groups in the "Online Jihad" section by analyzing three key components to their success—namely propaganda, recruitment, and training. Our analysis illustrates that Islamic terrorist groups' influence over the cybersphere is as significant as it has ever been and has undeniably led to major attacks over the past decade. Our findings also indicate that Islamic groups were evidently leading the online war of terror over the past few years as most nation-states failed to recognize the online threat that Islamic extremism represents.

We then focused our study on ways in which the fight against online terrorism is conducted, in the section called "The Fight against Online Islamic Terrorism," by identifying three major attack vectors: governments and international organizations, companies, and independent groups. Our findings suggest that international response to online jihadism has significantly increased over the past decade, considerably decreasing the gap between nation-states and terrorist groups in the cybersphere.

Finally, we have identified, in the section "Ways Forward," several challenges and threats that online terrorism will pose in the future. Although findings and newly built tools to counter online terrorism offer reason for optimism, new threats emerge at a similar rate through the expansion of technological advancement. Future work will have to efficiently recognize the importance of cybersecurity related to the online war of terror and the impact that neglecting it has had on the world. Containing online resources that advance terrorism is an

increasingly critical task, since a simple video, a brief message, or a single tweet could represent an individual's turning point between peace and terrorism.

Notes

[1] It is important to note that Islamic terrorism is based on a radical interpretation of the Quran that is, in general, not representative of the Islamic religion. The term "Islamic terrorism" is highly politicized and should by no means serve as a reference to Islamic tradition. It is used throughout this article exclusively as a means to describe violent groups who claim religious motivations behind their attacks.

[2] One example includes the use of a black banner. The black banner contains many different Islamic references. For instance, it is assumed that a black banner was used when Abu Muslim led the Abbasid Revolution in 747 CE.

[3] Video game mods are defined as "short modifications" of the game by external parties such as fans or players.

[4] Also known as Islamic State Tech.

[5] Also known as *The Sharp-Edged Sword*.

[6] One notable example relates to the "Think Again Turn Away" social media campaign, launched by the US Department of State, which accumulated a modest 44,000 followers on Twitter and Facebook combined (General Intelligence and Security Service, 2012).

References

Alfred, C. (2016, March 23). What the bombs used in Brussels reveal about the attacks. *Huffington Post.* Retrieved from https://www.huffpost.com/entry/bombs-brussels-attacks_n_56f2a25fe4b0c3ef52174c1d

Al-Rawi, A. (2016). Video games, terrorism, and ISIS's Jihad 3.0. *Terrorism and Political Violence*, *30*(4), 740–760. doi:10.1080/09546553.2016.1207633

Baker, M., Berners-Lee, T., & Cerf, V. (2019). EU terrorist content regulation will damage the internet in Europe without meaningfully contributing to the fight against terrorism. *Politco*. Retrieved from https://www.politico.eu/wp-content/uploads/2019/04/TCO-letter-to-rapporteurs.pdf

Berger, J. M., & Morgan, J. (2015, March). The ISIS Twitter census: Defining and describing the population of ISIS supporters on Twitter. *The Brookings Project on U.S. Relations with the Islamic World*, *20*. Retrieved https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf

Beuchelt, G. (2020, February 6). Opinion: AI and machine learning will power both cyber offense and defense in 2020. *Security Ledger.* Retrieved from https://securityledger.com/2020/02/opinion-ai-and-machine-learning-will-power-both-cyber-offense-and-defense-in-2020/

Brantly, A. (2017). Innovation and adaptation in jihadist digital security. *Survival*, *59*(1), 79–102. doi:10.1080/00396338.2017.1282678

Carafano, J. (2005, June 6). The future of anti-terrorism technologies. Retrieved from https://www.heritage.org/homeland-security/report/the-future-anti-terrorism-technologies

Carter, J. A., Maher, S., & Neumann, P. R. (2014). *#Greenbirds: Measuring importance and influence in Syrian foreign fighter networks.* Retrieved from the International Centre for the Study of Radicalisation and Political Violence website: https://icsr.info/wp-content/uploads/2014/04/ICSR-Report-Greenbirds-Measuring-Importance-and-Infleunce-in-Syrian-Foreign-Fighter-Networks.pdf

Cohen-Almagor, R. (2016). Jihad online: How do terrorists use the internet? In F. C. Freire, X. R. Araujo, V. A. Martinez, & X. L. Garcia (Eds.), *Advances in Intelligent Systems and Computing: Vol. 503. Media and metamedia management* (pp. 55–66). doi:10.1007/978-3-319-46068-0_8

Collins, B. C. (n.d.). The future of cyberterrorism: Where the physical and virtual worlds converge. Retrieved from http://www.crime-research.org/library/Cyberter.htm

Creighton, L. (2019, December 13). We need to stop pretending that we do enough to curtail terrorists' online influence. Retrieved from https://www.euronews.com/2019/12/13/we-need-to-stop-pretending-that-we-do-enough-to-curtail-terrorists-online-influence-view

Cyberterrorism: A look into the future. (2009). *Infosecurity*, *6*(6), 34–37. doi:10.1016/s1742-6847(09)70018-7

Digital counterterrorism: Fighting jihadists online. (2018, March 9). Retrieved from https://bipartisanpolicy.org/report/digital-counterterrorism-fighting-jihadists-online/

European Commission. (2018, September 12). Proposal for a regulation of the European Parliament and of the council on preventing the dissemination of terrorist content online. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0640&from=EN

European Parliament approves amendments to draft "terrorist content" legislation. (2019, April 24). Retrieved from https://www.perkinscoie.com/en/news-insights/european-parliament-approves-amendments-to-draft-terrorist-content-legislation.html

General Intelligence and Security Service. (2012, January). *Jihadism on the Web: A breeding ground for Jihad in the modern age*. Ministry of the Interior and Kingdom Relations of the Netherlands.

Ghost Security Group. (n.d.). Retrieved from https://ghostsecuritygroup.com/.

Ghost Security Group: 'Spying' on Islamic State instead of hacking them. (2015, November 23). BBC Trending. Retrieved from https://www.bbc.com/news/blogs-trending-34879990

Gladstone, R. (2015, April 10). Twitter says it suspended 10,000 ISIS-linked accounts in one day. *New York Times.* Retrieved from https://www.nytimes.com/2015/04/10/world/middleeast/twitter-says-it-suspended-10000-isis-linked-accounts-in-one-day.html

How CEP's eGLYPH technology works [video]. (2016, December 8). Retrieved from https://www.counterextremism.com/video/how-ceps-eglyph-technology-works

Ingram, H. J. (2014). Three traits of the Islamic State's information warfare. *The RUSI Journal*, *159*(6), 4–11. doi:10.1080/03071847.2014.990810

Jigsaw. (n.d.). Retrieved from https://jigsaw.google.com/projects/#against-violent-extremism-network

Kepel, G. (2004, December). Le terrorisme islamiste est né en Afghanistan. Retrieved from https://www.lhistoire.fr/«-le-terrorisme-islamiste-est-né-en-afghanistan-»

Le Figaro with AFP. (2019, March 5). Publication d'un "livre blanc et noir du terrorisme en Europe." Retrieved from http://www.lefigaro.fr/flash-actu/2019/03/05/97001-20190305FILWWW00190-publication-d-un-livre-blanc-et-noir-du-terrorisme-en-europe.php?redirect_premium

Lemieux, A. F., Brachman, J. M., Levitt, J., & Wood, J. (2014). InspireMagazine: A critical analysis of its significance and potential impact through the lens of the information, motivation, and behavioral skills model. *Terrorism and Political Violence*, *26*(2), 354–371. doi:10.1080/09546553.2013.828604

Martelle, M. (Ed.). (2018, August 13). Joint Task Force ARES and Operation GLOWING SYMPHONY: Cyber Command's Internet war against ISIL. Retrieved from https://nsarchive.gwu.edu/briefing-book/cyber-vault/2018-08-13/joint-task-force-ares-operation-glowing-symphony-cyber-commands-internet-war-against-isil

Online preachers of hate: Anwar al-Awlaki, "bin Laden of the internet." (2011, June 7). *Telegraph.* Retrieved from https://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8560438/Online-preachers-of-hate-Anwar-al-Awlaki-bin-Laden-of-the-internet.html

Pawlak, P. (2015). Cybersecurity: Jihadism and the Internet. *At a Glance*. Retrieved from http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_ATA(2015)557006

Rogers, K. (2015, November 25). Anonymous hackers fight ISIS but reactions are mixed. *New York Times*. Retrieved from https://www.nytimes.com/2015/11/26/world/europe/anonymous-hackers-fight-isis-but-reactions-are-mixed.html

Rosenblatt, N. (2019). All Jihad is local. Retrieved from https://www.newamerica.org/international-security/policy-papers/all-jihad-is-local/

Roy, E. A. (2019, April 24). "No right to livestream murder": Ardern leads push against online terror content. *Guardian*. Retrieved from https://www.theguardian.com/world/2019/apr/24/christchurch-call-ardern-leads-push-against-online-terror-content

Schmitt, E., & Sengupta, S. (2015, September 26). Thousands enter Syria to join ISIS despite global efforts. *New York Times*. Retrieved from https://www.nytimes.com/2015/09/27/world/middleeast/thousands-enter-syria-to-join-isis-despite-global-efforts.html

Scimeca, D. (2015, December 11). ISIS is using military simulator Arma 3 as a recruitment tool. Retrieved from https://www.dailydot.com/layer8/isis-using-arma3-recruiting-tool/

Stern, J., & Berger, J. M. (2016). *Isis: the state of terror*. London, England: William Collins.

Tarabay, J., Shiloach, G., Weiss, A., & Gilat, M. (2015, October 8). To its citizens, ISIS shows a softer side too. Retrieved from https://www.vocativ.com/world/isis-2/to-its-citizens-isis-also-shows-a-softer-side/

Tolido, R., Van Der Linden, G., Thieullent, A.-L., & Frank, A. (2019, November). *Reinventing cybersecurity with artificial intelligence: The new frontier in digital security*. Capgemini Research Institute.

Unanimously adopting Resolution 2199 (2015, February 12), security council condemns trade with Al-Qaida associated groups, threatens further

targeted sanctions. (2015). Retrieved from https://www.un.org/press/en/2015/sc11775.doc.htm

Wallace, M., & Townsend, F. F. (2017, November 30). The case for removing extremist videos from the internet. *New York Times*. Retrieved from https://www.nytimes.com/2017/11/30/opinion/youtube-extremist-videos-internet.html

Zelin, A. Y. (2019, November 8). A clearinghouse for jihādī primary source material, original analysis, and translation service. Retrieved from https://jihadology.net/