

## THE EVOLUTION OF CYBER JIHAD: FROM AL-QAEDA TO THE ISLAMIC STATE

*Анотація.* Метою статті є огляд еволюції кібер-джихаду, починаючи з 1990-х рр. до теперішнього часу. Встановлено, що наявні чотири етапи розвитку кібер-джихаду: перший етап вважається початковим і тривав у 1990-і рр., коли перші ісламістські групи використовували інтернет для впливу на світову спільноту, проте їм не вистачало належної майстерності, тому відмічався низький рівень загроз міжнародній стабільності; другий етап з'явився одночасно з Web 2.0 на початку XXI ст., що призвело до появи додаткових каналів зв'язку, наприклад, блогів і відеохостингів; третій перехідний етап був ініційований подіями, що отримали назву «арабська весна», та характеризувався масовим використанням терористами соціальних медіа; четвертий етап розпочався у 2014 р. з появою Ісламської держави та пов'язаний з багатомісними пропагандистськими кампаніями в мережі Інтернет, що можна характеризувати як вагому загрозу міжнародній безпеці.

**Ключові слова:** кібер-джихад, кібербезпека, тероризм, Ісламська держава, Аль-Каїда.

*Abstract.* This paper aims to provide an overview of the evolution of cyber jihad since the 1990s to the present day. It argues that so far there has been four stages of its development. The first, initial chapter started in the 1990s, when the first Islamist groups used the Internet in order to influence global audiences.

---

\*Assistant Professor, Department of International Relations, Faculty of Social Sciences, University of Silesia, Ph.D/habilitation

*These activities, however, lacked the proper skill and know-how, and therefore posed a little threat to international security. The second chapter was opened in parallel to the emergence of the Web 2.0 environment in the 21<sup>st</sup> century, which was manifested by the enrichment of communication channels exploited by jihadists (e.g. blogs, video hosting services). The third, transitional stage was initiated due to the experiences of the Arab Spring. It was characterized by the massive use of social networks by the Islamist terrorists and their sympathizers. Finally, the last chapter has started in 2014 in consequence of the Islamic State's emergence. This group has launched a massive, multidimensional and sophisticated propaganda campaign online, which proves to be a unique phenomenon generating serious threats to international security.*

**Key words:** cyber jihad, cybersecurity, terrorism, Islamic State, al-Qaeda.

***Аннотация.** Целью статьи является обзор эволюции кибер-джихада, начиная с 1990-х гг. и до настоящего времени. Установлено четыре этапа развития кибер-джихада: первый этап считается начальным и продолжался в 1990-е гг., когда первые исламистские группы использовали интернет для влияния на мировое сообщество, однако им не хватало должного мастерства, поэтому отмечался низкий уровень угроз международной стабильности; второй этап появился одновременно с Web 2.0 в начале XX в., что привело к появлению дополнительных каналов связи, например, блогов и видеохостингов; третий переходной этап был инициирован событиями, получившими название «арабская весна», и характеризовался массовым использованием террористами социальных медиа; четвертый этап начался в 2014 г. с появлением Исламского государства и связан с многомерными пропагандистскими кампаниями в сети Интернет, что можно характеризовать как весомую угрозу международной безопасности.*

**Ключевые слова:** кибер-джихад, кибербезопасность, терроризм, Исламское государство, Аль-Каида.

**Introduction.** Cyber jihad, understood as the Islamist terrorist groups' propaganda in the Internet, is a phenomenon which appeared initially in the second half of the 1990s. According to Albrecht Hofheinz, this term was coined by the Muslim students in the United States, who created first Islamic Web pages [1]. Since then major forms and specificity of cyber jihad have evolved, becoming a serious threat to national and international security. This trend has been proved by the emergence of the so called Islamic State, which initiated unique cyber jihadist campaign in 2014, directed mostly against the Western states and Muslim societies around the world [2]. Manipulation tools exploited by the Daesh proved to be very efficient in the Web 2.0 environment, composed of social media, blogs, video/music/graphic hosting services and various communication applications. The vast success of this campaign was symbolized by the images and recordings of the Western citizens' executions (e.g. James Foley), which have proliferated in cyberspace reaching millions of receivers around the world. It has to be stressed that the Islamic State has also partially succeeded in reaching out to Muslim youths living in developed countries [3] and terrorizing European societies [4].

In this context, this article aims to provide an overview of the evolution of the Islamist terrorist groups' propaganda in cyberspace since the 1990s to the present day. The article focuses on several aspects of cyber jihad: its major channels of communication, strategies of distribution, as well as forms of propaganda releases. This paper also aims to answer the question, what are the innovative features of the Islamic State's activities online that enabled its success in cyberspace, in comparison to the earlier attempts of extremists? In order to reach this goal, the manuscript has been divided into four parts. The first explains the reasons why the very phenomenon of cyber jihad has actually emerged. The second chapter covers the evolution of various Islamist terrorists' groups (Al-Qaeda, Hezbollah, Hamas) propaganda in the Web 1.0 environment, until the beginning of the 21<sup>st</sup> century. The third overviews the phenomenon of

cyber jihad in the Web 2.0 environment, and describes its most visible differences in comparison to the earlier stages of the Internet's development. Finally the last chapter focuses on the explanation why the Islamic State's propaganda campaign online proved to be a major success for terrorists.

**The roots of cyber jihad.** Islamist organizations and their supporters relatively quickly realized that the rising popularity and coverage of the Internet opens new possibilities for reaching their goals, including not only propaganda (radicalization, recruitment and incitement), but also financing, training, planning, execution of terrorist attacks, as well as conducting cyber attacks [5]. Since the second half of the 1990s various terrorist organizations, including al-Qaeda, Hamas and Hezbollah launched their first attempts to «conquer» the cyberspace with their messages, using various methods. They frequently manipulated beliefs and opinions of audiences, presented twisted interpretation of religious doctrines and reality, mythologized their own activities, utilized visual symbols in order to generate strong emotions among recipients, and used the rhetoric of confrontation [6].

In this context, understanding the phenomenon of cyber jihad is, however, impossible without the careful consideration of the very reasons, why the terrorists got interested in online environment in the first place. There are several causes, which explain this rising trend. To begin with, terrorism by definition seeks media interest in order to promote its political goals. The lack of media coverage and feedback, due to existence of various formal and informal barriers, was one of the major and traditional challenges that the terrorist organizations had to face in the past. Thus the emergence of cyberspace opened new chances for Islamists. It has quickly become an environment, which allowed informal and uncensored communication in various configurations (one-to-one, one-to-many) [7]. While the cyberspace rapidly grew in the 1990s, extremists gained almost direct and instant access to the millions of Internet users around the world, while avoiding multiple barriers, which were encountered in traditional media outlets. Thus, the initial lack of efficient online

communication regulations, combined with the constantly increasing pool of potential receivers, were therefore too tempting to not to take advantage of it [8]. Secondly, cyberspace allows relatively easily accessible anonymity for its users. While the attribution problem has become an exceptionally outstanding problem in context of cyber attacks [9], it is also a feature propitious for terrorist organizations attempting to launch information operations online. Thirdly, the relative inexpensiveness and simplicity of online activities also play a certain role. Communication in cyberspace, in form of e-mails, chats, communication software, social media accounts, blogs, is usually completely free, while it only requires basic computer knowledge and the Internet connection. This means that even an individual with little IT skills and scarce funds has a theoretical chance to conduct efficient psychological operation in an online environment [10]. Fourthly, cyberspace per se is a multimedia domain, which enables the creation of an innovative and interesting forms of propaganda by combining visual, audio, text and audiovisual content together. Finally, traditional media frequently use the Internet to find information about interesting stories and events. This means, that online propagandists may find a way to influence their news reports, and in effect, reach millions of offline audiences [11]. In this context, Internet may be also perceived as a perfect place for disinformation, as it is fulfilled with stories which are either false, or unverifiable. Despite this fact, many Internet users and media still fall for these messages.

To recapitulate, over the accelerating course of information revolution cyberspace has become a perfect place for terrorists' propaganda. The constant development of this domain, manifested by the plethora of innovative services, communication trends, applications and technologies, constitutes an environment, which opens new possibilities for psychological operations conducted by non-state actors. It is therefore not a surprise, that the interest of such groups in cyber jihad throughout the last two decades has been alike to the «snowball effect». This was perfectly summarized by one of the Islamic extremists in his message posted in the al-Qaeda-linked Global Islamic Media

Front website: «technology of the Internet facilitated everything. Today's Web sites are the way for everybody in the whole world to listen to the mujaheddin» [12].

**Cyber jihad in the Web 1.0 environment.** First Islamists which attempted to use cyberspace in order to promote their agenda emerged in the second half of the 1990s. According to Brunon Hołyst, they were inspired by the earlier experiences of Zapatistas in Mexico, Tamil Tigers in Sri Lanka, and Tupac Amaru Revolutionary Movement in Peru. All of them used the Internet to reach their political goals [13]. Initially jihadists' activities online were somewhat rudimentary, which was mostly caused by two factors. On the one hand, at the time they had relatively little knowledge on how to conduct efficient propaganda campaigns in the online environment. On the other, the Internet of the 1990s was still based on somewhat crude and undeveloped technologies, collectively referred to as the Web 1.0. Global access to the Internet was also very limited. There were only 40 million of its users in 1995 [14], which obviously restrained the scope of cyber jihad. Nevertheless, the aforementioned features of cyberspace were quickly recognized by such groups as al-Qaeda, Hezbollah and Hamas, as a chance to bypass state's and media censorship. In this context, Islamist online propaganda in the Web 1.0 environment had three common features, which proved to be a «cornerstone» of cyber jihad's development in the 21<sup>st</sup> century.

To begin with, it was initially focused on the text propaganda, in forms of simple articles, internet bulletins, as well as ideological declarations and statements. From time to time, these messages were enriched with pictures, banners and symbols. Most of the time, these materials were posted on isolated and rather primitive websites (e.g. Chechen kavkaz.org, started up in 1999 [15]). In time, at the verge of the 20<sup>th</sup> and the 21<sup>st</sup> centuries, jihadists also started to exploit audio content, which was manifested by the first Islamist online radios. Such existed, for instance, at the jehad.net website in 2002 [16]. When it comes to audiovisual releases, they were already recorded by some non-state actors in

the 1990s (for example, in Chechnya by the infamous Emir Khattab [17]), but the average Internet bandwidth was still too low to make it an efficient online propaganda tool. Secondly, cyber jihad exploited rather limited number of communication channels. The most common were dedicated, official, semi-official or unofficial websites, containing text messages and visual content. Sometimes these Web pages also included hidden, encrypted messages (e.g. with the use of steganography), understandable only for the members of terrorist organizations [18]. Other channels included: discussion boards, which gathered terrorists and their sympathizers, online chats and various communication applications [19]. Thirdly, due to the fact that the Middle Eastern Internet coverage was still lacking, in order to increase its scope, al-Qaeda utilized digital information carriers, such as CDs and DVDs, which were distributed by their members and sympathizers [20]. Fourthly, usually cyber jihadist materials targeted Muslim societies around the world, as the vast majority of them were produced in Arabic. In time, releases translated into English started to appear more commonly, which manifested that the greater priority was given to influencing global public opinion. And finally, Islamist propaganda content usually contained such motives as: selected Quran verses, images of jihadists (including their leaders, such as Osama bin Laden), burning flags of their enemies (the United States), fragments of classical theological works confirming the legitimacy of jihadist movement, news reports, as well as polemics with the real or imaginary enemies [21].

These initial jihadi information operations in the Internet had, however, a number of weaknesses. To begin with, since day one they were technologically outdated, and thus, rather unappealing for the audiences originating from developed states, which were accustomed to the more sophisticated communication methods. Furthermore, jihadists' websites were hardly accessible, as the search engines weren't yet as popular and efficient in the 1990s as in the 21<sup>st</sup> century. Moreover, there was an obvious language barrier, as only the minority of releases were translated into English. It meant that the

majority of Internet users at the time could not become acquainted with such content. And finally, also the very substance of jihadi messages were rather unappealing for yet unconvinced receivers, frequently taking forms of the long and wearisome considerations about the Quran, hadiths, obligations of Muslims and political events. Such approach proved that the terrorist organizations and their sympathizers had no well-thought-out strategy on how to use cyberspace efficiently against audiences originating from other, non-Muslim cultural zones. It is though not a surprise that these activities were barely noticed by the security services around the world.

To recapitulate, cyber jihad until the beginning of the 21<sup>st</sup> century was somewhat rudimentary phenomenon, which posed a little threat to international security. Its technical dimension was crude, as the Islamists usually did not possess proper know-how on creating and distributing messages efficiently in the environment of Web 1.0. Moreover, most of their propaganda was limited only to Arabic-speaking audiences and their content was wearisome for many of them.

**Cyber jihad in the Web 2.0 environment.** The aforementioned features of cyber jihad started to change at the beginning of the 21<sup>st</sup> century due to two groups of reasons. Firstly, it was caused by the eruption of the «war on terror». After 9/11 attacks messages released by terrorists started to draw more attention not only from the Muslim societies, but also Western governments, media and citizens [22]. It was especially visible during the American-led interventions in Afghanistan and Iraq. Secondly, at the beginning of the 21<sup>st</sup> century, the Internet underwent some major changes, resulting from the emergence of a number of innovative technologies. Web 1.0 environment was enriched by the new types of services, which allowed more active participation of Internet users in creation of the online content. This allowed the transformation of the old Internet into the Web 2.0 environment. By definition the term «Web 2.0» refers to the series of technological improvements, which enabled more interactions, content-sharing and collaboration between users. These technologies included among others:



wikis (Wikipedia), social media (Facebook, Twitter, Instagram, MySpace), blogs and microblogs, as well as new kinds of communication software [23]. This process was combined with the parallel dynamic development of the global Internet access and the emergence of the new digital technologies, which could be used for propaganda purposes. One can mention the popularization of cell phones (later on – smartphones), equipped with cameras, and the introduction of high-definition audiovisual standard. All of these devices and technologies could be exploited by the Islamist terrorists in order to improve the quality, scope and efficiency of their psychological operations online.

In this context, it has to be stressed that at that time the jihadists still favored classical websites as their main channel of communication with audiences. Al-Qaeda for instance, based on the network of semi-official or unofficial Web pages, including [drasat.com](http://drasat.com), [jehad.net](http://jehad.net), [alsaha.com](http://alsaha.com), [islammemo.com](http://islammemo.com), [jihadunspun.net](http://jihadunspun.net), [aloswa.org](http://aloswa.org) or [alned.com](http://alned.com). Their content included among others: Osama Bin Laden's preaching, lectures and statements, orders for al-Qaeda members and supporters, religious justifications explaining the World Trade Center attacks, and messages inspiring to conduct independent attacks against the «unbelievers» [24]. Other groups, like Hamas and Hezbollah adopted a different approach. Hamas, on the one hand, concentrated its online propaganda around its «official» website – the Palestine Info – which contained the majority of releases produced by this organization. Hezbollah, on the other hand, created a network of websites, which distributed materials created by the other media outlets belonging to the Party of God [25]. Except of them, there were plenty of independent initiatives online, led by the sympathizers of jihadists. One can mention, Pakistani [almuhrajiroun.com](http://almuhrajiroun.com) and [assam.com](http://assam.com), gathering Afghani, Chechen and Palestinian supporters of the Islamic holy war [26]. In 2006, experts estimated that there were about 4500 jihadi Web pages accessible in the Internet [27].

Except of websites, in time Islamists became increasingly active in other online communication channels, such as blogs and video hosting services.

Blogs, on the one hand, proved to be a handy tool of propaganda distribution as their reach was usually wider and more diverse than normal websites. They were also relatively easy to duplicate in case of deletion. On the other hand, video hosting services proved to be very useful when the audiovisual pieces of propaganda finally kicked in. While the asymmetric warfare against the foreign troops in the Middle East and Central Asia was ongoing, new technological abilities (cell phones with cameras), could be utilized by jihadists to record videos, which were subsequently posted online in various places such as dedicated websites and specialized hosting services, including both mainstream ones, such as YouTube and LiveLeak, and niche, which frequently contained gore content. One of the most popular Web pages of this kind at the beginning of the 21<sup>st</sup> century was ogrish.com. Later on, jihadist content could be also found at bestgore.com and zerocensorship.com [28]. These videos usually depicted battles with American or coalition soldiers, and executions of prisoners. Despite their low technical quality, they proved to be one of the greatest jihadi propaganda achievements, as websites containing such releases were sometimes visited by tens of thousands of Internet users per hour [29]. One of the first groups which massively produced such content was al-Qaeda in Iraq.

Except of the introduction of the new channels of communication, as well as audiovisual content, cyber jihadists also modernized their text propaganda. Simple and usually tedious Internet bulletins, articles and reports at that point started to transform slowly into the professional magazines, reminding best American journals. One of the first releases of this kind was «Inspire», which was published in 2010 in English by the al-Qaeda in the Arabian Peninsula. It had several interesting features which were formerly non-existent or rare. To begin with, its layout design was a clear reference to the leading Western magazines. Its creators used high-resolution pictures and professional computer graphics in order to enrich the visual layer of text messages. Moreover, it was basically the first jihadist magazine of this quality which was published purely in English and contained sophisticated manipulation techniques and carefully

considered articles. Their authors frequently used double-dealing or humorous argumentation. For instance, in one of the messages to Barack Obama posted in the «Inspire» magazine, Osama bin Laden stated: «If our messages can reach you by words, then they wouldn't have traveled by planes», which was an obvious reference to the 9/11 terrorist attacks. The major aim of these articles, as the journal's title suggests, was to inspire readers to support al-Qaeda and to participate in jihad. Some of the texts in the «Inspire» clearly aimed to convince and prepare recipients to conduct terrorist attacks against the developed states. The first issue even contained the text entitled: «Make a bomb in the kitchen of your Mom» [30].

Moreover, al-Qaeda had quickly noticed that its propaganda materials released online drew increased attention of global mass media. Therefore, it frequently attempted to generate extreme emotions among recipients by presenting shocking content, like e.g. decapitations. This in turn made these productions more suitable for generating interest among the journalists [31]. The very reason of these tendencies was accurately summarized by Ayman al-Zawahiri in 2005. In one of his letters he stressed: «I say to you: that we are in a battle, and that more than half of this battle is taking place in the battlefield of the media. And that we are in a media battle for the hearts and minds of our Umma» [32]. In other words, al-Qaeda managed to produce pieces of propaganda, which drew attention of the Western and Arabic media, in order to reach offline recipients.

These new features of cyber jihad, introduced mostly by al-Qaeda in the first decade of the 21<sup>st</sup> century, were quickly noticed, adopted and even upgraded by the other Islamist terrorist groups. They increasingly exploited video recordings, pictures, Internet magazines and even music to influence and persuade audiences about the legitimacy of their cause. One of the most significant examples was the Taliban Islamic Movement, which produced a wide spectrum of propaganda pieces, starting from the online journals (e.g «al-Samood»), through multi-language websites (in Dari, Pashtu, Urdu, Arabic,

English), to the nasheed and tarana music [33]. It has to be stressed that especially these last types of audio propaganda became increasingly popular among the Internet users in the following years. Frequently these productions contained extremist content and were related to the ideology of jihad [34].

#### **New quality of cyber jihad: the case of the Islamic State.**

Aforementioned evolution of cyber jihad in the first decade of the 21<sup>st</sup> century changed its global perception. Security services, academics and media around the world finally realized that the Islamist propaganda in the Internet had made a serious progress. Nevertheless, another milestone in its development occurred in 2011, as a side effect of the Arab Spring in the Middle East and Northern Africa. The consecutive revolutions against the authoritarian regimes were partially affected by the social networking which allowed to organize street protests and to avoid state censorship. Later on, the same social media, as well as video and picture hosting services were extensively exploited by all sides of the conflicts in Libya and Syria to share battle footage and official statements.

These experiences proved to be great lesson for terrorist organizations, which noticed and mimicked this trend. Since 2011 various jihadist groups have started to be increasingly active in multiple social media services, with the special emphasis put on Facebook, Twitter, and Instagram. Moreover, also YouTube and LiveLeak were getting increasingly popular among them [35]. However, still the majority of releases were poorly prepared, which was a factor that limited the scope and efficiency of their PSYOPs conducted in the Web 2.0 environment.

In this context, a new chapter in the history of cyber jihad was opened by the so called Islamic State, which started to develop its online propaganda capabilities throughout the conflict in Syria. This was proved by the series of its materials posted in the Internet both in 2012 and 2013. The proper campaign has been, however, initiated in the first half of 2014, which slightly predated the proclamation of the «Caliphate» [36]. According to many academics who analyzed materials released by the ISIS/IS, it proved to be a very advanced and

sophisticated online campaign [37]. Its uniqueness and efficiency was manifested by the «popularity» of the infamous execution videos released in 2014 among the Internet users. In cyberspace alone, they were viewed millions of times. Moreover, due to the traditional mass media activities, reports on these brutal decapitations reached tens of millions of Western citizens, intensifying their fear of the Islamic State.

There are several features, which supposedly contributed to this unusual success of the Islamic State's cyber jihad. To begin with, its technical quality was outstanding, when compared to the majority of the other Islamist productions. For instance, audiovisual propaganda created by the Islamic State's specialized cells (e.g. Al-Hayat Media Center, Amaq News Agency, al-Furqan Media), were usually professionally recorded, directed, edited, and utilized advanced post-production methods (special effects, 2D and 3D computer graphics). Most of them were available online in high-definition standard. This is a major change in comparison with the amateurish, crude and grainy videos released by the other Islamist groups. Many commentators suggested that the quality of the Daesh videos were comparable to the best American (Hollywood) productions [38]. It has proved to be an important characteristic, as it stroke a chord with the Western audiences, which were accustomed to such technical solutions. Secondly, the Islamic State's propaganda since its launch has been multilingual. Except of Arabic, Daesh's materials were among others released in English, Russian, French, Turkish, Urdu, Chinese or Polish [39]. This meant that it was the first campaign of this kind in history, which had a truly global scale. This also proved that the IS's propaganda cells strictly cooperated with its foreign members in order to prepare accurate translations of their messages. Thirdly, the Islamic State cyber jihad covered a wide spectrum of propaganda types, including text messages, audio, visual, as well as audiovisual content. The first group included not only traditional declarations, statements and news reports, but also a plethora of professional magazines, of a much better quality than the al-Qaeda's aforementioned «Inspire». One can mention: «Al-Masra»,

al-Naba», «Dabiq», «Islamic State News», «Istok», «Dar al-Islam», «Konstantiniyye», and «Furat.Press» [40]. Audio content included mostly the radio broadcasts recordings (al-Bayan radio), which were posted online and could be easily streamed by the Internet users with their browsers. Moreover, Islamic State's nasheed music was also met with great interest online. Strictly visual propaganda was also diversified. Except of banners, pictures and symbols, which were usually used to decorate magazines or videos, this group included memes and infographics. On the one hand, memes were extensively used to reach younger audiences, accustomed with this type of messages. On the other, professionally prepared infographics were simply a shorter and more attractive version of news reports. Both were very popular in social media. Finally, the audiovisual content contained battle footage, executions, short advertisements and interviews (e.g. so called mujatweets), «documentaries» and «reportages», as well as nasheed music videos. Two of these were met with great interest among the Internet users. On the one hand, the aforementioned executions, which differed significantly from the videos released by the other Islamist groups. Except of the statements of prisoners and executioners, they contained wide references to the current political or military events, sophisticated manipulations and advanced post-production effects. On the other hand, nasheed music videos, published in multiple languages, also reached wide audiences. Some of them were prepared by the Western citizens, such as the former German rapper – Deso Dogg. He was responsible for creating one of the ill-famed nasheeds – Fisabilillah. Other audiovisual productions, despite being a big less attractive for the massive audiences, were usually produced in the same, fully-professional manner. Fourthly, the distribution strategy of the propaganda content was carefully considered. The Islamic State used a wide spectrum of communication channels, which increased the scope and efficiency of this campaign. Except of «conventional» means like websites and blogs, the Islamic State concentrated its efforts on social media (Facebook, Twitter, Instagram) and video/picture/audio hosting and streaming services like YouTube and LiveLeak.

With the use of a large group of the IS's supporters and sympathizers, it was able to distribute its productions almost instantly throughout the social networks all over the world. Moreover, the Islamic State used methods similar to the viral marketing, which additionally improved the efficiency of the social media campaign. And finally, the Islamic State often utilized well-considered manipulation methods, which aimed to convince receivers about the legitimacy of its motivations and goals. Among the most frequent techniques, one can mention: testimonial, glittering generalities and distortion of data [41].

**Summary.** The aforementioned Islamist online propaganda has a long and complicated history. Being a convergence of jihadist ideology and digital technologies, it was influenced both by the information revolution and a number of important international events, such as the conflicts in Iraq, Afghanistan, the Arab Spring and the civil war in Syria. In this context, so far there has been four stages of its evolution. In the beginning, cyber jihad was merely a marginal addition to the «classic» modus operandi of terrorists and their supporters. Most of their productions were of poor quality, composed of simple Internet bulletins, articles and religious texts in Arabic, as well as crude banners depicting terrorists' symbols or their respected leaders.

The next stage occurred at the beginning of the 21<sup>st</sup> century, when the Web 2.0 environment emerged. It took, however, several years and the experiences of the Iraqi and Afghanistan wars, until the cyber jihadists fully recognized the true potential of the new Internet technologies. The most popular video hosting services, Islamist websites and blogs became a perfect place to distribute new propaganda pieces, such as recordings depicting executions and battle footage or the infamous nasheeds. At the same time, al-Qaeda frequently managed to influence broadcasts of traditional media outlets, using messages which were distributed online.

The next, transitional chapter of its history was opened mostly due to the experiences of the Arab Spring. While the social media and hosting services got increasingly popular around the world, terrorists started to mimic and develop

propaganda activities conducted by various Middle Eastern revolutionary and rebel groups in the «new media». This was perfectly visible in Libya in 2011 and in Syria since 2011. Gradually most of cyber jihadist productions grew more sophisticated, however, they were still far behind the average quality of the Western media productions, which obviously limited their efficiency. Despite the fact that the most of the Islamist propaganda videos were still poorly directed and grainy, lacking even basing post-processing, their distribution strategies changed, ensuring massive audiences. Moreover, other forms of cyber jihad aroused increased interest among Internet users, just to mention online magazines published in English or the nasheed music videos.

The last stage, being a pinnacle of cyber jihad's development, started in 2014, due to the emergence of the Islamic State. Its propaganda campaign in cyberspace conducted by the number of professional cells, has proved to be unique and highly efficient when compared to other terrorist organizations active in the online environment. The Islamic State has used almost all possible forms of propaganda, including among others memes, infographics, Internet bulletins, magazines, execution videos, advertisements, interviews, radio broadcasts, and nasheed music videos. These releases were distributed with the use of traditional communication channels (websites, discussion boards), Web 2.0 tools (social media, videos/picture hosting services, blogs), and various applications such as Telegram or Skype. It has to be stressed that the overwhelming majority of these releases had an outstanding technical quality, which generated exceptional interest from the Western audiences. Many also contained advanced manipulation techniques and references to the popular culture, which improved the global reception of these propaganda pieces, especially among the youths.

In this context, it has to be stressed that the Islamic State's propaganda campaign founded a new model of cyber jihad, which is and will be mimicked by the other terrorist organizations around the world. This is already visible in many materials released in the recent years by such groups as the Harakat al-



Shabab al-Mujahideen from Somalia or al-Qaeda. Moreover, it can be expected that this trend will expand in the coming years, even if the Islamic State will be removed from Syria and Iraq. Its experiences from the last two years proved that, despite the NATO's/EU's efforts, there are still many uncontrolled channels of online communication, which can be efficiently exploited by the extremists. Thus, the cyber jihad will be a constantly evolving phenomenon, utilizing all possible new technological innovations in order to poison public debate with its radical propaganda. This, in turn, will generate various international and national security threats, such as: lone-wolf terrorism, intimidation of targeted societies, recruitment of terrorists, their online training, gathering support of and inspiration of Muslim societies around the world. The efficient response to all of these challenges will require finding a proper counter-strategy, which will block and push back the Islamist messages in the Internet.

## REFERENCES

1. Bari Atwan, A., (2006). *The Secret History of al Qaeda*. Los Angeles: University of California Press, 127.
2. Shori Liang C. (2015). *Cyber Jihad: Understanding and Countering Islamic State Propaganda*. «GSCP Policy Paper», No. 2.
3. The Soufan Group (2015, December). *Foreign Fighters. An Updated Assessment of the Flow of Foreign Fighters into Syria and Iraq*.
4. Europeans agree ISIS is a top threat (2016). PewResearchCenter. 10.06.2016. Retrieved from: <http://www.pewglobal.org/2016/06/13/europeans-see-isis-climate-change-as-most-serious-threats/epw-all-major-threats-web-version/>.
5. United Nations Office on Drugs and Crime (2012). *The Use of Internet for Terrorist Purposes*, New York, 3-12.
6. Kosmyńska, S., (2013). *Cyberdżihad. Wykorzystanie internetu przez współczesny terroryzm islamistyczny*. In Podraza, A., Potakowski, P., Wiak, K. (eds.). *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*. Warszawa: Difin, 105.

7. Hołyst, B., (2010). *Terroryzm*. Warszawa: LexisNexis, 173-224.
8. A Framework for Understanding Terrorist Use of the Internet (2006). «ITAC Presents», No. 2, 2.
9. Rid, T. & Buchanan, B. (2015). *Attributing Cyber Attacks*. *The Journal of Strategic Studies*, Vol. 38, No. 1-2.
10. Lakomy, M. (2015). *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*. Katowice: Wydawnictwo Uniwersytetu Śląskiego, 95-96.
11. Weimann, G. (2004, March). *www.terror.net*. *How Modern Terrorism Uses the Internet*. United States Institute of Peace Special Report 116, 3.
12. Davis, B.R. (2005). *Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance*. «*CommLaw Prospectus*» Vol. 15, 122.
13. Hołyst, B. (2010). *Terroryzm*. Warszawa: LexisNexis, 205.
14. The rather petite Internet of 1995. Royal Pingdom. 31.03.2011. Retrieved from: <http://royal.pingdom.com/2011/03/31/internet-1995/>.
15. Bari Atwan, A. (2006). *The Secret History of al Qaeda*. Los Angeles: University of California Press, 127.
16. Jihad.net. Wayback Machine. – 03.12.2016. – Retrieved from: <https://web.archive.org/web/20021003073728/http://www.jihad.net/3.htm>,
17. Hołyst, B. (2010). *Terroryzm*. Warszawa: LexisNexis, 205.
18. Kosmyńska, S., (2013). *Cyberdżihad. Wykorzystanie internetu przez współczesny terroryzm islamistyczny*. In Podraza, A., Potakowski, P., Wiak, K. (eds.). *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*. Warszawa: Difin, 103.
19. Hołyst, B. (2010). *Terroryzm*. Warszawa: LexisNexis, 204-211.
20. Hołyst, B. (2010). *Terroryzm*. Warszawa: LexisNexis, 205.
21. Kosmyńska, S., (2013). *Cyberdżihad. Wykorzystanie internetu przez współczesny terroryzm islamistyczny*. In Podraza, A., Potakowski, P., Wiak, K. (eds.). *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i*

prawna. Warszawa: Difin, 111; Hołyst, B. (2010). Terroryzm. Warszawa: LexisNexis, 209.

22. About the rising role of Internet in terrorism and counterterrorism after the World Trade Center attacks see for example: Janbek, D. & Williams, V. (2014). The Role of the Internet Post-9/11 in Terrorism and Counterterrorism. *Brown Journal of World Affairs*, Vol. XX, No. 2.

23. Lakomy, M. (2015). Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw. Katowice: Wydawnictwo Uniwersytetu Śląskiego, 48-49; Web 2.0. WhatIs.com. Retrieved from: <http://whatis.techtarget.com/definition/Web-20-or-Web-2>.

24. Weimann, G. (2004, March). [www.terror.net](http://www.terror.net). How Modern Terrorism Uses the Internet. United States Institute of Peace Special Report 116, p. 10-11.

25. Jihad Online: Islamic Terrorists and the Internet (2002). Anti-Defamation League, 9-29; Lakomy, M. (2015). Internet w działalności tzw. Państwa Islamskiego: nowa jakość cyberdżihadyzmu?. «*Studia Politologiczne*» Vol. 38, 158.

26. Weimann, G. (2004, March). [www.terror.net](http://www.terror.net). How Modern Terrorism Uses the Internet. United States Institute of Peace Special Report 116, p. 10-11.

27. Bari Atwan, A. (2006). *The Secret History of al Qaeda*. Los Angeles: University of California Press, 127.

28. Hołyst, B. (2010). Terroryzm. Warszawa: LexisNexis, 204-211; Snyder, B. (2015). Why I Can't Stop Watching Horrifying ISIS Decapitation Videos. «*Wired*». 02.11.2015. Retrieved from: <https://www.wired.com/2015/02/on-watching-gore-and-death-online/>.

29. Lakomy, M. (2014). Oblicza cyberterroryzmu. In Szczurek, T. (ed.). *Asymetryczne zagrożenia bezpieczeństwa narodowego w XXI wieku*. Warszawa: Wydawnictwa Wojskowej Akademii Technicznej, 196.

30. Complete Inspire Al-Qaeda in the Arabian Peninsula (AQAP) Magazine (2010). Public Intelligence. 14.07.2010. Retrieved from: <https://publicintelligence.net/complete-inspire-al-qaeda-in-the-arabian-peninsula-aqap-magazine/>

31. Torres Soriano, M.R. (2008). Terrorism and the Mass Media after Al Qaeda: A Change of Course?, «Athena Intelligence Journal», Vol. 3, No. 1.
32. Browne, D. & Silke, A. (2011). The impact of the media on terrorism and counter-terrorism. In Silke, A. (ed.). *The Psychology of Counter-Terrorism*. London-New York: Routledge, 89.
33. Taliban Propaganda: Winning the War of Words? (2008). International Crisis Group Asia Report, No. 158, 12-16.
34. Jihad Nasheeds (2006). Stylus Magazine. 26.05.2006. Retrieved from: <http://stylusmagazine.com/turtable/2006/05/26/jihad-nasheeds/>.
35. About the social media and cyber jihad see e.g.: Klausen, J. (2015). Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq. «Studies in Conflict & Terrorism», Vol. 38, No. 1; Weimann, G. (2014). New Terrorism and New Media. «Wilson Center Research Series», Vol. 2.
36. Month: May 2014 (2014). Jihadology. Retrieved from: <http://jihadology.net/2014/05/>. Becker, O. (2014). ISIS Has a Really Slick and Sophisticated Media Department. Vice News. Retrieved from: <https://news.vice.com/article/isis-has-a-really-slick-and-sophisticated-media-department>.
37. Winter, C. (2015). The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy. London: Quilliam Foundation; Hoffman, A. & Schweitzer, Y. (2015, April). Cyber Jihad in the Service of the Islamic State (ISIS). «Strategic Assessment», Vol. 18, No. 1; Shori Liang C. (2015). Cyber Jihad: Understanding and Countering Islamic State Propaganda. «GSCP Policy Paper», No. 2.
38. Williams, L. (2016, February). Islamic State propaganda and the mainstream media. Iowy Institute for International Policy, 3.
39. Bari Atwan, A. (2006). *The Secret History of al Qaeda*. Los Angeles: University of California Press, 20.
40. Wejkszner, A. (2016). Państwo Islamskie. Narodziny nowego kalifatu? Warszawa: Difin, 138-160.

41. Lakomy, M. (2015). Internet w działalności tzw. Państwa Islamskiego: nowa jakość cyberdżihadyzmu?. «Studia Politologiczne» , Vol. 38.