Humaniora. Czasopismo Internetowe
No. 1 (25)/2019, pp. 53–61

OR ANAT ELIMELECH RAISKIN*
Israeli Prime Minister's Office

ISIS's use of cyberspace – furthering the organization's goals utilizing new media

Abstract. *ISIS engages a wide array of new media tools: Facebook, Instagram, Twitter, YouTubeand other social media outlets.ISIS uses advanced knowhow, technological innovations, social media, and has even launched applications. This allows it to influence and recruit outside of its physical borders in Syria and Iraq. This paper will describe the various ends motivating ISIS's usage of new media tools, such as worldwide propagation of ideology, recruitment of personnel and assets, establishing terrorist cells and guiding terror attacks.In addition, this paper will discuss ISIS's ideology, the underlying religious jurisprudence dissonance and cyber-jihad – the use of technology and cyberspace to advance violent militaristic jihad against the perceived enemies of Islam.*

Keywords: *ISIS, New Media, Cyber-jihad, Terror, Fatwas*

Introduction

The world is transitioning towards modernization and a technological era, a time when there are no protective boundaries and countries are penetrable to information, ideas, people and materials. This reality enables a new expression of terrorism: a threat in which a terrorist located in a remote part of the world has significant

* Author is analyst at Israeli Prime Minister's Office.

damage potential, which completely transforms the former balance of power and is able to infiltrate security systems, recruit followers and threaten nations.[1]

The term "Cyber Jihad" (henceforth: Cyber Jihad) refers to the use of 21st century technological abilities and exploiting cyberspace (computer communication environment) for the furthering of violent militaristic Jihad against those labeled by adherents as "enemies of Islam." The Cyber Jihad phenomenon has evolved and changed throughout time. Today, the concept of Cyber Jihad refers mainly to the use of online social media outlets such as Facebook, Twitter, YouTube and Tumblr.

ISIS's Cyber Jihad also includes offensive use of cyberspace for attacking various websites; terror organizations call this offensive activity "A'zwa" (which translates as "Attack" or "Raid" in Arabic, and sometimes used as "Electronic A'zwa") in the spirit of the raids that Prophet Mohammed (henceforth: Mohammed) used circa Islam's genesis against non-believers. Prominent examples of this kind of Cyber Jihad are the takeover of US central command's social media accounts and the attacks on French websites after the Charlie Hebdo massacre in Paris. In the latter, ISIS affiliated hacker groups conducted raids on more than 19.000 French websites in the week following the terror attack, and as a result, multiple web servers hosting those sites were incapacitated.[2]

1. New media'sinfluence

Internet websites and services, collectively "new media" and specifically: streaming media, YouTube, Facebook, Twitter, blogging, podcasts, websites and so on – have significantly changed the communication landscape.

Writing blogs on the internet has become a popular means of political expression and an increasingly important source of political communication data. Twitter, the micro blogging site, has also become a popular avenue for political communication. Social networks of all kinds but particularly Facebook have quickly entered the realm of political communication practice.[3]

The online social network website Facebook is one of the most important platforms for social interaction between people worldwide. The geographical distances are being replaced with social interactions powered by the revolution of new technology where almost all kinds of people can equally be part of the new global communication apparatus. New media technologies are playing a pivotal role in the societies where media is not free. Newspapers, radio and TV can be

[1] G. Siboni, D. Cohen, A. Rotbart, *The Threat of Terrorist Organizations in Cyberspace*, "Military and Strategic Affairs" 2013, Vol. 5, No. 3.

[2] A. Hoffman, Y. Schweitzer, *Cyber Jihad in the Service of the Islamic State (ISIS)*, "Strategic Assessment" 2015, No. 18(1), p. 73.

[3] P.A. Soukup, *Political Communication*, "Source Communication Research Trends" 2014, Vol. 33, issue 2.

banned and manipulated, but the internet cannot be completely banned, blogs and Facebook cannot be abandoned, mobile phone messaging cannot be stopped by the governments. In recent popular uprisings in Arab countries like Egypt, Tunisia and Libya against their governments, new media played an important role in facilitating the huge agitation campaigns against then incumbent Arab rulers. Arabic services are available in all of the major search engines such as Google and Yahoo, and nowadays the internet is heavily used in the Arab countries.[4]

Social media is being increasingly used in a political context. Microblogging and social network sites are believed to have the potential for increasing political participation. Twitter is an example of an ideal platform for users to spread not only information in general but also political opinions publicly through their networks.

Mainstream adoption of social media applications has changed the physics of information diffusion. Social media is increasingly used recently in political context both by citizens and political actors. Social media provides a connection between social networks, personal information channels, and the mass media, and it enables political actors to directly interact with each other.[5]

New media technologies have changed the world dramatically and have also influenced the patterns of political communications.The features of current political communication present formidable challenges for media policy makers.

Executives from governments, regulators and mass-media acknowledge that the media eco-structure is changing although they still cling to long standing paradigms and models to explain and regulate it. The ethos of broadcast still prevails in the majority of policy thinking, and new media concepts such as interactivity, social networking and user generated content are treated as a secondary tier of public communication.[6]

2. ISIS's usage of new media

One of the greatest motivators for individuals to commit Cyber-Jihad are religious decisions ("Fatwas"). Al-Azhar University issued a Fatwa allowing the hacking of American and Israeli websites which offend Islam as part of cyber-jihad.According to a fatwa the Muslim must stand against brutal attacks against Islam aimed to depict it unworthily. This will be done by electronic attacks, and all available resources should be diverted for these kinds of wars.The Al-Azhar Fatwa has

[4] S. Riaz, *Effects of new media technologies on political communication*, "Journal of Political Studies" 2010, No. 17(2), p. 161.

[5] S. Stieglitz, L. Dang-Xuan, *Social media and political communication: a social media analytics framework*. "Social Network Analysis and Mining" 2013, No. 3(4), pp. 1277–1291.

[6] M. Gurevitch, S. Coleman, J.G. Blumler, *Political communication—Old and new media relationships*, "The ANNALS of the American Academy of Political and Social Science" 2009, No. 625(1), pp. 164–181.

gained the support of several religious clerics. Dr. Muhammad Ali Al-Zahoul, the dean of Jordanian Muata University's Sharia faculty, has expressed his support of the Fatwa and added that cyber-jihad is a part of the jihad of the pen and the word.

Dr. Muhammad Fuad Al-Brazi, the head of the Islamic association in Denmark, and a member of the European council for research and Sharia has expressed support of the Fatwa and said that attacking Israeli websites and other harmful websites to Islam is considered part of Jihad.[7]

3. The "Lone Wolf" Terrorist in Cyberspace

Two major effects of Cyber Jihad are the acceleration of foreign fighters' recruitment and the encouragement of attacks on the West by "lone wolves." Young people, arrested for trying to join ISIS, have testified that being exposed to ISIS's propaganda in online social media played a key role in their decision to try and join the organization.

ISIS's Cyber Jihad encourages the "lone wolf" phenomenon: people committing terrorist acts in line with ISIS's vision, but without an official connection to it. This was how, for example, the terror attacks in Sydney, Paris and Copenhagen were conducted by individuals influenced by ISIS and carrying its flag, but not officially subscribed to it. Official ISIS saw these terror attacks as successful and "pocketed" them as its own. In addition, ISIS published video clips celebrating Omar Al Hussein, the Copenhagen terrorist, and calling for more terror attacks on the West by "lone wolves."

This kind of terror attacks, usually committed without any early warning, allows ISIS to operate outside the Middle East through supporters and activists who adhere to its ideals. The "lone wolf" phenomenon presents a clear threat to western nations, which has been realized several times in the past, and it appears that it would not have been so dramatic without the use of social media.[8]

The characterization of the "lone wolf" terrorist will aid in his tracking and with the coping of western governments against this phenomenon. Spontaneous terrorist attacks in western countries do not need organizational infrastructure in target countries. Using online activities' patterns of specific population sections, governments can ascertain sign of the will to commit terrorist attacks.[9]

---

[7] Al-Azhar Fatwa *Hacking U.S., Israeli Websites Is Permissible as Part of Electronic Jihad*, 29.08.2008, http://cjlab.memri.org/uncategorized/al-azhar-fatwa-hacking-u-s-israeli-websites-is-permissible-as-part-of-electronic-jihad/ [14.12.2018].

[8] A. Hoffman, Y. Schweitzer, *Cyber Jihad in the Service of the Islamic State (ISIS)*, "Strategic Assessment" 2015, No. 18(1), p. 73.

[9] G. Siboni, D. Cohen, T. Koren, *The Islamic State's Strategy in Cyberspace*, "Military and Strategic Affairs" 2015, No. 7(1), pp. 127–144.

4. Building the Caliphate

The purpose of ISIS's online activities allows its followers to receive useful information, including courses on bomb and car-bomb making, alongside Fatwas, legitimizing atrocities in ISIS controlled territories. Another purpose is indoctrination, such as the publishing of the newsletter "DABIQ – the return of the Caliphate," which focuses on topics related to the establishment of the new Islamic State headed by the organization's leader Abu Bakr el-Baghdadi.[10]

5. Innovative terrorist expression

There are at least 46,000 active accounts of ISIS followers on Twitter, and American advisors estimated that ISIS generates about 90,000 tweets per day. Twitter use relies on ISIS's online supporters to advance and propagate its media in unprecedented volumes versus previous terrorist organizations. ISIS's distributive nature is not random, but a part of a cognizant ISIS strategy to better spread its messages through cyberspace.[11]

6. Analyzing ISIS Psychological Warfare

Beheading operations target two audiences - local and global. Locally, these video clips are mostly used to gain the psychological advantage against local dissenters and strike them with fear. The global audience, especially the USA, Great Britain and Australia, is targeted to achieve political and propaganda gains, such as influencing popular opinion by terrorizing it and recruiting potential activists.[12]

7. Cyber Jihad – social networks and modern terrorism

As an example of the seriousness with which terrorists refer to media and political communication, we can quote from 2005, Al Qaeda's then second in command Ayman al Zaeahiri wrote to Al Qaeda`s Emir Abu Musab Zarqawi: "We are in a battle, and more than half of this battle is taking place in the battlefield of the

[10] G. Siboni, T. Koren, *Cyberspace in the Service of ISIS*, "INSS Insight" 2014, No. 601.

[11] A. Hoffman. *The Islamic State's Use of Social Media: Terrorism's Siren Song in the Digital Age*, in Y. Schweitzer, O. Einav (eds), *The Islamic State: How Viable Is It*, Institute for National Security Studies, Tel Aviv 2016, pp. 99-105.

[12] G. Siboni, D. Cohen, T. Koren, *The Islamic State's Strategy in Cyberspace*, "Military and Strategic Affairs" 2015, No. 7(1), pp. 127–144.

media."[13] The Jihadists use new media methods for their internal communication, as they provide possibilities for new, cheaper and faster forms of recruitment, and it is also a platform for propaganda and boasting. It helps in spreading fear to those who are targeted. It allows the dissemination of their desired message in a cheap, visible and unbelievably fast manner.

World media, social media users and virtually anyone who is to any extent engaged in the world affairs, are providing terrorists with secondary "advertisement" for their actions by paying attention to them and talking about them. As the 1990s came, the internet and specifically, its communication methods, were beginning to be used, both by the general public and terrorist groups, which brought along not only a shift in their operation scope, but also new threats.

As time passed, a significant shift has been made in the way Jihadists reach out to their audience. A shift has also been made in the way the audience responds to the message as well as in the way western media treats newcomers. New media, especially social media, have opened up an arena of unprecedented scope and possibilities.[14]

Narrowcasting is a method of aiming messages at specific segments of the public defined by values, preferences, demographic attributes, or subscription. Terrorist groups such as ISIS, and their sympathizers, are using predominantly Western online communities like Facebook, Myspace, and Second Life, as well as their Arabic counterparts. New media online platforms used to promote electronic Jihad are also used for operational purposes such as instruction and training, data mining, coordination, and psychological warfare. In the 2008 terrorist attacks on numerous locations inMumbai, India, the attackers used advanced communication technologies, including handheld GPS devices to plan and execute their attack. They utilized Google Earth satellite imagery and mobile phones providing live updates from their handlers about the location of hostages, especially foreigners.

Terrorists use YouTube videos as well as Facebook postings to teach how to operate explosives, direct followers to websites with instructional material, promote hacking techniques, and share encryption programs. These postmodern terrorists are trained in virtual online camps, using the rich variety of new social media capabilities.[15]

Stretching from Al Qaeda, Al Shabaab, Boko Haram all the way to ISIS, this cyber caliphate flourishes in the techno nutrient rich, binary soil of the internet and is continually reinforced via graphic imagery and unique story telling in publications

---

[13] J. Stern, J.M. Berger, *ISIS: The State of Terror*, Harper Collins Publishers, New York 2015, pp. 287–288.

[14] M. Sonkova, *Power of Words: When Terrorism Goes Viral, "Politikon. The IAPSS Journal of Political Science" 2016*, Vol. 29, p. 215.

[15] G. Weimann. *New terrorism and new media*. Wilson Center Common Labs, 13.05.2014, https://www.wilsoncenter.org/publication/new-terrorism-and-new-media [14.12.2018].

such as Dabiq and Kybernetiq. In the Energy and Financial sectors, cyber-attacks have already begun, and there are no solutions that offer total blanket protection from all of these threats. Layered security that detects, responds to and predicts threats will continue to be the most vital of technical tools in any meaningful cyber defence arsenal[16].

8. Challenges of facing ISIS

One can assume that ISIS has cyberspace offensive capabilities for a number of reasons:

1. ISIS's leaders, split of Al-Qaeda in June 2014, are led by a highly technologically knowledgeable group of young radicals, aware of Al-Qaeda's abilities and experience in cyberspace, including transmission of encrypted messages, Fatwa, online explosives training, car bombs, etc.

2. There is a viable advanced technology information leakage route between Iran (and its ally North Korea) and various terror organizations.

3. ISIS has amassed an asset pile of around USD 2 billion, stemming from oil, gas and loot sales, allowing cyber terror funding uses "Dark Wallet" to reach international terror groups.

4. In 2014, ISIS affiliated elements took control of the Twitter account of the group Anonymous, using very similar techniques to those used by the hacker organization the "Electronic Syria Army," affiliated with the Assad regime, which displays a high level of sophistication.

5. Analysis by American intelligence company InterCrawler suggests that since August 2014 there has been a dramatic increase of malicious code (njRAT) distribution from around four major cities: Baghdad, Irbil, Basra and Mosul.

6. Elements affiliated with "ISIS Electronic Army" stated their intention to commit Cyber Jihad.[17]

The increase in the influence given to media effects in contemporary strategic affairs was motivational for ISIS to formulate its media policy in order to achieve maximum audience at a minimum cost and time. Consequently, ISIS was successful in attracting international media and influencing its agenda. As a result, the present penetration of ISIS in international media is allowing it considerable attention from public opinion and is making it the center of attraction.

Despite the willingness to limit ISIS's influence on the media, the international community has so far been unable to achieve its objective due to ISIS`s strategy of decentralizing its media approach.

---

[16] J. Scott, D. Spaniel, *The Anatomy of Cyber-Jihad: Cyberspace is the New Great Equalizer*, Institute for Critical Infrastructure Technology, Washington D.C. 2016.

[17] G. Siboni, T. Koren, *Cyberspace in the Service of ISIS*, "INSS Insight" 2014, No. 601.

Although ISIS has certain military capabilities and control and command structure, it is its media strategy that is constructing images and building public perceptions to its favor through different means and methods.[18]

Conclusions

Cyberspace is home to substantial terrorist activities using it as a medium, enabling control over multiple distant territories and wide audiences, recruitment of activists and funds, dissemination of psychological messages and recruitment of lone terrorist agents.

This phenomenon has religion discourse woven into it. The contradictions and the resistance. On the one hand, the desire to stick to the known roots, imitating the Prophet's life, the roots of Islam, and avoiding change and progress; On the other hand, the use of technology in general and new media in particular to spread Islam around the world efficiently, by recruiting followers, and advancing the acquisition of new territories.

ISIS understands the advantages of cyberspace, its opportunities and its influence, popular opinion, media developments and the effective attack capabilities against countries in cyberspace and the importance of lone wolf terrorists fuelled by new media. ISIS manifests itself in blogs, social networks, applications and servers.

Defensive authorities are forced to confront a young, dynamic, technologically savvy, and learning organization; these are new challenges. The key to facing this challenge cannot rely on cybersecurity alone. It is based on learning the language and understanding the religious goals, studying the customs, the sensitivities and the contradictions, the Fatwas, and the innovations of the Salafi-Jihadi movement with its many factions.

Literature

Gurevitch M., Coleman, S. and Blumler, J.G., *Political communication—Old and new media relationships*, "The ANNALS of the American Academy of Political and Social Science" 2009, No. 625(1).

Hoffman A., Schweitzer, Y., *Cyber Jihad in the Service of the Islamic State (ISIS)*, "Strategic Assessment" 2015, No. 18(1).

Hoffman A., *The Islamic State's Use of Social Media: Terrorism's Siren Song in the Digital Age*, in Y. Schweitzer, O. Einav (eds), *The Islamic State: How Viable Is It*, Institute for National Security Studies, Tel Aviv 2016.

[18] A.S. Khawaja A.H. Khan, *Media Strategy of ISIS: An Analysis*, "Strategic Studies" 2016, No. 36(2).

Khawaja A.S., Khan, A.H., *Media Strategy of ISIS: An Analysis*. "Strategic Studies" 2016, 36(2).

Riaz S., *Effects of new media technologies on political communication*. "Journal of Political Studies" 2010, No. 17(2).

Scott J., Spaniel D., *The Anatomy of Cyber-Jihad: Cyberspace is the New Great Equalizer*, Institute for Critical Infrastructure Technology, Washington D.C. 2016.

Schori L.C., *Cyber Jihad: Understanding and Countering Islamic State ropaganda*, "GCSP Policy Paper" 2015, No. 2.

Siboni G., Cohen D., Rotbart A., *The Threat of Terrorist Organizations in Cyberspace*, "Military and Strategic Affairs" 2013, Vol. 5, No. 3.

Siboni G., Koren T., *Cyberspace in the Service of ISIS*, "INSS Insight" 2014, No. 601.

Siboni G., Cohen D., Koren, T., *The Islamic State's Strategy in Cyberspace*, "Military and Strategic Affairs" 2015, No. 7(1).

Sonkova M., *Power of Words: When Terrorism Goes Viral*, "Politikon. The IAPSS Journal of Political Science" 2016, Vol. 29, No. 215.

Soukup P.A. *Political Communication*, "Source Communication Research Trends" 2014, Vol. 33, issue 2.

Stern J. & Berger J.M., *ISIS: The State of Terror*, Harper Collins Publishers, New York 2015.

Stieglitz S. & Dang-Xuan L., *Social media and political communication: a social media analytics framework*. "Social Network Analysis and Mining" 2013, No. 3(4).

Weimann G., *New terrorism and new media*. Wilson Center Common Labs, 13.05.2014, https://www.wilsoncenter.org/publication/new-terrorism-and-new-media

Al-Azhar Fatwa, *Hacking U.S., Israeli Websites Is Permissible as Part of Electronic Jihad*, 29.08.2008, http://cjlab.memri.org/uncategorized/al-azhar-fatwa-hacking-u-s-israeli-websites-is-permissible-as-part-of-electronic-jihad/