Dominika LISZKOWSKA
Politechnika Koszalińska
Wydział Humanistyczny
dominika_liszkowska@wp.pl
https://orcid.org/0000-0001-6312-341X
https://doi.org/10.34739/dsd.2023.02.09

CYBERTERRORISM AS A CONTEMPORARY THREAT TO THE SECURITY OF THE STATE AND SOCIETY

ABSTRACT: The phenomenon of globalization, the development of technology, and the widespread use of the Internet have led to the creation of a digital space for information processing and exchange. Currently, it is used by various users, including public institutions, private companies, and individual users who have access to the network at home and on private electronic devices. Cyberspace protection has therefore become one of the main strategic goals in the security area of every states. Ensuring it depends mainly on the creation of effective mechanisms for preventing and combating threats on the Internet. The aim of this article is to present the issue of cyberterrorism as one of the main threats to the security of society and the state in cyberspace. With the development of the Internet, terrorists have new opportunities to act, regardless of where they are at any given time. Therefore, the article attempts to define the concept of cyberterrorism and the possible applications of this form of activity on the Internet. An important aspect has become the analysis of the benefits of using cyberspace for terrorist groups, including in terms of the radicalization of young people.

KEYWORDS: cyberterrorism, cyberthreats, radicalization, terrorism, terrorist organizations

CYBERTERRORYZM JAKO WSPÓŁCZESNE ZAGROŻENIE DLA BEZPIECZEŃSTWA PAŃSTWA I SPOŁECZEŃSTWA

ABSTRAKT: Zjawisko globalizacji, rozwój technologii i powszechne wykorzystanie Internetu doprowadziły do powstania cyfrowej przestrzeni przetwarzania i wymiany informacji. Jest ona obecnie wykorzystywana przez różnych użytkowników, m.in. instytucje państwowe, firmy prywatne, a także użytkowników indywidualnych, którzy mają dostęp do sieci w swoich domach i na prywatnych urządzeniach elektronicznych. Ochrona cyberprzestrzeni stała się zatem jednym z głównych celów strategicznych w obszarze bezpieczeństwa każdego państwa. Jej zapewnienie zależy w głównej mierze od stworzenia skutecznych mechanizmów zapobiegania i zwalczania zagrożeń w Internecie. Celem niniejszego artykułu jest przedstawienie problematyki cyberterroryzmu jako jednego z głównych zagrożeń dla bezpieczeństwa społeczeństwa i państwa w cyberprzestrzeni. Wraz z rozwojem Internetu, przed terrorystami pojawiają się bowiem nowe możliwości działania, niezależnie od tego, gdzie się w danym momencie znajdują. W artykule podjęto zatem próbę zdefiniowania pojęcia cyberterroryzmu i możliwych zastosowań tej formy działania w Internecie. Ważnym aspektem stała się analiza korzyści płynących z wykorzystania cyberprzestrzeni dla grup terrorystycznych m.in. w zakresie radykalizacji postaw młodych ludzi.

SŁOWA KLUCZOWE: cyberterroryzm, cyberzagrożenia, organizacje terrorystyczne, radykalizacja, terroryzm

INTRODUCTION

Due to the emergence of the phenomenon of cyberterrorism and its continuous development, new questions arise about the components of this category, its forms, methods of operation, perpetrators, objects, and targets of the attack. Undertaking an analysis of all these aspects, the author will try to show that in the coming years, cyberterrorism will be one of the most important threats, permanently accompanying states and societies. The possibilities of operating in cyberspace have opened up new directions for potential activities in all areas of life[1]. Thus, technological progress and widespread digitization do not bypass the phenomenon of terrorism, the functioning of terrorist organizations, or activities that can be defined as acts of terror. The Internet gives a greater opportunity to conduct a propaganda campaign and present a specific vision of the world. As a result, it is an excellent tool for reaching people vulnerable to radicalization and exerting influence on governments and societies. It also gives the opportunity to select new members for various types of organizations. Terrorists can also take advantage of the resources available in the digital world (such as networks) and organize their activities online without being physically involved. It can be recognized that cyberspace now concerns all aspects of terrorist activities. However, in this regard, further progress will be made by the activities of numerous organizations, terrorists, and hackers. An increase in the degree of professionalization of terrorist activities in cyberspace, as well as the emergence of new terrorist threats, should also be expected.

The article consists of four parts. In the first, the author attempted to define cyberterrorism and its possible applications, which directly affect society and the state. Referring to the definition of traditional terrorism, the author acknowledges that cyberterrorism is one of its modern forms. The second part characterizes cyberterrorists and their activities on the Internet according to the criteria of the entity of action. Furthermore, attention was paid, among others, to the problem of the 'invisibility' of representatives of terrorist groups in cyberspace and the difficulties that result from it. The next part of the article analyzes the benefits that the Internet provides to terrorists. In this part, the author indicates, among others, examples that confirm the benefits of the use of cyberspace by terrorist groups. The last part of the article draws attention to the problem of radicalization, which is now easier thanks to the Internet. Young people, or the main users of the Internet, are a group extremely susceptible to the influence of terrorists and attempts at radicalization. To reach this group, terrorists use not only social media but also other network platforms, including gaming portals. This state of affairs requires the development of new solutions to counteract the process of radicalization among young people in the coming years.

In the research process, the author used a descriptive-explanatory approach, which allowed both the description of the phenomenon and its explanation. The research method used was desk research and analysis of existing data. The data used in the analysis comes from

[1] M. Górka, *Wybrane aspekty definicyjne cyberterroryzmu i ich znaczenie w perspektywie polityki bezpieczeństwa*, „Cywilizacja i Polityka" 2017, 15, p. 297.

publicly available scientific articles and Internet sources. The author compiled, mutually verified, compared, and then processed them. The result of the analysis is the current diagnosis of the situation related to the activities of cyberterrorists on the Internet, as well as a supplement to the existing research results.

DEFINITION OF CYBERTERRORISM

The first announcements about the threats posed by attacks using computer systems appeared in 1979 and were issued by the Swedish Ministry of Defense. This ministry recommended the involvement of the government in supervising public and private computer networks in connection with cyberterrorism, which included all activities involving computers aimed at destroying ICT systems, supervision and control systems, programs, data, etc. These actions could have contributed to intimidating governments and societies to exert psychological pressure, resulting in a threat to life or significant harm[2]. This was the moment in which people began to systematically talk about the dangers aimed at society through computer systems[3].

However, defining cyberterrorism is not clear-cut. The area of activity in this matter is wide and difficult to define precisely. One of the definitional difficulties is the tendency to use the terms cyberwar, cyberterrorism, cybercrime, and hacktivism interchangeably, despite the differences between these concepts[4]. Therefore, when considering the issue of cyberterrorism, it is necessary to distinguish whether an action is terrorism or not. It is of particular importance to take a proper judgment of the perpetrator and, if possible, holding him accountable. For example, hacktivists are often identified with terrorists. However, although this group is politically motivated, its main goal is actually to protest, demonstrate, or attempt to overthrow the existing order, not to cause destruction or incite fear, as is the case with terrorists[5].

Barry Collin formulated one of the definitions of terrorism, the platform of which is cyberspace. The researcher defined this term as "the convergence of cybernetics and terrorism" and concluded that terrorists enter the virtual world from the real world[6], which gives them the opportunity to commit terrorist attacks without leaving home. In this context, cyberterrorism is "the conscious use of an IT system, computer network, or its components in order to support or

[2] I. Oleksiewicz, *Dilemmas and challenges for EU anti-cyberterrorism policy: The example of the United Kingdom*, "Teka Komisji Politologii i Stosunków Międzynarodowych" 2016,11(3), p. 136.
[3] J. Bieniek, *Cyberterroryzm zagrożeniem bezpieczeństwa państw współczesnego świata*, "Rocznik Bezpieczeństwa Morskiego" 2021, 15, p. 152.
[4] J. Brickey, *Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace*, "CTC Sentinel" 2012, 5(8), August, https://ctc.westpoint.edu/defining-cyberterrorism-capturing-a-broad-range-of-activities-in-cyberspace/ (20.09.2023), pp. 4-6.
[5] T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, "Zeszyty Naukowe Akademii Marynarki Wojennej" 2005, 1, p. 183.
[6] B. Collin, *The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge,* 11th Annual International Symposium on Criminal Justice Issues: The Future of CyberTerrorism:Where the Physical and Virtual Worlds Converge 1997, http:// www.crime-research.org/library/Cyberter.htm (20.09.2023).

facilitate the conduct of a terrorist action"[7]. Understanding cyberterrorism in this way, it can be concluded that Internet technology resources provide terrorist groups with significant benefits, such as the ability to spread propaganda, recruit new members, or create networks of contacts. However, apart from easier communication, organizing terrorist cells, recruiting, and planning attacks, the Internet itself can be used to carry out a terrorist attack[8].

Dorothy E. Denning from Georgetown University, whose definition of cyberterrorism is one of the most frequently cited, recognizes that "cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear"[9]. Although this definition does not indicate tools used by terrorists, it can be assumed that the author considers a cyberterrorist attack to include, among others, physically destroying computers, networks and information stored therein in order to intimidate or force the government or society to implement the political or social motives of terrorists. Cyberterrorist acts can, therefore, take many forms, such as mass destruction or intimidation.

In the definition formulated by James Lewis, cyberterrorism means "the use of computer network tools to shut down critical national infrastructures (such as energy, transportation, and government operations) or to coerce or intimidate a government or civilian population"[10]. As this definition shows, cyberspace gives terrorists a wide range of possibilities in terms of the form of attack. They can, for example, hack into national banking systems and international financial transactions, which will contribute to the loss of confidence in the economy. Another possibility is to gain access to air traffic control systems and cause a disaster in the airspace, or to hack into the computers of pharmaceutical companies and thus change the composition of selected drugs (leading to the annihilation of thousands of people). A form of terrorism on the Internet may also be hacking into the systems of public utility companies and causing, for example, changes in gas installations, detonations, and consequently explosions and fires in many places[11]. However, to be classified as terrorism, an attack on critical infrastructure in cyberspace should

[7] W.L. Tafoya, *Cyber Terror*, LEB FBI, November 2011, https://leb.fbi.gov/articles/featured-articles/cyber-terror (20.09.2023).
[8] N.K. Kadir, J. Judhariksawan, M. Maskun,, *Terrorism and Cyberspace: A Phenomenon of Cyber-Terrorism as Transnational Crime*, "Fiat Justisia" 2019, 13(4, pp. 332-335.
[9] D.E. Denning, *Statement*, Georgetown University 2000, https://irp.fas.org/congress/2000_hr/00-05-23denning.htm (20.09.2023).
[10] J.A. Lewis, *Assessing the risk of cyber terrorism, cyber war and other cyber threats*, Center for Strategic and International Studies 2002, https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf (20.09.2023), p. 1.
[11] M. Iqbal, *Defining Cyberterrorism*, "UIC John Marshall Journal of Information Technology & Privacy Law" 2004, 22(2), p. 397.

cause specific effects[12], i.e., be characterized by the use of violence against persons or property, or at least be significant enough to cause fear.

The object of cyberterrorist attacks is not only critical infrastructure but also information. Among them, there are three basic groups that are important in the case of cyberterrorism[13]. The first is military information related to the arms industry, new types of weapons, and armament technologies. The next group is economic information, which may concern bank transactions or credit card numbers. The third group is personal data, which includes private correspondence, personal data, and user identification numbers. Thus, obtaining information is an auxiliary method for terrorist organizations that allows them to gather knowledge about the target of the attack.

CYBERTERRORISTS AND THEIR ACTIVITIES IN CYBERSPACE

The types of cyberterrorism are distinguished based on subjective and objective criteria[14]. In the first case, we are talking about cyberterrorists and their victims, or the subjects of action and the subjects of the attack. The subjects of action include organized groups and individual cyberterrorists. Within the first distinction, there are classic terrorist organizations (Tamil Tigers, Hezbollah, or al-Qaeda) that use conventional means, but also use the Internet in their activities. The second category among organized groups is terrorist organizations consisting of computer hackers whose field of operation is exclusively in cyberspace[15]. In turn, individual terrorists are usually professional hackers with specific qualifications who, for a fee, can perform political activities ordered by terrorist organizations (in this case, cyberterrorists may be people who are not radicalized and are not associated with any terrorist organization[16]). The hackers' services were used by The Irish Republican Army on Halloween night in 1992, known as the Night of the Long Knives[17]. The aim was to penetrate computers and obtain the addresses of law enforcement and intelligence officers. The data obtained online was used to develop plans to kill the officers if the British government did not meet the terms of a new ceasefire. Although hacking was not used to wreak havoc in cyberspace in this case, it did show that terrorists can use hacking as a way to gain intelligence to use physical violence in the 'real world'[18].

[12] S. Schjolberg, *Terrorism in Cyberspace – Myth or reality*, "CyberCrime Law" 2006, https://www.cybercrimelaw.net/documents/Cyberterrorism.pdf (20.09.2023), p. 14.
[13] P. Maj, *Cyberterroryzm w stosunkach międzynarodowych*, "Consensus. Studenckie Zeszyty Naukowe" 2001, 1, p. 75.
[14] W. Smolski, *Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa*, [in.] M. Marszał (ed.), *Rodzinna Europa*, Wrocław 2005, p. 482.
[15] Ibidem, p. 482.
[16] S. Soesanto, *Cyber Terrorism. Why it exists, why it doesn't, and why it will*, Real Instituto Elcano, April 2000, https://www.realinstitutoelcano.org/en/analyses/cyber-terrorism-why-it-exists-why-it-doesnt-and-why-it-will/ (20.09.2023).
[17] D. Haverty, *IRA's Night of Long Knives' part in Northern Ireland's peace process*, Irish Central, November 2019, https://www.irishcentral.com/opinion/others/iras-night-long-knives-peace-process (20.09.2023).
[18] D.E. Denning, op. cit.

The basic feature of cyberterrorists activities is their political motivation. The aim of the activities is, therefore, to influence political decisions and disseminate a specific ideology[19]. However, regardless of whether the motivations are political, religious, or ideological, they remain largely hidden, so the connection with terrorism may not be revealed at all[20]. A permanent feature of the Internet is the 'invisibility' of its operation and, to some extent, also of the effects of activities conducted within it[21]. In many cases, it is difficult to hold terrorists legally accountable because there is insufficient knowledge about who they are. Therefore, it can be concluded that, as a result of the development of cyberspace, states have lost the ability to combat 'invisible' enemies. Moreover, in many cases, legal loopholes do not provide an opportunity to launch international cooperation in order to identify the enemy and his status[22].

The case of Mourad T. shows that it is difficult for the secret services of many states and the police to reach the wanted extremist (despite evidence such as contacts through fake Facebook accounts, instant messaging conversations, or photos). In the fall of 2016, the Polish Internal Security Agency (ABW) detained a Moroccan citizen, Mourad T., accused of collecting information in Europe for jihadists of the Islamic State (ISIS). After the attacks in Paris (2015), services around the world began to trace his connections with Abdelhamid Abbaoud, who contributed to the deaths of more than a hundred people. Interpol's findings show that in 2014, Mourad T. was banned from entering Türkiye. Despite this, at the end of 2014, he stayed in the Turkish city of Edirne and met with the most active ISIS extremists in Europe. Then he went along the "Balkan route" to Greece and further to Austria. There, based on false data, the Federal Office for Foreigners and Asylum issued him a residence card at the beginning of 2015. This enabled him to legalize his new identity as 19-year-old Mourad Sultan from Syria and obtain refugee status. After 'legalizing' his stay in Europe, he went to Poland, where he married a citizen of this state. He was finally detained due to a CIA investigation, which informed the Polish services that one of the seven ISIS scouts was on its territory (the others were stationed in Belgium[23]).

Terrorist organizations constitute a dynamic system that evolves over time and adapts to specific circumstances. Until recently, they were considered hierarchical and centralized structures within which leaders (at the very top) controlled the activities of the whole[24]. Therefore, the groupings had a properly defined chain of control and their hierarchical nature enabled them to effectively maintain cohesion. In modern terrorist organizations, the scope of the organization and the leadership have changed. It is related to the decentralization of the structure of

[19] P. Maj, op.cit., p. 79.
[20] S. Soesanto, op.cit.
[21] A. Rożej-Adamowicz, *Rola i znaczenie informacji pochodzących ze źródeł otwartych w zwiększaniu podatności na zagrożenia bezpieczeństwa w cyberprzestrzeni, ze szczególnym uwzględnieniem cyberterroryzmu*, "Terroryzm – studia, analizy, prewencja" 2022, 1, p. 182.
[22] Ibidem, p. 182.
[23] I. Kacprzak, G. Zawadka, *Jak namierzono terrorystę z ISIS*, Rzeczpospolita, March 2018, https://www.rp.pl/sluzby/art9895411-jak-namierzono-terroryste-z-isis (20.09.2023).
[24] S. Zeiger, J. Gyte, *Prevention of Radicalization on Social Media and the Internet*, [in.] A. Schmid (ed.), *Handbook, Part II: Prevention of Radicalisation*, Hague 2020, p. 360.

groups that currently have many operationally, logistically, and financially independent divisions (and focus on opposing 'enemies'). There has also been a change in the specialization of the executive structures of individual groups and in the recruitment of experts useful in conducting terrorist activities[25].

Taking into account the assumptions of Albert-László Barabási, a special feature of modern terrorist networks is adaptation and natural growth. These structures can expand, depending on needs, in any geographical direction, in any cultural or social environment, and create the most effective connections between nodes[26]. As a result of this state of affairs, due to the wider reach of terrorist networks, they can continue to operate even when one or more cells are seriously damaged or dismantled[27]. Thus, centralized groups with a hierarchical structure, which until recently operated within one country, have now become "networks". State borders have disappeared in their activities, and terrorism has become transnational. Extremists, united by one ideology to which they are ready to devote their lives, have ceased to represent one country and have become an organization of representatives of various nations from different parts of the world.

THE INTERNET AS A USEFUL TOOL FOR TERRORISTS

Cyberspace has several important features that make it an extremely useful tool for terrorists. Firstly, it enables fast and relatively safe "virtual" communication in real time between individual members and cells of terrorist organizations[28]. In turn, the use of encryption guarantees a high level of anonymity, which is extremely important for terrorists. The Internet is also a cheap means of communication and allows the functions of the armed forces, government institutions, or companies to be duplicated at low costs[29]. For example, in its activities, al-Qaeda used the network as part of its so-called 'cyberplanning', which preceded, among others, the attacks of September 11, 2001. Thanks to cyberspace, terrorists communicated with each other using encrypted connections and had the opportunity to collect information about their targets[30].

The Internet gives terrorist organizations an easier opportunity to obtain funds. The Internet's offer comes down not only to wide coverage and timeliness, but also to maintaining a certain degree of anonymity and security, both for donors and recipients of financial support. Organizations that argued for collecting and transferring funds to support their activities include

[25] M. Adamczuk, *Ewolucja strategii i metod działania islamskich ugrupowań terrorystycznych i ich wpływ na bezpieczeństwo Polski*, "Bezpieczeństwo Narodowe" 2011, 19, p. 205.
[26] A. Wejkszner, *Globalna sieć Al-Kaidy. Nowe państwo islamskie?*, Warszawa 2017, p. 128.
[27] S. Zeiger, J. Gyte, op. cit., p. 360.
[28] M. Lakomy, *Internet w działalności tzw. Państwa Islamskiego: nowa jakość cyberdżihadyzmu?*, "Studia Politologiczne" 2011, 38, pp. 156-157.
[29] T.W. Grabowski, *Wykorzystanie Internetu przez ugrupowania terrorystyczne*, [in:] *E-administracja publiczna i (nie)bezpieczeństwo cyberprzestrzeni*, M.K. Zwierżdżyński, M. Lakomy, K. Oświecimski (red.), Kraków 2015, p. 151.
[30] G. Małyga, *Dżihad epoki cyfrowej. Jak muzułmańscy terroryści z Państwa Islamskiego wykorzystują Internet w swojej działalności*, "Refleksje. Pismo Naukowe studentów i doktorantów WNPiD UAM" 2016, 14, p. 123.

al-Qaeda, Hamas, Lashkar-e-Taiba, and Hezbollah[31]. The first of these organizations is related to the story of Younis Tsouli, known as Irhabi 007, who, thanks to his online activities, became an extremely important figure for Jihad supporters. In the literature, he is referred to as the most famous virtual terrorist[32]. His activities began in mid-2003, when he decided to participate publicly on several websites, collecting information intended for Islamic fighters. Initially, he used free websites where he posted hacking tips and extremist propaganda[33]. However, due to the limited capabilities of these channels, he moved his activities to websites with better technical capabilities that required financing. To sponsor his activities, Tsouli stole the numbers of 37,000 people's credit cards, through which he earned approximately 3.5 million dollars in funds by laundering dirty money on a number of gambling sites[34]. His potential was noticed by the leaders of al-Qaeda. They asked him, among others, to create websites for the organization and run forums. All of this made Irhabi 007 the main distributor of the organization's materials in Iraq[35].

Terrorist organizations with large funds have a staff of media specialists and, in many cases, special departments responsible for media communication. The most famous are: As-Sahab (al-Qaeda), Al-Malahem Media (al-Qaeda in the Arabian Peninsula – AQAP), Al-Hayat Media Center and Al-Furqan Institute (ISIS[36]). Thanks to the work of specialists, numerous materials are published on the Internet, such as online magazines, books, manuals and films. A significant part of them consists of instructional content and propaganda for future fighters[37]. The first English-language magazine published online by terrorist organizations is "Inspire", published by AQAP. This periodical is of a propaganda and instructional nature. It includes, among others, interviews with leaders of terrorist groups, unit commanders, and Muslim clerics. Moreover, it documents the organization's achievements and describes in detail the terrorist attacks committed by it[38]. The magazine is addressed to a specific group of recipients residing in countries of Western civilization and uses a mechanism to motivate terrorist activities[39]. This mechanism involves arousing in the recipient a sense of hostility toward the living environment, then encapsulating this environment and depriving the reader of empathy toward potential victims. Then, by dehumanizing the enemy group, the fighters are motivated to take action[40].

[31] M. Jacobson, *Terrorist Financing and the Internet*, "Studies in Conflict & Terrorism" 2010, 33, p. 353.
[32] M. Jacobson, *Terrorist Financing and the Internet*, "CTC Sentinel" 2009, 2(6), June, https://ctc.westpoint.edu/wp-content/uploads/2010/06/Vol2Iss6-Art6.pdf (20.09.2023).
[33] B. Hołyst, J. Pomykała, *Wykorzystywanie kryptografii przez środowiska terrorystyczne*, "Prokuratura i Prawo" 2008, 2.
[34] M. Jacobson, op. cit., 2010, p. 355.
[35] G. Corera, *The world's most wanted cyber-jihadist*, BBC News, January 2010, http://news.bbc.co.uk/2/hi/americas/7191248.stm (20.09.2023).
[36] K. Wojtasik, M. Szczepański, *Nowoczesne Technologie i Internet w służbie organizacji terrorystycznych. Próba analizy socjologicznej*, "Studia Humanistyczne AGH" 2017, 16 (2), p. 47.
[37] Ibidem, p. 46.
[38] Ibidem, p. 47.
[39] J. Dziewanowski, *Magazyn AQAP „Inspire" narzędziem motywującym do podjęcia działań terrorystycznych*, "Przegląd Bezpieczeństwa Wewnętrznego" 2019, 20, p. 139.
[40] Ibidem, p. 153.

The global reach of the Internet means that even small terrorist groups have a reach comparable to much larger organizations and, with a relatively low expenditure of resources, can reach a wide audience and promote their activities on a large scale. In addition to using mainstream social media, organizations use a wide range of less popular platforms (Flickr, Vimeo, SoundCloud, or JustPaste.it) and also create their own blogs and websites. This "style of increasing visibility" of terrorist groups gives them the appearance of being more powerful than they may actually be. This phenomenon, referred to in the literature as "force multiplication[41]", has extremely significant effects because, by increasing its communication, even a small group can create the image of a large and strong group. Thus, by projecting the appearance of having a crowd of followers, it is also possible to increase the number of real followers of specific profiles[42].

It is also common today that with an Internet connection, the user can obtain much more than what is offered by common browsers such as Google or Yahoo, which can prohibit the publication of certain harmful content and block it[43]. The resources of websites hidden from most users (i.e., the darknet) have provided enormous opportunities for criminal activities, including terrorist ones. However, according to Pierluigi Paganini, access to common domains is much more beneficial for terrorists, as it allows them to reach a larger number of recipients[44]. However, this does not change the fact that terrorists use browsers such as Tor or I2P to ensure anonymity and to ensure that their identity is not detected by the services. One example concerns events that took place a few hours after the attack in Paris (13 November 2015). Cyberterrorism experts then found a new terrorist propaganda platform on the Tor network, which included translations into English, Turkish, and Russian. It was created by ISIS terrorists who decided to publish it in connection with repeated attacks by special services and hackers[45] "unraveling" their activities on open resources.

Some studies indicate that up to 90% of terrorist activity on the Internet is carried out through social media[46]. They allow terrorist organizations to recruit new active candidates, send friend requests, or upload videos. Moreover, the popularity of the Internet among terrorists is due, among others, to universal access to smartphones, the constant growth of its users, the ease of operating via it, as well as the lack of financial costs resulting from the use of the media available on it[47]. According to Statistica data, in July 2023, the number of Internet users was 5.19 billion, or 64.6% of the total world population. Of this number, as many as 4.88 billion

[41] S. Zeiger, J. Gyte, op. cit. p. 364.
[42] Ibidem, p. 364.
[43] B. Józefiak, *Terroryści niechętnie korzystają z darknetu*, Cyberdefence24, March 2016, https://cyberdefence24.pl/terrorysci-niechetnie-korzystaja-z-darknetu (20.09.2023).
[44] Ibidem.
[45] Ibidem.
[46] M. Marcu, C. Bălteanu, *Social Media – a real source of proliferation of international terrorism*, "Annales Universitatis Apulensis Series Oeconomica" 2014, 16(1), p. 164.
[47] G. Bator, M. Knapik, *Rola mediów społecznościowych jako instrumentu terroryzmu: analiza zamachu Brentona Tarranta*, "Annales Universitatis Paedagogicae Cracoviensis Studia de Securitate" 2020, 10(1), p. 59.

(59.9% of the world's population) were social media users[48]. The percentage of men using the Internet was 69% and that of women was 63%. Among Arab countries and Africa, this disproportion, taking into account the gender of the users, was even higher and amounted to approximately 10%. It is also not surprising that the largest group using the Internet's resources are young people aged 15-24. In Europe, the percentage of such users is as high as 98%[49]. This last aspect is extremely important considering the possibility of reaching the millennial generation and young people via social media. This group is more susceptible to radical thinking and manipulation used by terrorist networks. Furthermore, young people are actively involved in the spontaneous spread of radical thought and they easily pass on the information they receive to their peers[50].

Some terrorists post manifestos on the Internet, which are very popular among Internet users. Their dissemination helps to reach millions of recipients around the world[51]. In 2016, the Islamic State released the document *Media Operative. You Are a Mujahid, Too*, which contains a set of recommendations for actively promoting the idea of ISIS in the media, especially on the Internet[52]. One of the recommendations contained in the document referred to the necessary equipment for every fighter, or weapons, as well as a smartphone, which is to be used to document the fighters' activities and disseminate them. Charlie Winter even admits that among ISIS leaders, propaganda production and the channels for its dissemination are treated as more important than armed jihad[53]. The Islamic State's media message itself can be considered a well-prepared product, treated as a weapon with long-term reach, containing both positive and negative narratives, and building a sense of separateness in the group to which it refers. However, this top-down communication does not limit the personal activity of the organization's fighters and supporters. It even inspires the activity of individuals themselves who, in many cases, demonstrate a very good knowledge of using social media[54]. Therefore, social media turned out to be an extremely valuable tool for the organization, allowing it to reach ISIS's target audience, or the 'millennial generation', also in Western countries. For this group, the ISIS propaganda wing, al-Hayat, has even prepared productions imitating Hollywood action films and music videos[55]. The content of these materials includes translations into English and other European languages in order to understand the fighters' message.

[48] A. Petrosyan, *Number of internet and social media users worldwide as of July 2023*, Statistica, https://www.statista.com/statistics/617136/digital-population-worldwide/ (25.09.2023).
[49] Ibidem.
[50] G. Yumitro, et al., *The influences of social media toward the development of terrorism in Indonesia*, "Jurnal Studi Komunikasi" 6(1) 2020, pp. 20-21.
[51] Centrum Prewencji Terrorystycznej ABW, *Treści o charakterze terrorystycznym w Internecie*, 2023, https://tpcoe.gov.pl/cpt/materialy/1839,Tresci-o-charakterze-terrorystycznym-w-Internecie.html (20.09.2023).
[52] P. Polko, *Propaganda 2.0. Nowe media a charakter współczesnych konfliktów zbrojnych*, "Społeczeństwo i Edukacja. Miedzynarodowe Studia Humanistyczne" 2018, 29 (2), p. 163.
[53] Ch. Winter, *Media jihad: the Islamic state's Doctrine for Information Warfare*, International centre for the study of Radicalisation 2017, https://icsr.info/wp-content/uploads/2017/02/ICSR-Report-Media-Jihad-The-Islamic-State%E2%80%99s-Doctrine-for-Information-Warfare.pdf (20.09.2023), p. 3.
[54] P. Polko, op. cit., pp. 163-164.
[55] L. Blaker, *The Islamic State's Use of Online Social Media*, "Military Cyber Affairs" 2016, (1), p. 3.

Due to the increase in bandwidth and software development, terrorists can distribute even extremely complex content without causing major problems to all groups of potential recipients. Until recently, the mainstream media did not offer such an opportunity. One of the limitations is censorship and self-censorship[56]. Their use results primarily from serious consequences resulting from the publication of inappropriate content (one of which may be, for example, the withdrawal of the granted license). In the case of the Internet, the boundaries of censorship have moved significantly, and the offer of content presented every day is enormous. Furthermore, on the Internet, users can present their position at any time and comment on the content of publications or messages sent by the sender. In the case of traditional media, the message is one-sided and the recipient is not able to respond quickly to the published content.

One of the main goals of terrorists is publicity, which is an extremely important factor in their strategy[57]. Cyberspace has therefore become a useful means of transmitting the execution of acts of terror, giving the expected publicity, among other things, and intentionally creating a sense of anxiety and fear among recipients[58]. The terrorist attack carried out on 15 March 2019, in Christchurch, New Zealand, was broadcast live on the social networking sites Twitter and Facebook. Before going to the first target, the terrorist activated a small camera attached to his helmet, which made it possible to record the entire event[59]. Although the publication, which lasted approximately 17 minutes, was removed from social media platforms as it contained too many brutal and drastic scenes, copies were available on other websites. In turn, several minutes after the shooting ended, articles describing the event appeared on numerous websites[60]. The event ultimately dominated the media coverage of all national television and radio programs in New Zealand for the rest of the day. Terrorist visibility is therefore ensured not only by having more content on the Internet, but also by simultaneously attracting attention in other media (news).

THE USE OF THE INTERNET IN THE PROCESS OF RADICALIZATION

As mentioned earlier, initially, an important place of terrorist activity and radicalization of users was the darknet, or a part of the Internet invisible to users using standard browsers[61]. The hidden network was a source for acquiring new members, a space for exchanging information and instructions for the production of improvised explosives, and a place for sharing videos of executions, terrorist attacks, and other aspects of terrorist activities. Although the darknet allowed for almost anonymous, direct contact with other users, its reach could be described as significantly limited[62].

[56] G. Bator, M. Knapik, op. cit., p. 58.
[57] J. Bieniek, op. cit., p. 148.
[58] T. Wałek, *Pojęcie, geneza i klasyfikacja zjawisk terrorystycznych*, "Securitologia" 2018, 2(28), p. 116.
[59] W. Mastelarz et. al., *Zamachy w Christchurch z 15 marca 2019 roku*, "Securo" 2021-2022, 8-9, p. 80.
[60] G. Bator, M. Knapik, op. cit., p. 65.
[61] Słownik pojęć IT, *Darknet*, 2023, https://www.kei.pl/slownik/darknet (20.09.2023).
[62] G. Bator, M. Knapik, op. cit., p. 59.

With the development of technology, terrorism also began to evolve. Today, social media have become a tool for spreading propaganda, playing an increasingly important role in the radicalization of attitudes among young people, impressionable people, people in mental crisis, or individuals determined to act due to difficult life situations or inspired by world events[63]. It is worth noting that, thanks to the Internet, the process of radicalization in recent years has been taking place much faster and on a wider scale than it was a few years ago[64].

Radicalization is an individual process that leads to the adoption by an individual of extreme political, social, or religious ideals and aspirations. It is both a mental and emotional process. During it, the individual is prepared and motivated to engage in violent behavior[65]. A typical model of the process of radicalization among supporters of terrorist organizations consists of four stages that overlap each other[66]. The first is pre-radicalization, or the period leading to radicalization before falling fully into extremism. This is the time before adopting the jihadist ideology as one's own. The second stage is conversion, identification, or self-identification. The individual then decides to convert to Islam or begins to identify with the general idea of a "struggle". This is a time of searching, delving into extremist ideology, and discovering Islam in its radical version. The third stage is indoctrination and progressive bonding of the group. Contacts with active extremists, who determine the further path of activity, play an important role at this stage. As the process deepens and as a result of contact with people with similar views, the potential willingness to commit an attack in the 'name of Allah' increases significantly. The final stage of action, jihadization, is the planning or committing of acts of terrorism. During this period, there is active involvement in the search for targets, planning, and finally implementing attacks. Then, members of a given group consider it their duty to participate in terrorist activities, marking their life path as holy fighters of jihad[67].

In a situation where there are limited possibilities for using mosques or public places for the activities of Islamic radicals, virtual space is increasingly used to present extremist ideology, recruit, and train fighters[68]. In research conducted by Gregory Waters and Robert Postings, the aim of which was to map the global network of supporters of the Islamic State on Facebook, the authors analyzed the relationships between 1,000 profiles belonging to ISIS fighters or supporters and over 5.3 thousand connections between them[69]. The study showed that the profiles analyzed connect into a global network whose main task is to share ISIS propaganda materials.

[63] L. Wojnicz, *Walka z gwałtowną radykalizacją postaw w Unii Europejskiej. Podejście normatywne i instytucjonalne*, „Przegląd Zachodni" 2017, 2, p. 26.
[64] M. Adamczuk, *Rodzimy terroryzm jako zjawisko zagrażające bezpieczeństwu w Europie*, "Bezpieczeństwo Narodowe" 2011, 17, p. 73.
[65] A. Wilner, C.J. Dubouloz, *Homegrown Terrorism and Transformative Learning: An Interdisciplinary Approach to Understanding Radicalization*, "Global Change, Peace & Security" 2010, 22(1), p. 38.
[66] M. Adamczuk, *Rodzimy terroryzm*…, op.cit., p. 67-68.
[67] Ibidem, p. 67-68.
[68] Ibidem, p. 73.
[69] G. Bator, M. Knapik, op. cit., p. 60.

Their promotion mainly served to arouse the interest of people not associated with terrorist organizations and, consequently, to radicalize them[70].

Currently, the Internet is used at every stage of radicalization and terrorist activity, from financing, through fueling extremes, to full activity and execution of the attack[71]. Peter R. Neumann draws attention to a certain dangerous trend that has become visible in recent years, which is the decreasing age of people deciding to carry out terrorist attacks. Until recently, a man aged 18-25 was considered a typical terrorist. Today, even 12-year-old children are subjected to radicalism using young-generation platforms such as TikTok or Twitch[72]. In the context of the radicalization of young people on the Internet, the case of 19-year-old rapper Al-Afrat Hassan (who writes lyrics and performs songs published on Spotify and YouTube, serving to glorify ISIS murders[73]) and his 15-year-old fan is cited. They were both described as "fosters of hatred" toward infidel Muslims who were considered enemies and wanted to undergo martyrdom for Islam[74]. The teenagers were accused of planning an attack in central London after viewing a tutorial and propaganda videos from the organization[75]. The older teenager also allegedly purchased chemicals and other components for preparing a bomb on the Amazon platform[76]. In turn, in July 2023, Polish media reported the detention of an 18-year-old young man suspected of an attack using a suicide vest in Poland. According to information provided to the media by the Internal Security Agency, the teenager was a highly radicalized Islamic convert who started cooperating with representatives of the Islamic State[77]. The teenager's first contact with the organization took place when he was 16 years old. Then he and his family went to one of the Benelux countries. After returning to Poland, his contacts with ISIS members were carried out via the Internet, where he talked in groups with other fighters and collected information to prepare him for the attack[78].

However, the online threat that allows young people to contact militants is not limited to the darknet or social media. In 2022, the US Ministry of Homeland Security decided to launch research on radicalization resulting from online games, which increases the threat of terrorism.

---

[70] G. Waters, R. Postings, *Spiders of the Caliphate: Mapping the Islamic State's Global Support Network on Facebook*, Counter Extremism Projects 2018, https://www.counterextremism.com/sites/default/files/Spiders%20of%20the%20Caliphate%20%28May%202018%29.pdf (20.09.2023), p. 6.

[71] M. Adamczuk, *Rodzimy terroryzm*…, op. cit., p. 70.

[72] J. Wójcik, *Nastoletni terroryści. Granica radykalizacji obniża się*, Infosecurity24, 2023, https://infosecurity24.pl/za-granica/nastoletni-terrorysci-granica-radykalizacji-obniza-sie (20.09.2023).

[73] D. Gardham, *ISIS-supporting drill rapper Al-Arfat Hassan bought chemicals for terrorist bomb attack to kill 1,000 in central London helped by a 15-year-old fan, court hears*, 2023, https://www.dailymail.co.uk/news/article-12174395/ISIS-supporting-drill-rapper-Al-Arfat-Hassan-bought-chemicals-terrorist-bomb-attack.html (20.09.2023).

[74] Ibidem.

[75] D. Gardham, *Drill rapping 'terrorist' Al Arfat Hassan 'threatened blood and torment if his girlfriend left him', court hears*, Sky News, October 2022, https://news.sky.com/story/drill-rapping-terrorist-al-arfat-hassan-threatened-blood-and-torment-if-his-girlfriend-left-him-court-hears-12723779 (20.09.2023).

[76] R. Vinter, *London terror plot accused watched IS videos, court told*, The Guardian, 2023, https://www.theguardian.com/uk-news/2023/jun/08/london-terror-plot-accused-watched-is-videos-court-told (20.09.2023).

[77] *Dolnośląskie. Nastolatek planował zamach terrorystyczny przy pomocy pasa szahida*, Polsat News, 2023, https://www.polsatnews.pl/wiadomosc/2023-07-14/nastolatka-planowala-zamach-terrorystyczny-przy-pomocy-pasa-szahida/ (20.09.2023).

[78] *Nastolatek chciał przeprowadzić zamach w Polsce. Są nowe informacje*, Salon24, 2023, https://www.salon24.pl/newsroom/1313331,nastolatek-chcial-przeprowadzic-zamach-w-polsce-sa-nowe-informacje (20.09.2023).

The aim of the analyses is to include, among others, jointly developing methods to combat radicalization, counteract the increase in the terrorist threat in gaming communities, and protect platform users who are most susceptible to negative influence[79]. The main concern is the possible activities of recruiters of terrorist organizations and radicals disseminating extremist propaganda in players' networks and the lack of awareness of platform operators about the problems related to extremism in these communities. In the report of the Tech Against Terrorism organization published in January 2023 on current trends in the threat of terrorism and extremist ideology in cyberspace, it was noted that online gaming platforms are part of a broader problem[80]. The gaming networks used by extremists are used in various ways. In addition to spreading threatening content and establishing networks, extremists use online gaming platforms to perform voice and video verification of people who are to gain access to closed materials. Gaming addiction is not the only problem parents of the youngest users of gaming networks should be paying attention to today.

CONCLUSIONS

In the modern world, cyberterrorism is one of the greatest threats to both the state and society. Cyberspace gives terrorists the opportunity to operate in all areas of our lives, regardless of where we are. With globalization, the spread of societies and the flow of information, this phenomenon cannot be ignored. In the face of threats related to acts of cyberterrorism, the widespread use and continuous updating of security systems and mechanisms is becoming very important to ensure Internet security. Their nature should be comprehensive and concern both the level of transmission, processing, and storage of information.

Effective protection against cyberterrorism is a key task for the functioning of the state and its institutions. It is necessary not only to cooperate and coordinate institutional activities in consultation with specialists in the field of computer systems and security, but also to educate users (especially young people, who are most vulnerable to the influence of radicalization or disinformation). In combating online threats, the human factor always plays a key role, affecting both the attacker and the victim. Therefore, to counteract the effects of terrorist activities on the Internet, the state should introduce appropriate legal standards and provide effective solutions to protect individuals, remembering, however, that the regulations created do not violate their fundamental rights.

REFERENCES

Adamczuk Magdalena. 2011. "Ewolucja strategii i metod działania islamskich ugrupowań terrorystycznych i ich wpływ na bezpieczeństwo Polski" [The evolution of the strategies

[79] M. Fraser, *Radykalizacja w grach online. Zwiększone zagrożenie terroryzmem*, 2022, https://cyberdefence24.pl/polityka-i-prawo/radykalizacja-w-grach-online-zwiekszone-zagrozenie-terroryzmem (20.09.2023).
[80] J . Wójcik, *#CyberMagazyn: Platformy gier online celem ekstremistów*, CyberDefence24, 2023, https://cyberdefence24.pl/technologie/cybermagazyn-platformy-gier-online-celem-ekstremistow (20.09.2023).

and methods of operation of Islamic terrorist groups and their impact on the security of Poland]. Bezpieczeństwo Narodowe 19: 199-223.

Adamczuk Magdalena. 2011. "Rodzimy terroryzm jako zjawisko zagrażające bezpieczeństwu w Europie" [Homegrown terrorism as a phenomenon that threatens security in Europe]. Bezpieczeństwo Narodowe 17: 61-80.

Bator Grzegorz. Knapik Monika. 2020. "Rola mediów społecznościowych jako instrumentu terroryzmu: analiza zamachu Brentona Tarranta" [The role of social media as an instrument of terrorism: an analysis of the Brenton Tarrant attack]. Annales Universitatis Paedagogicae Cracoviensis Studia de Securitate 10(1): 56-69.

Bieniek Joanna. 2021. "Cyberterroryzm zagrożeniem bezpieczeństwa państw współczesnego świata" [Cyberterrorism as a threat to the security of states in the modern world]. Rocznik Bezpieczeństwa Morskiego 15: 145-164.

Blaker Lisa. 2016. "The Islamic State's Use of Online Social Media". Military Cyber Affairs. (1). https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1004&context=mca

Brickey Jonalan. 2012. "Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace". CTC Sentinel 5(8). https://ctc.westpoint.edu/defining-cyberterrorism-capturing-a-broad-range-of-activities-in-cyberspace/.

Centrum Prewencji Terrorystycznej ABW. 2023. Treści o charakterze terrorystycznym w Internecie [Terrorist content on the Internet]. https://tpcoe.gov.pl/cpt/materialy/1839,Tresci-o-charakterze-terrorystycznym-w-Internecie.html.

Collin Barry. 1997. "The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge". 11th Annual International Symposium on Criminal Justice Issues*:* The Future of CyberTerrorism:Where the Physical and Virtual Worlds Converge. http:// www.crime-research.org/library/Cyberter.htm.

Corera Gordon. 2008. The world's most wanted cyber-jihadist. BBC News, 16 January 2008. http://news.bbc.co.uk/2/hi/americas/7191248.stm.

Denning Dorothy. 2000. "Statement". Georgetown University. https://irp.fas.org/congress/2000_hr/00-05-23denning.htm.

Dziewanowski Jacek. 2019. "Magazyn AQAP 'Inspire' narzędziem motywującym do podjęcia działań terrorystycznych" [AQAP magazine 'Inspire' as a tool motivating terrorist activities]. Przegląd Bezpieczeństwa Wewnętrznego 20: 139-155.

Fraser Małgorzata. 2022. Radykalizacja w grach online. Zwiększone zagrożenie terroryzmem [Radicalization in online games. Increased threat of terrorism]. CyberDefence24. 22 September 2022. https://cyberdefence24.pl/polityka-i-prawo/radykalizacja-w-grach-online-zwiekszone-zagrozenie-terroryzmem.

Gardham Duncan. 2022. Drill rapping 'terrorist' Al Arfat Hassan 'threatened blood and torment if his girlfriend left him', court hears. Sky News. 18 October 2022. https://news.sky.com/story/drill-rapping-terrorist-al-arfat-hassan-threatened-blood-and-torment-if-his-girlfriend-left-him-court-hears-12723779.

Gardham Duncan. 2023. ISIS-supporting drill rapper Al-Arfat Hassan bought chemicals for terrorist bomb attack to kill 1,000 in central London helped by a 15-year-old fan, court hears. Mail Online. 8 June 2023.https://www.dailymail.co.uk/news/article-12174395/ISIS-supporting-drill-rapper-Al-Arfat-Hassan-bought-chemicals-terrorist-bomb-attack.html.

Górka Marek. 2017. "Wybrane aspekty definicyjne cyberterroryzmu i ich znaczenie w perspektywie polityki bezpieczeństwa" [Selected definitional aspects of cyberterrorism and their importance in the perspective of security policy]. Cywilizacja i Polityka 15: 295–315.

Grabowski Tomasz. 2015. "Wykorzystanie Internetu przez ugrupowania terrorystyczne" [The use of the Internet by terrorist groups]. In Marcin Zwierżdżyński. Mirosław Lakomy. Konrad Oświecimski (ed.). E-administracja publiczna i (nie)bezpieczeństwo cyberprzestrzeni [Public e-administration and cyberspace (in)security], Wydawnictwo Uniwersytetu Ignatianum w Krakowie.

Haverty Dan. 2019. IRA's Night of Long Knives' part in Northern Ireland's peace process. Irish Central. 8 November 2019. https://www.irishcentral.com/opinion/others/iras-night-long-knives-peace-process.

Hołyst Brunon. Pomykała Jacek. 2008. "Wykorzystywanie kryptografii przez środowiska terrorystyczne". Prokuratura i Prawo 2: 5-22.

Iqbal Mohammad. 2004. "Defining Cyberterrorism". UIC John Marshall Journal of Information Technology & Privacy Law 22(2): 397-408.

Jacobson Michael. 2009. "Terrorist Financing and the Internet". CTC Sentinel 2(6). https://ctc.westpoint.edu/wp-content/uploads/2010/06/Vol2Iss6-Art6.pdf.

Jacobson Michael. 2010. "Terrorist Financing and the Internet". Studies in Conflict & Terrorism 33(4): 353–363. https://doi.org/10.1080/10576101003587184

Józefiak Bartosz. 2016. Terroryści niechętnie korzystają z darknetu [Terrorists are reluctant to use the darknet]. Cyberdefence24. 30 March 2016. https://cyberdefence24.pl/terrorysci-niechetnie-korzystaja-z-darknetu.

Kacprzak Izabela. Zawadka Grażyna. 2018. Jak namierzono terrorystę z ISIS [How an ISIS terrorist was tracked down]. Rzeczpospolita. 11 March 2018. https://www.rp.pl/sluzby/art9895411-jak-namierzono-terroryste-z-isis.

Kadir Nadiah Khaeriah, Judhariksawan J., Maskun M. 2019. "Terrorism and Cyberspace: A Phenomenon of Cyber-Terrorism as Transnational Crime". Fiat Justisia 13(4): 333-344. https://doi.org/10.25041/fiatjustisia.v13no4.1735

Lakomy Miron. 2011. "Internet w działalności tzw. Państwa Islamskiego: nowa jakość cyberdżihadyzmu?" [The Internet in the activities of the so-called Islamic State: a new quality of cyber-jihadism?]. Studia Politologiczne 38: 156-157.

Lewis James A. 2002. Assessing the risk of cyber terrorism, cyber war and other cyber threats. Center for Strategic amd International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf.

Maj Przemysław. 2001. "Cyberterroryzm w stosunkach międzynarodowych" [Cyberterrorism in international relations]. Consensus. Studenckie Zeszyty Naukowe 1: 67-86.

Małyga Grzegorz. 2016. "Dżihad epoki cyfrowej. Jak muzułmańscy terroryści z Państwa Islamskiego wykorzystują Internet w swojej działalności" [Jihad of the digital age. How Muslim terrorists from the Islamic State use the Internet in their activities]. Refleksje. Pismo Naukowe studentów i doktorantów WNPiD UAM 14: 121–131.

Marcu Mihaela. Bălteanu Cristina. 2014. "Social Media – a real source of proliferation of international terrorism". Annales Universitatis Apulensis Series Oeconomica 16(1): 162-169.

Mastelarz Wiktoria. et al. 2021/2022. "Zamachy w Christchurch z 15 marca 2019 roku" [Christchurch attacks on March 15, 2019]. Securo. (8-9): 75-85.

Oleksiewicz Izabela. 2016. “Dilemmas and challenges for EU anti-cyberterrorism policy: The example of the United Kingdom”. Teka Komisji Politologii i Stosunków Międzynarodowych 11(3): 135-146.

Petrosyan Ani. 2023. Number of internet and social media users worldwide as of July 2023. Statistica. 20 September 2023. https://www.statista.com/statistics/617136/digital-population-worldwide/.

Polko Paulina. 2018. “Propaganda 2.0. Nowe media a charakter współczesnych konfliktów zbrojnych” [Propaganda 2.0. New media and the nature of contemporary armed conflicts]. Społeczeństwo i Edukacja 20(2): 159-174.

Polsat News. 2023. Dolnośląskie. Nastolatek planował zamach terrorystyczny przy pomocy pasa szahida [Lower Silesia. The teenager planned a terrorist attack using a shahid belt]. Polsat News. 14 July 2023. https://www.polsatnews.pl/wiadomosc/2023-07-14/nastolatka-planowala-zamach-terrorystyczny-przy-pomocy-pasa-szahida/.

Rożej-Adamowicz Anna. 2022. “Rola i znaczenie informacji pochodzących ze źródeł otwartych w zwiększaniu podatności na zagrożenia bezpieczeństwa w cyberprzestrzeni, ze szczególnym uwzględnieniem cyberterroryzmu” [The role and importance of information from open sources in increasing vulnerability to security threats in cyberspace, with particular emphasis on cyberterrorism]. Terroryzm – studia, analizy, prewencja 1: 147-199.

Salon24. 2023. Nastolatek chciał przeprowadzić zamach w Polsce. Są nowe informacje [The teenager wanted to carry out an attack in Poland. There is new information]. 14 July. https://www.salon24.pl/newsroom/1313331,nastolatek-chcial-przeprowadzic-zamach-w-polsce-sa-nowe-informacje.

Schjolberg Stein. 2006. Terrorism in Cyberspace – Myth or reality? https://www.cybercrimelaw.net/documents/Cyberterrorism.pdf.

Słownik pojęć IT. 2023. Darknet. https://www.kei.pl/slownik/darknet.

Smolski Wiesław. 2005. Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa [Cyberterrorism as a contemporary threat to state security]. In. Paweł Fiktus, Henryk Malewski, Maciej Marszał (eds). “Rodzinna Europa”. Europejska myśl polityczno-prawna u progu XXI wieku [“Family Europe”. European political and legal thought at the threshold of the 21st century, 481-494. Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.

Soesanto Stefan. 2000. Cyber Terrorism. Why it exists, why it doesn’t, and why it will. Real Instituto Elcano. https://www.realinstitutoelcano.org/en/analyses/cyber-terrorism-why-it-exists-why-it-doesnt-and-why-it-will/.

Szubrycht Tomasz. 2005. “Cyberterroryzm jako nowa forma zagrożenia terrorystycznego” [Cyberterrorism as a new form of terrorist threat]. Zeszyty Naukowe Akademii Marynarki Wojennej 1: 173-187.

Tafoya William L. 2011. Cyber Terror. LEB FBI. 1 November. https://leb.fbi.gov/articles/featured-articles/cyber-terror.

Vinter Robyn. 2023. London terror plot accused watched IS videos, court told. The Guardian. 8 June. https://www.theguardian.com/uk-news/2023/jun/08/london-terror-plot-accused-watched-is-videos-court-told.

Wałek Tomasz. 2018. “Pojęcie, geneza i klasyfikacja zjawisk terrorystycznych”. Securitologia. 28(2): 110-124.

Waters Gregory. Postings Robert. 2018. Spiders of the Caliphate: Mapping the Islamic State's Global Support Network on Facebook. Counter Extremism Projects. https://www.counterextremism.com/sites/default/files/Spiders%20of%20the%20Caliphate%20%28May%202018%29.pdf.

Wejkszner Artur. 2017. Globalna sieć Al-Kaidy. Nowe państwo islamskie? [Al-Qaeda's global network. A new Islamic state?]. Warsaw: Difin.

Wilner Alex S. Dubouloz Claire-Jehanne. 2010. "Homegrown Terrorism and Transformative Learning: An Interdisciplinary Approach to Understanding Radicalization". Global Change, Peace & Security 22(1): 33–51. https://doi.org/10.1080/14781150903487956.

Winter Charlie. 2017. Media jihad: the Islamic state's Doctrine for Information Warfare. International Centre for the Study of Radicalisation. https://icsr.info/wp-content/uploads/2017/02/ICSR-Report-Media-Jihad-The-Islamic-State%E2%80%99s-Doctrine-for-Information-Warfare.pdf.

Wójcik Jan. 2023. #CyberMagazyn: Platformy gier online celem ekstremistów. CyberDefence24. 18 February. https://cyberdefence24.pl/technologie/cybermagazyn-platformy-gier-online-celem-ekstremistow.

Wójcik Jan. 2023. Nastoletni terroryści. Granica radykalizacji obniża się. Infosecurity24. 28 July. https://infosecurity24.pl/za-granica/nastoletni-terrorysci-granica-radykalizacji-obniza-sie.

Wojnicz Luiza. 2022. "Walka z gwałtowną radykalizacją postaw w Unii Europejskiej. Podejście normatywne i instytucjonalne" [Fighting violent radicalization in the European Union. Normative and institutional approach]. Przegląd Zachodni 2: 25-45.

Wojtasik Karolina. Szczepański Marek. 2017. "Nowoczesne Technologie i Internet w służbie organizacji terrorystycznych. Próba analizy socjologicznej" [Modern Technologies and the Internet in the service of terrorist organizations. An attempt at sociological analysis]. Studia Humanistyczne AGH 16(2): 41-50.

Yumitro Gonda. et al. 2022. "The influences of social media toward the development of terrorism in Indonesia". Jurnal Studi Komunikasi 6(1): 16-31.

Zeiger Sara. Gyte Joseph. 2020. "Prevention of Radicalization on Social Media and the Internet". In. Alex P. Schmid (ed.) Handbook, Part II: Prevention of Radicalisation. Hague: International Center for Counter Terrorism.