UDC 2.343 https://doi.org/10.48010/2023.1/1999-5849.12

ONLINE VISIBILITY AND RADICALIZATION: CONCEPTS, CONTEXTUALIZATION, AND CASES

Göktuğ Sönmez

ABSTRACT

In recent decades, security institutions have placed high priority on understanding the relationship between radicalization, violent extremism, terrorism, and the use of both traditional and new media tools. The terrorist attacks of 9/11 brought global attention to terrorism and its cross-border impact, but the use of information and communication technologies (ICT) by terrorist groups has increasingly become a crucial aspect of terrorism. The rise of ISIS and their adept use of social media and the internet, in particular, has been a significant milestone in demonstrating how effective these tools can be for terrorist organizations, even after the groups demise, and inspiring others to follow suit.

Key words: Terrorism, Propaganda, Social Media, ICT, Counter-Terrorism.

Necmettin Erbakan University, Konya, Türkiye; Akhmet Yassawi International Kazakh-Turkish University, Turkistan, Kazakhstan

Author-correspondent: Göktuğ Sönmez, goktugsonmez@gmail.com

Reference to this article: Göktuğ Sönmez. Online Visibility and Radicalization: Concepts, Contextualization, and Cases // Adam alemi. – 2023. – No. 1 (95). – P. 132-141.

Желідегі көріну және радикалдану: концепциялар, контекстуализация және жағдайлар

Аңдатпа. Соңғы онжылдықтарда қауіпсіздік институттары радикалдану, зорлық-зомбылық экстремизм, терроризм және дәстүрлі және жаңа медиа құралдарын пайдалану арасындағы байланысты түсінуге үлкен басымдық берді. 11 қыркүйектегі лаңкестік шабуылдар жаһандық назарды терроризмге және оның трансшекаралық әсеріне аударды, бірақ лаңкестік топтардың ақпараттық-коммуникациялық технологияларды (АКТ) пайдалануы терроризмнің маңызды аспектісіне айналды. ДАИШ-тің күшеюі және олардың әсіресе әлеуметтік желілер мен интернетті шебер пайдалануы бұл құралдардың топ жойылғаннан кейін де террористік ұйымдар үшін қаншалықты тиімді болатынын көрсетуде және басқаларды да үлгі алуға шабыттандыруда маңызды кезең болды.

Түйін сөздер: терроризм, үгіт-насихат, әлеуметтік желілер, АКТ, терроризмге қарсы күрес.

Онлайн-видимость и радикализация: концепции, контекстуализация и примеры

Аннотация. В последние десятилетия органы безопасности уделяли первостепенное внимание пониманию взаимосвязи между радикализацией, насильственным экстремизмом, терроризмом и использованием как традиционных, так и новых средств массовой информации. Террористические атаки 11 сентября привлекли внимание всего мира к терроризму и его трансграничному влиянию, но использование информационных и коммуникационных технологий (ИКТ) террористическими группами все чаще становится решающим аспектом терроризма. Подъем ИГИЛ и их умелое использование социальных сетей и Интернета, в частности, стал важной вехой в демонстрации того, насколько эффективными могут быть эти инструменты для террористических организаций даже после распада группировки, и вдохновил других последовать их примеру.

Ключевые слова: терроризм, пропаганда, социальные сети, ИКТ, борьба с терроризмом.

Introduction

The internet, and social media in particular, have provided ordinary people with valuable opportunities to stay informed about global events, share their opinions with a wide audience, connect with like-minded individuals, and feel part of a larger community. However, criminal networks, as well as radical and terrorist groups, have also exploited these platforms to their strategic advantage. These include the ability to maintain anonymity to a certain extent, disseminate messages quickly and cheaply to their target audience and global broadcasters, update their narratives in response to changing circumstances, use polarization, victimhood, and enmity to gain support, pursue «propaganda by deed» through claiming responsibility for attacks, plan operations using messaging applications, and conduct fundraising through social media and crypto currencies, which facilitates illegal financial transactions.

Although terrorist groups have benefited from the virtual world's features, it is important to recognize that states also have advantages in combating such groups. The same characteristics that provide ordinary people and criminal networks with advantages also enable states to monitor radical groups' online activities and recruitment efforts, develop and implement strategies to counter these groups, identify and engage with key individuals known as «gatekeepers,» track and stop illicit financial transactions, and monitor, filter, and store data related to these groups and their members. Despite the threats posed by these groups, states can leverage the power of the virtual world to gain insights and take effective action against them.

It is reasonable to say that the internet has become an essential aspect of daily life for all actors, from social networking and propaganda to fundraising and monitoring criminal activities. As such, it has become a key area of concern in international security, one that can be attacked at any time by a variety of actors, making its protection challenging. Securing this front requires speed, resources, knowledge, and measures, which are often scarce resources for states, particularly without effective cooperative frameworks in place.

Since 2000, when the internet had around 740 million users, the number of people connected has risen to over 3.5 billion in 2017, which is slightly more than half of the world population. This increase in internet usage has not only provided advantages to ordinary citizens but has also significantly expanded the target audience and pool of potential recruits for radical and terrorist groups. Moreover, the rise of populist politics, xenophobia, and anti-refugee discourse has contributed to a vicious cycle of radicalization and marginalization. Currently, there are slightly over 3 billion active social media users, and North African and Middle Eastern countries have seen significant growth in internet and social media usage since the 1990s and the first decade of the new millennium [1]. Messaging apps, too, which are widely used by groups either striving for political and social change and by criminal networks and terrorist groups have a wide and growing penetration in the broader MENA region. In short, as Simon Kemp argues, "Digital is growing faster in the Middle East than anywhere else in the world" [2]. Due to the fact that over 60% of the population in the Middle East is under the age of 30, it is crucial to understand the link between social movements, radical groups, criminal networks, and vulnerable young people. These groups are increasingly using online material to recruit and indoctrinate young people, which can have severe security consequences in the future. It is alarming to note that the average age of an ISIS fighter falls between the ages of 18 and 25, highlighting the vulnerability of young people to extremist groups. This trend is further exacerbated by the widespread use of social media in the region. With fewer penetration rates during the 1990s and the

first decade of the new millennium, North African and Middle Eastern countries are experiencing a significant increase in the use of the internet in general and social media in particular. As such, active social media users have exceeded 3 billion worldwide, and with the rise of social media, radical and terrorist propaganda, populist politics, xenophobia, and anti-refugee discourse have become increasingly prevalent. These factors are equally important pillars of a vicious cycle that perpetuates radicalization, marginalization, and violent extremism. As the world becomes increasingly interconnected through technology, it is important to acknowledge that the internet has become an indispensable part of everyday life for individuals and organizations alike. However, the ease and anonymity provided by the internet have also made it a key front in the context of international security, which can be attacked by actors almost instantaneously. As such, securing this front requires speed, resources, know-how, and time, which are often scarce resources for states. It is imperative that effective cooperative frameworks are established to tackle this issue, particularly in regions where the youth population is particularly vulnerable to the influence of extremist groups. It is not by chance that the youth, considered one of the most vulnerable groups, have been among the most active users of the internet and social media. Due to their marginalized status, poverty, and limited access to education and employment opportunities, young people are particularly attractive targets for recruitment by radical and terrorist organizations, who view them as a valuable resource pool to exploit.

Methodology

According to the ideas presented by Alex Schmid and Janny de Graaf, terrorism can be considered as a form of communication. The message being conveyed by the terrorist is of utmost importance, while the victim is secondary in significance and is only important insofar as they contribute to the spread of the message. This idea is not new, as various groups throughout history have utilized mass media to further their agendas. For instance, in the 1915 silent film «The Birth of a Nation,» the Ku Klux Klan was portrayed as «saviors» and this film was used for decades to recruit militants and gain sympathizers, resulting in a membership of 4.5 million by 1920. Similarly, many other organizations, such as the Red Army Faction in West Germany, the Red Brigades in Italy, the IRA, and the FARC, have used magazines and brochures to communicate with media outlets before and after their actions. The FARC, for instance, utilized radio stations to spread their message. With the advent of the internet and social media, these groups have had an even greater ability to communicate and spread their message. Far-right groups, such as neo-Nazis and the Aryan Nation, have also sought to increase their visibility through the use of mass media. In the 1980s, they began to appear on television and later established their own websites. This demonstrates how the rise of the internet and social media has facilitated the spread of extremist messages and enabled groups to communicate with a wider audience than ever before [3].

Rapoport asserts that the majority of terrorist organizations have a short lifespan, with 90 percent lasting less than a year [4]. However, al-Qaeda has managed to remain a prominent and active group for decades due to its adept use of the online world. Azzam.com, launched in 1997, is considered the first genuine al-Qaeda website and was instrumental in establishing the group's online presence. By 1998, less than 15 terrorist organizations were operating in the online space. However, within just a few years, the number of websites promoting terrorist content had grown to over 4,300. Osama bin Laden, in a 2003 video, acknowledged the importance of psychological warfare and the need to defend against the massive propaganda machinery of the

United States. Similarly, Ayman al-Zawahiri, who succeeded bin Laden as the leader of al-Qaeda, emphasized the significance of spreading the group's message to Muslims and lifting the media siege. In 2002, al-Qaeda launched the al-Neba website, which featured speeches from scholars affiliated with the group, along with news on the conflicts in Afghanistan and Iraq. Zawahiri pointed out in 2005 that more than half of the war was taking place in the media [5, p. 101].

In line with this focus of extremist groups on the online realm, this article, mainly using secondary sources, will elaborate on its selected case studies, namely ISIS and selected Shi'a militia groups which will provide a comparative understanding of how extremist groups can utilise social media and internet in general. In order to do that, besides benefitting from the secondary sources analysing these groups and their online presence, their online outlets and visibility channels, as primary sources will be used. This will allow the reader to see how the hypothesis of increasing online capability and visibility of radical groups reflect upon the realities on the ground from propaganda efforts to recruitment and fundraising efforts by such groups.

Terrorism and the Cyber Realm: The Case of ISIS

ISIS is known for its effective use of social media, video-streaming websites, and messaging applications, which have given it an unprecedented cyber presence and visibility. The group has used popular social media and messaging applications such as Telegram, WhatsApp, Facebook, and Twitter, as well as video-streaming websites such as YouTube, to great effect. It is important to analyze the strategies and aims of the group when using cyber means. One key strategy of ISIS is to attack and de-legitimize groups and individuals who adopt an anti-ISIS stance. By doing so, the group aims to legitimize its position, especially from a religious perspective. Additionally, the group uses cyber means to promote the idea of a utopia in the areas under its control. Through videos and other media, ISIS compares the failed or failing state structures that have failed to provide services and social and economic benefits to the people, with the provision of such services by ISIS, making people happy to live harmoniously under the group's control. Another strategy of ISIS is to show its strength and brutality against its enemies on the ground. Through videos and other media, the group aims to spread fear and prove its capabilities, such as through videos of the group brutally executing people or fighting its enemies on the ground. Supporters of the group also try to deepen polarization between the group's «righteous cause» and the «enemy's inhumane actions» by using images and videos of the atrocities committed by its enemies in different parts of the world, underlining the group's «victimhood» rhetoric and legitimizing its position and narrative. The online realm has also been a major area for planning and carrying out attacks, providing the group with cheap and fast organizational advantages. Recruitment and fundraising have also been key aims of the group in the online world. Overall, the group's use of cyber means has been an important part of its strategy, allowing it to promote its message, legitimize its position, and carry out its violent actions.

To carry out the strategies and achieve their goals, ISIS utilized various tools, with one of the most significant being their e-journals. These journals, such as Dabiq in English, Konstantiniyye in Turkish, Dar-al Islam in French, and Istok in Russian, were visually appealing and professional in their design. They were utilized to achieve their goals, which included delegitimizing those who opposed ISIS, promoting a utopian image of the areas under their control, showcasing their strength and brutality against their enemies, and deepening polarization between their cause and that of their enemies. In addition to these goals,

the e-journals focused on particular topics of interest in the countries or regions where they were published. However, following ISIS' gradual decline after mid-2015, these e-journals ceased to be published one by one, with the last remaining journal, Dabiq, disappearing after Turkey's Euphrates Shield Operation. Apart from the e-journals, ISIS supporters utilized social media and video-streaming websites to disseminate the group's material. According to Clarke and Winter, ISIS was once in control of 54 media offices around the world. For them to operate effectively seven times higher wages were paid to the people who can produce propaganda material including graphic designers and cameramen [6].

The decline of ISIS on the ground has also affected the group's propaganda efforts in the cyber realm. At its peak in mid-2015, the group was producing over 200 propaganda materials per week, including magazines, videos, and radio programs. However, with the group's territorial losses, the number of propaganda materials produced also significantly decreased. By late 2017, the group was producing a modest 20 outputs per week. This decline in the group's online presence and propaganda activities has been a result of the damage suffered by its propaganda machine. Winter (2015, 2017a, and 2017b) has noted the significant loss of capability and visibility experienced by the group's propaganda efforts, indicating that the challenge for ISIS in the cyber realm has been just as great as the difficulties on the ground [7].

The success of ISIS in the cyber realm has not gone unnoticed by other terrorist groups worldwide. In fact, it is no surprise that the increased visibility of ISIS in the online world was followed by the increased visibility of other extremist groups, ranging from al-Qaeda to far-right extremists. Terrorist groups have demonstrated impressive learning curves, not only in terms of tactics on the ground, but also in terms of propaganda strategies and mediums. They can quickly adopt new tactics both in the real and virtual worlds and strive to make effective use of them. As a result, we can expect that the online «legacy» of ISIS will persist for decades to come. The experienced propagandists who remain from the group can bring their expertise back to their home countries or act as propagandists for new groups in the countries where they currently reside. They could also be recruited by other groups, either in Iraq and Syria or in their home countries in the West. Even if all of the experienced ISIS propagandists were to disappear suddenly, the memory of the group's effective online propaganda will continue to inspire other groups.

Shi'a Non-State Armed Actors and Online Recruitment

Hezbollah was founded in 1982 with the primary goal of fighting against Israel. Since then, the group has steadily increased its influence, not only in Lebanon but throughout the Middle East. One of Hezbollah's key strategies has been to establish an alternative economic, political, and social system that operates independently of the official state structure. By providing a space for the Shi'a population in Lebanon, Hezbollah has sought to establish itself as the primary representative of this group and marginalize the official government. This alternative system has allowed Hezbollah to offer services and support to Shi'a communities, such as healthcare, education, and social services, which has helped to solidify its position and support among this population. One of the ways Hezbollah has expanded its influence beyond Lebanon is through its involvement in the Syrian civil war. The group provides financial incentives to those who join the fight in Syria, with payments ranging from $500 to $1200. By participating in the conflict, Hezbollah has been able to project its military power and establish itself as a key player in the region. However, this involvement has also

drawn criticism and condemnation from other nations and organizations, who view Hezbollah's actions as destabilizing and dangerous [8].

According to sources, a percentage of Hezbollah's human force, estimated to be around 50 thousand in total, has been transferred to Syria, ranging from approximately 8 to 15 percent (4 thousand to 8 thousand). Prior to Hezbollah secretary-general Nasrallah announcing the presence of its forces in Syria in 2013, the group began recruiting fighters online using images of the Sayyidah Zaynab shrine. Websites and phone numbers were made available for volunteers to contact, including a separate phone number for leaving and sending messages. By May 2013, over 3200 people had registered to fight in Syria through ValieAmr.com. The Ghobe.ir website also began accepting volunteers and meeting them on the Syrian border. Facebook was also used to gather and distribute contact information to potential volunteers, with Zulfiqar Army stating that the contact information was for «pilgrims» who wanted to visit the Sayyidah Zaynab shrine.

Shiite groups referred to the protection of Sayyidah Zaynab shrine as the «Holy Defense» or «al-Difa al-Muqaddes,» which was also used during the Iran-Iraq War. The shrine plays a significant role in regional Shi'a politics and the expansion of Iran's influence in the area. In 2003, over 200,000 Iranian tourists visited the shrine. Protecting the shrine has been a central goal in the formation and strengthening of the Fatemiyoun and Zeynabiyoun Brigades [9].

Afghan refugees in Iran are motivated to fight in Syria for financial and citizenship benefits, as well as sectarian reasons. They can earn between 500 to 700 dollars per month and hope to obtain Iranian citizenship for themselves or their families. The 2016 citizenship law, which grants citizenship to those who fought and died for Iran in the Iran-Iraq War, also includes fighters from Afghanistan and Pakistan who fight in Syria. These incentives have played a significant role in motivating Afghan refugees to travel to Syria to fight [10].

An Afghan fighter who was captured by the Free Syrian Army in October 2012 was shown in a short interrogation video that was posted on Youtube. Later, in July 2013, an official declaration of martyrdom was made for a fighter named Safer Mohammad who died in Syria, and in this declaration, the Hezbollah flag, the Syrian regime flag, and the flag of Afghanistan were used together. It has been reported that over 640 Shiite Afghans have died while fighting in Syria, according to [11].

Zeynabiyoun Brigades is the group that Pakistani Shiite fighters fight under. Starting from 2013, Pakistani Shiites from the Turi tribe and Hazaras from Quetta have been arriving in Syria to participate in the conflict. According to the Facebook page of Zeynabiyoun Brigades, volunteers need to be between the ages of 18 and 35 and physically fit. The group pays its fighters $1,200 per month and allows them a 15-day vacation every three months. Initially, the fighters lost their lives while protecting the Sayyidah Zaynab shrine, and later, seven of them died while defending the Imam Hasan Mosque in Damascus. In March and April 2016, at least 11 Pakistani Shiite fighters killed in Syria were buried in Qum [12, p. 5-6].

Following the capture of Mosul by ISIS in June 2014, a Shiite group called Kata'ib al-Imam Ali emerged in Iraq. This structure, founded by the people who left the Mahdi Army of Muqtada al-Sadr, is known to have particularly brutal killing methods and to spread them online. Recruitment and propaganda activities of Kat'aib al-Imam Ali for the Syrian civil war are carried out by the group more intensely than many other groups. It is known that the group strives to recruit fighters in the vicinity of Najaf by using photographs of the Sayyidah Zaynab shrine through the offices, billboards, and social media accounts of the group.

The group is known for its brutal killing methods and widespread dissemination of these methods online. Kat'aib al-Imam

Ali conducts recruitment and propaganda activities for the Syrian civil war more intensely than many other groups, using photos of the Sayyidah Zaynab shrine on group offices, billboards, and social media accounts to attract fighters in the Najaf area.The Nujaba Movement, another group of Iraqi Shiite fighters in Syria, was formed separately from the Asa'ib Ahl al-Haq group in 2013 by Sheikh Akram al-Kaabi. Through social media, the Nujaba Movement announced its presence in Aleppo, Nubl, and Zahraa in May 2013. In July 2015, the group announced an increase in its military presence in Idlib, and Kaabi visited the Nujaba fighters to assess their readiness. The group stated that its fighters intended to recapture Jisr al-Shugur, which is currently held by Jaysh al-Fateh [13].

Social media accounts linked to Kat'aib al-Imam Ali also announced in July that the group sent fresh troops along with experienced fighters to the region, and several photos of the fighters in Damascus were published while the group announced that «great victories» were achieved in Syria. In August, it was announced by the TV channel of the Nujaba Movement that the fighters of the group were actively fighting around Aleppo, Hama, and Latakia.

In addition to the aforementioned two main groups, it is seen that some other groups try to increase their activities in the field, too. First of all, large groups such as Badr Organization, Asa'ib Ahl al-Haq (under the name of Liwa al-Sayyida) [14, p. 14-18] and Kata'ib Hezbollah send fighters to Syria. In 2014, the Badr Organization made a photo including Ayatollah Muhammad Baqir al-Sadr, Ayatollah Khamenei and a telephone number from which the volunteers could get the contact information in the cover photo of its Facebook page (Quwet al-Shahid Muhammad Baqr al-Sadr) and urged the volunteers to the "defense of Sayyidah Zaynab shrine". The organization was also one of the first groups to use YouTube in its efforts to recruit fighters, and in even mid-2014, uploaded Youtube videos containing images of war in Syria accompanied by songs praising the ideology of the group and directing viewers to the organization's Facebook page. The images in the videos were later broadcasted on the TV channel of the group, al-Qadir TV, too [15].

Conclusion: How to Cope with the Cyber Challenges, Way Forward, and Challenges

To address the growing threat of cyber attacks that are carried out by terrorist groups using information and communication technologies, it is essential for states to leverage the same advantages of the online world that are used by these groups. Specifically, states must make effective use of the internet's fast and low-cost communication capabilities to disseminate their messages and engage with the public. By doing so, they can more effectively counter the messaging strategies of terrorist groups and reduce their visibility and credibility in the cyber realm. One of the key advantages of using the internet to combat terrorist propaganda is the ability to disseminate messages quickly and efficiently. By adopting similar tactics to those used by terrorist groups, such as using social media platforms, states, security agencies, and NGOs can reach millions of people with their messages in a matter of minutes. This not only helps to counter the spread of extremist ideologies but also provides an opportunity for states to engage with the public and build support for their counter-terrorism efforts. Another advantage of using the internet to combat terrorist propaganda is the ability to quickly adjust messaging strategies in response to specific incidents or changes in the tactics used by terrorist groups. This enables states to respond to terrorist threats in real-time and adapt their messaging strategies to more effectively counter the tactics of these groups. By leveraging social media networks, counter-messaging efforts can

reach a wide audience, including vulnerable individuals, former fighters, and victims of terrorist brutality. This is particularly important since social media networking can be seen in the form of «friends of friends,» which at the end of the circle could cover all humanity. Therefore, by reaching out to hundreds of millions of people, including those who have been affected by terrorist groups, counter-messaging efforts can help to build support for counter-terrorism efforts and reduce the appeal of extremist ideologies. To achieve the most significant impact, counter-messaging efforts must also be creative and engaging. Approaches such as using cartoons, personal stories, and humorous videos can be effective in countering terrorist propaganda and reducing their visibility and credibility in the online space. In summary, using the same advantages of the online world that are used by terrorist groups, states can more effectively counter the messaging strategies of these groups and reduce their impact on society. By leveraging the internet's fast and low-cost communication capabilities, states can disseminate their messages quickly, adjust messaging strategies in real-time, and engage with the public to build support for counter-terrorism efforts.

The primary obstacle to monitoring the cyber realm and implementing legal measures to address pro-terrorist content is the near-complete control of this realm by private companies. As a result, effective initiatives to tackle this issue and cooperation between companies, NGOs, and states are critical. Despite their influence in this vast realm, neither companies nor states can claim complete success in eliminating pro-terrorist content due to the slow decision-making and legal amendment processes of the latter, as well as the limited control they have over companies and the internet in general. It is important to note that the international community and ordinary people around the world are increasingly calling on leading global IT firms to take necessary actions to address the growing threat in the cyber world. For example, following the attacks in Barcelona and San Bernardino, Twitter and Facebook were sued for enabling communication among ISIS supporters, which allowed them to plan and organize attacks and propagate them by claiming responsibility via social media platforms [16]. In response to mounting pressure from various stakeholders, technology companies gradually adopted a more stringent approach to combatting pro-terrorist content, though criticisms remained that their efforts were not sufficient. For instance, Twitter suspended over 1.2 million accounts since August 2015 as part of its efforts to combat terrorism. Despite these actions, some continue to criticize the company's stance as insufficient [17]. The company reported that its «internal tech tools» identified 93% of accounts disseminating pro-terrorist propaganda, and 74% of those accounts were suspended before they could publish their first tweet, preventing the dissemination of pro-terrorist content. Facebook, meanwhile, has been using artificial intelligence (AI) to flag such content, and in the first quarter of 2018, the company took action on 1.9 million pieces of such content. The company reports that 99% of this content was identified using AI and internal reviewers, without the need for reports from ordinary users. Furthermore, more than 600,000 pieces of pro-terrorist content were removed in the first quarter of 2018 alone [18]. Google-owned YouTube has implemented the «Redirect Method,» which guides users who search for or show interest in pro-terrorist content toward anti-terrorist messaging and narratives. By leveraging machine learning, algorithms, and human reviewers, the company has also made efforts to remove extremist content from its platform. According to Juniper Downs, the head of public policy at YouTube, the company can remove almost «70% of extremist content within 8 hours of upload and nearly half of it in 2 hours» [19]. In an effort to identify

individuals spreading pro-terrorism content and expand their reach, major tech companies like Microsoft, Google, Facebook, and Twitter established a shared database of digital fingerprints, known as «hashes.» This database allows companies to track and monitor the spread of such content across their platforms and remove it as quickly as possible. Additionally, the database is continuously updated and expanded to include new hashes as they are identified [20].

Several challenges remain in terms of ISIS's online presence and influence. Firstly, the group will continue to inspire new and existing extremist groups, who may learn from both the group's successes and failures. Secondly, the knowledge and expertise gained by ISIS during its existence could be passed on to other groups, either by former members joining other organizations or by selling their expertise. Thirdly, individuals may continue to contribute to ISIS's online presence even as the group's influence wanes. Finally, in addition to propaganda, the group's online expertise could also be used to facilitate illicit financial activities and the procurement of weapons for future attacks.

The challenges of balancing security and personal liberties are a major concern in the fight against online radical and extremist groups like ISIS. Balancing the need for cybersecurity with concerns about privacy, freedom of expression, and belief is a complex issue that requires careful consideration. Additionally, legal and bureaucratic constraints can hinder states' ability to take swift action against extremist groups. Effective cooperation among international organizations and regional mechanisms is also crucial for successfully combating online extremism. Institutions such as the UN's Counter-Terrorism Executive Committee Directorate, the EU's European Cybercrime Centre, and law enforcement agencies like EUROPOL and INTERPOL play a key role in this effort. However, the effectiveness of such cooperative efforts remains to be seen, as there have been past challenges with cooperation on the ground in the physical world.

To sum up, the challenges that the cyber world presents in the fight against extremism and terrorism are numerous and complex. These challenges include not only the ability to combat extremist groups in the online realm but also the need to balance security and liberties, as well as the difficulties of establishing and operating effective cooperative schemes and institutions. The threat posed by extremist groups in the cyber world is not limited to the activities of the groups themselves but also includes the inspiration and know-how that they can pass on to other groups. The fight against extremism and terrorism in the cyber world requires the cooperation of states, private companies, and international organizations. States must be willing to work together to devise and implement online and offline measures that can combat the activities of extremist groups. Private companies, particularly those that operate online platforms, must also be willing to work with states to identify and remove extremist content. International organizations such as the UN and the EU can play a key role in coordinating these efforts and ensuring that information and experience are shared among their members. The cyber realm provides numerous advantages to both criminals and law enforcement agencies, making the fight against extremism and terrorism a constant challenge. Extremist groups like ISIS have already shown their ability to exploit these advantages, and other groups will likely continue to follow their lead. States must therefore be willing to adapt and respond quickly to these new threats, which requires speeding up their own legal and bureaucratic processes. In conclusion, the fight against extremism and terrorism in the cyber world is an ongoing battle that requires the cooperation of states, private companies, and international organizations. While the challenges are significant, it is important

to remain vigilant and continue to develop new strategies and technologies to combat the activities of extremist groups in the cyber realm.

References

1 Dave Ch. Global Social Media Research Summary 2018 // *Smart Insights*. – 28 March 2018.

2 Damian R. & Lam A. Social Media In The Mıddle East The Story Of 2017: Key developments, stories and research findings. - University of Oregon, 2018.

3 Wintz C.D., Dixon Jr.Th. The Clansman: A Historical Romance of the KuKluxKlan. – New York, Routledge, 2001; Scribner Ch. Buildingson Fire: The Situationist International and the Red Army Faction // *Grey Room*. – 2007. - No.26. - P. 30-55.

4 Rapoport D. Terrorism // Routledge Encyclopedia of Government and Politics. Volume II. – London, Routledge, 2000. - P. 1061-1082.

5 Ariel Victoria Lieberman. Terrorism, the Internet, and Propaganda: A Deady Combination // *Journal of National Security, Law & Policy*. – 2017. - №9. - P. 95-124.

6 Clarke C., Charlie W. The Islamic State May be Failing, But Its Strategic Communications Legacy is Here to Stay // *War on the Rocks*. – 17 August 2017.

7 Charlie W. Documenting the Virtual "Caliphate". - Quilliam Foundation, October 2015.

8 Hanin Gh. Perceiving the Shia Dimension of Terrorism // *The Georgetown Security Studies Review.* Special Issue: What the New Administration Needs to Know About Terrorism and Counterterrorism. - 2017. – P. 15-19.

9 Smyth Ph. The Shiite Jihad in Syria and Its Regional Effects // The Washington Institute for Near East Policy. Policy Focus 138, 2014.

10 Farzam R.& Sarı İ. Fatimiyyun: İran'ın Afgan Milisleri // *USAD*. – 2017. - №6. – P. 267-290; Termill W. A. Iran's Strategy for Saving Asad // *Middle East Journal*. – 2015. – 2(69). – P. 222-236.

11 Alfoneh A. Shia Afghan Fighters in Syria // *Syrian Voices*. – 19 April 2017.

12 Zahid F. The Zainabiyoun Brigade: A Pakistani Shiite Militia Amid the Syrian Conflict // Terrorism Monitor. – 2016. - Volume XIV, issue 11. – P. 1-10.

13 Smyth Ph. The Shiite Jihad in Syria and Its Regional Effects // The Washington Institute for Near East Policy. Policy Focus 138, 2014.

14 Clarke C., Smyth Ph. The Implications of Iran's Expanding Shi`a Foreign Fighter Network // *The CTC Sentinel*. Volume 10. Issue 10 (November 2017). - P. 14-18.

15 Smyth Ph. The Shiite Jihad in Syria and Its Regional Effects //The Washington Institute for Near East Policy. Policy Focus 138, 2014.

16 Collins K. Families of San Bernardino victims sue Facebook, Google, Twitter // *CNet*. – 5 May 2017; Robinson J. Daughters of California man killed in Barcelona terror attack sue Google, Facebook and Twitter "for aiding, abetting and knowingly providing support and resources" to ISIS // *Mail Online*. – 6 October 2017.

17 Lomas N. Twitter claims more progress on squeezing terrorist content // *Tech Crunch*. - 5 April 2018.

18 Locklear M. Facebook details its fight to stop terrorist content // *Engadget*. – 23 April 2018.

19 Shinal J.Facebook, Google tell Congress they're fighting extremist content with counterpropaganda // *CNBC*. – 17 January 2018.

20 Solon O. Facebook, Twitter, Google and Microsoft team up to tackle extremist content // *The Guardian*. - 6 December 2016.

INFORMATION ABOUT THE AUTHOR

Göktuğ Sönmez — Associate Professor, PhD, Necmettin Erbakan University, Konya, Türkiye; Akhmet Yassawi International Kazakh-Turkish University, Turkistan, Kazakhstan, Almaty, Kazakhstan, email: goktugsonmez@gmail.com, ORCID ID: 0000-0001-5067-4693

Гөктуғ Сөнмез — доцент, PhD, Некметтин Эрбакан Университеті, Конье, Түркия; Қожа Ахмет Ясауи атындағы Халықаралық қазақ-түрік университеті, Түркістан, Қазақстан, email: goktugsonmez@gmail.com, ORCID ID: 0000-0001-5067-4693

Гөктуғ Сөнмез — доцент, PhD, Университет Некметтина Эрбакана, Конье, Турция; Международный казахско-турецкий университет имени Ходжи Ахмеда Ясави, Туркестан, Казахстан, email: goktugsonmez@gmail.com, ORCID ID: 0000-0001-5067-4693