CYBER TERRORISM AS THE EXEMPLIFICATION OF MEDIA TERRORISM

Agnieszka Kos[1]
Ajit Velu[2]

Abstract

Today, there are many forms of terrorism. Technological advances have enabled the development of new forms of terrorism, and these advances in technology are being exploited by terrorist organizations in finding new, more efficient methods of carrying out acts of terrorism. The authors of this article are highlighting the extremely important issue of cyber terrorism, which constitutes an act of terrorism carried out by means of available information technology. The article shows that this kind of terrorism can take various forms. It should be noted that the cyberattacks are being used by terrorists more frequently as a means of attacks. In doing so, they are exploiting the state and its citizens' growing dependence on cyberspace and social media.

Keywords: terrorism, cyber terrorism, media terrorism, media.

Introduction

The global nature and reach of media makes the phenomenon of media terrorism a challenge on a massive scale, and this is further aided by modern means of communication. Terrorists use media to not only to get publicity and spread propaganda, but also to intimidate the public. Terrorists make the most of technological advances, efficiently using the Internet, television, satellite and mobile telephony.

The symbiotic relationship between media and terrorism certainly is an aspect for discussion and consideration whether the media can exist without

[1] PhD, The Witelon State University of Applied Sciences in Legnica, Poland.
[2] MBA – INSEAD, France/Singapore.

terrorism, because terrorism without access to the media, is unusable. The mutual relationship between the media and terrorism is the subject of consideration for this work, aimed at highlighting cyber terrorism.

What is terrorism

This literature discusses two main issues related to the concept of terrorism. The first is to define the essence of terrorism as a political phenomenon, and the second is to study terrorism as a means of intimidation, aimed primarily at enforcing specific reactions and achieving desired result[3]. Ideologically motivated terrorism is the meticulously planned and organized actions of individuals or groups, taken to enforce certain behaviors[4]. Most often, acts of terrorism strike innocent bystanders and civilians, and involve the ruthless use of violence, both mental and physical, or with weapons.[5]

One definition of terrorism describes this phenomenon as follows: "Terrorism is a method of arousing social anxiety by repeated acts of violence, adopted by secret individuals, groups or state entities, elected for criminal or political reasons, while the ultimate goal is not the harm of the actual victims of the violence. Direct human victims usually are selected randomly, blindly or selectively to the target population, and serve only as media for their messages. The dialog between terrorists, victims and theultimate targets are used to manipulate the ultimate target (a community or communities), turning them into a target of terror or requests or the focus public attention, depending on whether the offender intended it to intimidate, compel or merely propaganda".[6]

The word terrorism contains a lot of related phrase.[7] In the world of communications and politics, definitions of relatively similar activities often vary depending on perspective. So guerrillas are people attacking military facilities and soldiers, while terrorists take aim at civilian targets and citizens.[8]

---

[3] See: K. Liedel, *Zarządzanie informacją w walce z terroryzmem*, Wydawnictwo TRIO, Warszawa 2010, p. 14.

[4] See: K. Mroziewicz, *Moc, przemoc i niemoc,* Wydawnictwo BRANTA, Bydgoszcz 2015, p. 50.

[5] See: K. Sławik, Password- „Terroryzm" [in:] *Nowa Encyklopedia Powszechna,* PWN, vol. 6, Warszawa 1997, p. 370-371.

[6] T. Goban-Klas, *Media i terroryści. Czy zastraszają nas na śmierć?,* Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2009, p. 17.

[7] See: W. Filipowski, *Internet – przestępcza gałąź gospodarki,* „Prokurator" 2007, no 1, p. 10.

[8] Ibid., p. 18.

Acts of terrorism, without references to ideological, political or religious justifications are nothing but malicious acts.[9] The greater part of terrorist organizations do not refrain from mass murder, utilizing explosives, and the use of profits from illegal sources. Generally, one can define the phenomenon of terrorism as a number of actions involving either the use of force, or the threat of using it, and a penchant for violence.[10]

Today, terrorism is an international phenomenon because, with globalization, follows the occurrence of violence on a greater scale. Modern means of communication exacerbate this state of affairs by showing the scale of the problem through television or virtual media. [11]

Media as an instrument to fight terrorists

As everyone knows, terrorism and the media remain in close symbiosis. Terrorists threaten public opinion, authorities, and society through media. On the other hand, journalists are looking for themes that will ensure them high audience.[12] Without media coverage, terrorist attacks fail to fulfill their most important role.[13] Information does not reach the public and does not cause the targets assumed by terrorist organizations.[14] Terrorists who use the mass media to amplify their own interests, are spreading fear through the media coverage, which has an excellent and quick reach.[15] Thanks to TV stations, viewers can follow the actions of the terrorists, which are still the subject of TV stories. Wide access to these resources and the extolling violence leads to a warped sense of realism for the mass viewer because terrorism in the world of media will become ordinary and mundane. That is why terrorists are seeking new forms of use of terror, which will surprise, attract and retain the attention of the media and the public for longer durations.

The modern world functions primarily based on communication. And the media in all its forms – mass, independent, private, global and national –

---

[9] See: B. Hoffman, *Oblicza terroryzmu,* Wydawnictwo Bertelsmann Media, Warszawa 1999, p. 150.

[10] See: K. Liedel, *Zarządzanie…,* p. 17.

[11] Ibid., p. 20.

[12] Ibid., p. 19.

[13] See: T. Hanausek, *W sprawie pojęcia współczesnego terroryzmu,* „Problemy Kryminalistyki" 1980, no 143, p. 12.

[14] See: K. Liedel (ed.), *Terroryzm w medialnym obrazie świata,* Wydawnictwo TRIO, Warszawa 2010, p. 19-20.

[15] See: J. Matusitz, *Symbolism in Terrorism: Motivation, Communication and Behavior,* Lanham-Boulder-New York-London 2014, p. 77.

has become a modern day necessity. Terrorists depend mostly on publicity in the mass media, with access to the largest number of customers. Their intent is to influence the public because it has to shape the consciousness of the viewer and attract his/her attention. Without the media, it would not be possible[16]. The effectiveness of terrorists is conditioned by the skillful use of available media. Their incompetent use may have unintended consequences, for example exposed or failed action. Internal media are fully supervised by terrorist organizations, but external and independent media reach the most customers, which is the prime goal of terrorists.

Mass media has tremendous influence on society, especially in times of impending crisis like during war, unemployment, economic crisis, or in the face of the terrorist threats. In such times, the authorities would be happy to use the help of the media to familiarize themselves with the public, as, it is a kind of guideline for them in making important decisions.[17]

Terrorism in the media must be based on violence, manipulation and exerting pressure. Public interest in the situation of terrorists would not be possible without communication through the mass media or their own media, and that is why the media and terrorism, like friends, interact with each other[18]. The mass recipient willingly tracks events related to acts of terrorism in the media, which give thorough reports on everything on a regular basis, fueling the situation with pertinent comments, while pursuing the goal of terrorists – publicity.[19]

But availability of media is not always a favorable tool for terrorists. "Media messages, instead of gaining sympathizers, may discourage supporters through the use of graphic material, who will not approve of abuse of women or children. The publicity which the terrorists primarily seek may not have the desired effect, since the majority of customers and the media will not support demands or actions of terrorist organizations.[20]

Organizations that undertake terrorist attacks use social media as information channels, which in this case are categorized into three levels: information channels, and the propaganda of a terrorist organization, systems of internal communication, mass media.

Today, the Internet is a place that brings together in the most powerful way for individuals to exchange information and beliefs or search

---

[16] See: T. Goban-Klas, *Media iterroryści…,* p. 78-79.

[17] Ibid.*,* p. 98-108.

[18] See: G. Weimann, C. Winn, *The Theater of Terror: Mass Media and International Terrorism,* New York 1994, p. 50.

[19] See: K. Liedel (ed.), *Terroryzm w medialnym…*, p. 21.

[20] See: T. Goban-Klas, *Media iterroryści…,* p. 88.

propaganda materials. Terrorists are able to communicate with each other not only through websites but also forums. Another advantage of electronic media is anonymity. The terrorists who freely move in the virtual world are able to publish materials, exchange experiences, occupy certain positions, share correspondence through email, chat rooms or forums. Terrorist organizations meet their assumptions just via the Internet, publishing propaganda materials, which are intended to persuade Internet users to the convictions of terrorists. In addition to the assumptions of propaganda and training, there are calls for participation in the attacks and coordination of attacks through chat rooms and discussion forums.[21]

Public executions are aimed to affect the recipient in such a way that everyone who sees them knows what the consequences of collaboration with the enemy or lack of cooperation with terrorists will be. The actions of terrorists supported by electronic media are becoming more frequent due to the technological progress.[22] Cyber terrorist attacks are one of the newer forms of the use of terrorism, for example blocking of websites, hacking, gaining control over and destruction of systems using viruses.[23]

Cyberspace the largest arena of war for terrorists, where with the click ofa mouse they can move and reach audiences around the world. One can say that the Internet is the safest place that allows someone to communicate freely and operate or appoint groups affirming the terrorists. Individuals recruiting and checking for potential jihadists log on to online forums and chat rooms, acquiring volunteers from all over the world[24].

Materials related to the attacks available on the Internet spread much faster than any mentions in the traditional media. Information and Internet resources are continuously available, while broadcast on television is not. Movies, which are available for virtually every Internet user, show how brutal and dangerous tool is the Internet. Interactivity of the Internet allows for the inclusion of communication between the recruiter and the recruit, and all this happens with a computer and other portable devices with the ability to surf the Internet.[25]

"If terrorism can be considered as a specific communication process, it is nota big surprise that the effect of the information revolution is used with ingenuity and increasing efficiency by extremists. Even sworn

---

[21] See: K. Liedel (ed.), *Terroryzm w medialnym…,* p. 107-117.

[22] See: P. Pawlak, *Rola propagandy w terroryzmie*, „e-Terroryzm.pl", no 2/2013 (14), 10.05.2016 y.

[23] See: K. Liedel (ed.), *Terroryzm w medialnym…,* p. 118-119.

[24] See: D. Verton, J. Brownlow, *Black Ice: The Invisible Threat of Cyber-Terrorism,* Osborne 2003, p. 120.

[25] See: W. Dietl, K. Hirschmann, *Terroryzm*, PWN, Warszawa 2011, p. 208-211.

enemies of modernity are willing to use the most modern communication techniques".[26]

Cyber terrorism

Cyber terrorism is a concept closely associated with the term cyberspace, which is also referred to as the network of networks.[27] Describing the phenomenon of cyber terrorism is therefore impossible without explaining what cyberspace really is. The literature defines cyberspace as a general relationship of the virtual dimension, formed and functioning due to physical manifestations like computers.[28] "Cyberspace as a sphere of human activity fundamentally differs from physical space. First of all, attention should be paid to the independence of the place occupied in the physical space.

Cyber terrorism is an act of terrorism, however, it uses information technology to carry out attacks in networks, exchanging information or transmitting requests and threats. Modern computer networksare nothing but a "nervous system" of the state. Disruption of this system could have dire consequences within the security and the economy of the country.

Cyber terrorism takes many forms: planting bombs in strategic places, hackers taking control over systems.[29] „The threat of cyber terrorism is also a propaganda aspect. The message of the terrorist ideology, supported by the message about violence and the risk it poses to the stability of societies and states, is an expression of the struggle for "government of souls" and to gain dominance in the sphere of information and the impact on broad society groups".[30] Cyber terrorism are also activities having a criminal or terrorist character, taken in cyberspace by criminal or terrorist groups.

Cyber terrorism, with the progress of technology, will grow at an alarming rate, and so will in a matter of time scenarios of flooding a city, cutting off electricity to the wider area by socio technicians – spies and data thieves.[31]

---

[26] K. Liedel (ed.), *Terroryzm w medialnym…,* p. 155-156.

[27] See: T. R. Aleksandrowicz, *Sieciowy paradygmat bezpieczeństwa państwa w stosunkach międzynarodowych,* Akademia Obrony Narodowej, Warszawa 2013, p. 72.

[28] See: A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie,* Oficyna Wydawnicza ASPRA-JR, Warszawa 2003, p. 37.

[29] See: K. Liedel, *Zarządzanie…,* p. 24-25.

[30] Ibid., s. 25.

[31] See: T. Trejderowski, *Kradzież tożsamości. Terroryzm informatyczny,* Wydawnictwo ENETEIA, Warszawa 2013, p. 165-166.

The advantage of cybercrime is the anonymity of operations, which is why cybercriminals are seeking to disguise their identity on the Internet. Unquestionable facilitation is to use a wireless network, which is characterized by a low level of security. Thanks to the wireless Internet, cybercriminals can carry out an attack without arousing suspicion or carry out an attack to steal data. Cyber terrorist activities can be divided into: activism, hacking and cyber terrorism.

Activism is causing destruction through the use of the network for propaganda purposes that support campaigns. It gathers a group of supporters on social networks and enables communication between criminals. On the other hand, hacking is associated with destructive aims, however, it does not entail major and significant losses. Hacking bring together primarily user groups capable of blocking websites and making changes to sites.

Cyber terrorism is associated with attacks of terrorist groups in the network and these result in enormous property damage in the real world, eg. blocking of communication, which may lead to road accidents or plane crashes. When it comes to classifying cyber terrorism through the prism of its targets, the attacks are made, inter alia, to: telephone and Internet networks, transport and storage networks, financial institutions and gathering valuable goods, logistics systems, systems involved in the production and distribution of energy or water, the police, military and rescue services. The effects of the attacks usually lead to a domino effect, which further demonstrates the scale of the threat of cyber terrorism.[32]

Not without reason it is said that in the future, wars probably will have a virtual dimension. One of the reasons is the lower cost of the attacks on the network, compared to the classic terrorist activities. Furthermore, operations of this type do not require specialized knowledge, as a tool that allows one to attack is a computer, the thing now in the possession of almost every human being.[33]

The times of buying weapons or explosives has given way to viruses, worms, spam messages or social engineering activities. The most frightening is the fact that the target attacked most often does not realize that it has just become the victim of the attack. It is extremely difficult to discern who undertook the attack, with what intention, what skills and tools were used. Internet, where it is easier to act anonymously, becomes an ideal field for the actions of terrorists who give false information and use pseudonyms, without worrying about the physical location of their activity. Members of

---

[32] Ibid., p. 167.
[33] See: A.M. Colarik, *Cyber Terrorism. Political and Economic Implications,* Hershey-London-Melbourne-Singapore 2006, p. 40.

terrorist groups through a global network can organize, communicate, plan attacks, carry out operations anywhere in the world, which makes the detection of the source of the attack nearly impossible.[34]

Organizations that use new techniques fall into three categories. The first of these is a group that uses the internet network for obtaining necessary information. The second one is a group focused on the destruction of information systems through violence. The third category includes activities of extremists in the network – this is the use of new techniques to carry out cyberattacks.[35] Terrorist organizations that use the Internet to conduct war have some common characteristics. The activities are characterized by the building and changing communication and coordination plans. Organizations can be linked together in an informal way, there is no structure, which mainly manages the organization. Communicating with people outside the organization is the last characteristic of organizations that use the network.[36]

Usage of the internet by cyber terrorists increases the chance of the emergence of clusters of terrorist groups, which, thanks to the network will establish dialogue between themselves. This may result in the fact that members of the organization will plan in virtual world meetings, as well as operations in the real world, then they will destroy evidence of their presence on the Internet, scattering themselves or simply modifying or destroying data.[37] Given the global reach of the Internet, each with its customers around the world can obtain information from the network. Both true and false information is spread on the Internet. Through such information, terrorist organizations reach internet users, spreading ideologies and propaganda campaigns. Some available materials are designed to carry out a psychological war, manipulate, build anxiety.[38]

Cyber terrorism can also cause social harm, for example, attacks against stations which treats water in big cities; attacks on systems of traffic, air or rail management. These attacks are so easy to perform since the control system connects to the Internet network. Systems of critical infrastructure

---

[34] See: N. Noga, *Cyberterroryzm – nowe oblicze terroryzmu* [in:] e-Terroryzm.pl no 4/2013 (16), 7.05.2016 y.

[35] See: R. Białoskórski, *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku – zarys problematyki,* Wydawnictwo Wyższej Szkoły Cła i Logistyki, Warszawa 2011, p. 59.

[36] See: N. Noga, *Cyberterroryzm – nowe oblicze terroryzmu* [in:] e-Terroryzm.pl, no 5/2013 (17), 17.05.2016 y.

[37] See: K. Liedel (ed.), *Sieciocentryczne niebezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji,* Wydawnictwo DIFIN, Warszawa 2014, p. 100.

[38] See: A. Chorobiński, *Walka informacyjna, jako fundamentalny składnik działalności terrorystycznej   w przyszłości,* p. 6, http://konkursy.byd.pl/userfiles/files/chorobinski.pdf, 20.05.2016 y.

in the West are largely managed and accessed via the Internet. In the case of any kind of irregularity in these systems, for example outdated software – it is easier to make an attack on these systems. As you can guess, the effects of this attack can consume an incredible number of casualties, and it first of all may be the target of terrorist organizations. Yet another system vulnerable to attacks of cyber terrorists can be a building management system, responsible for access of monitoring, air conditioning, elevators or doors. The effects of cyberattacks are as follows: permanent or temporary loss of control over the performance of activities, damage to infrastructure, data leakage, casualties, as well as the propaganda and media effect.[39]

Cyber terrorists use a variety of techniques to carry out attacks. Tools, which they use on the network are, for example, malicious software, bacteria, which are programs that breed in the victim's processor memory and makes it difficult to use a computer. Worms are programs that exploit vulnerabilities in e-mail or websites to spread themselves in the network. Viruses are codes that cause changes in the functioning of the equipment, they can damage data and infect more areas in the computer.

Today, terrorism has many variations, but technological progress is responsible for aiding the development of new forms and methods used by terrorist organizations. Cyber terrorism is an extremely difficult phenomenon to define, in addition, it is a challenge to the twenty-first century, which is both a puzzle and a problem, because cyber terrorist attacks will be more frequent methods of fighting for terrorists who will use dependence on cyberspace in the functioning of states. Internet and critical infrastructure nowadays play a very important role in society, which is why they are the weakest point, so hitting this point may undermine the efficient operation of the entire state. The attacks, which took place September 11, 2001 are proof that even a small group, but well-organized and prepared, which has technological and financial support, is capable of influencing the infrastructure of a whole state. Victims of attacks in cyberspace can become every country that has a computerized economy.

Conclusions

Cyberattacks are very real and highly likely. Perhaps in the future, wars in cyberspace will affect the disposal of critical infrastructure of countries, which triggers a new look at the issue of cyber terrorism. The Internet has become a target, but also a tool in the hands of terrorists who are becoming

---

[39] See: K. Liedel (ed.), *Sieciocentryczne…,* p. 153-154.

perfect strategists, who are diligently using its resources and deepening the knowledge about the targets. One may say, that cyber terrorism is an easy tool to use, because it does not require a physical presence or logistical support. Persons who carry out attacks in cyberspace are certain of the fact that they themselves will not suffer physical injury and will not have to endanger their own lives. These attacks also do not require the act of suicide. In addition, a terrorist does not need to have special skills or knowledge, because he or she can hire relevant persons who will break security for the appropriate payment. It is worrying that countries still have limited awareness of attacks or crimes in cyberspace, which leads to the inability to issue a sanction.

The issue of cyber terrorism is therefore a problem of international security in XXI century. The internet plays an increasingly important role in human life with tremendous benefits associated with the use of the network. However it also increases the risk of new forms of terrorism. To carry out the attacks one does not need an army of terrorists or violation of a state border – the attack itself can cause total paralysis of information systems, and thus destabilize a state.[40]

References:

Aleksandrowicz T. R., *Sieciowy paradygmat bezpieczeństwa państwaw stosunkach międzynarodowych,* Akademia Obrony Narodowej, Warszawa 2013.

Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku – zarys problematyki,* Wydawnictwo Wyższej Szkoły Cła i Logistyki, Warszawa 2011.

Bógdał-Brzezińska A., Gawrycki M. F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie,* Oficyna Wydawnicza ASPRA-JR, Warszawa 2003.

Colarik A. M., *Cyber Terrorism. Political and Economic Implications,* Hershey-London-Melbourne-Singapore 2006.

Chorobiński A., *Walka informacyjna, jako fundamentalny składnik działalności terrorystycznej w przyszłości,* http://konkursy.byd.pl/userfiles/files/chorobinski.pdf

Dietl W., Hirschmann K., *Terroryzm*, PWN, Warszawa 2011.

Filipowski W., *Internet – przestępcza gałąź gospodarki,* „Prokurator" 2007, no 1.

Goban-Klas T., *Media i terroryści. Czy zastraszają nas na śmierć?,* Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2009.

Hanusek T., *W sprawie pojęcia współczesnego terroryzmu,* „Problemy Kryminalistyki" 1980, no 143.

Hoffman B., *Oblicza terroryzmu,* Wydawnictwo Bertelsmann Media, Warszawa 1999.

Liedel K., *Zarządzanie informacją w walce z terroryzmem*, Wydawnictwo TRIO, Warszawa 2010.

---

[40] See: N. Noga, *Cyberterroryzm – nowe oblicze terroryzmu* [in:] e-Terroryzm.pl no 4/2013 (16), p. 15, 29.05.2016 y.

Liedel K. (ed.), *Terroryzm w medialnym obrazie świata,* Wydawnictwo TRIO, Warszawa 2010.

Liedel K. (ed.), *Sieciocentryczne niebezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji,* Wydawnictwo DIFIN, Warszawa 2014.

Matusitz J., *Symbolism in Terrorism: Motivation, Communication and Behavior,* Lanham-Boulder-New York-London 2014.

Mroziewicz K., *Moc, przemoc i niemoc,* Wydawnictwo BRANTA, Bydgoszcz 2015.

Noga N., *Cyberterroryzm – nowe oblicze terroryzmu* [in:] e-Terroryzm.pl no 4/2013 (16).

Noga N., *Cyberterroryzm – nowe oblicze terroryzmu* [in:] e-Terroryzm.pl, no 5/2013 (17).

Pawlak P., *Rola propagandy w terroryzmie*, „e-Terroryzm.pl", no 2/2013 (14).

Sławik K., Password – „Terroryzm" [in:] *Nowa Encyklopedia Powszechna,* PWN, tome 6, Warszawa 1997.

Trejderowski T., *Kradzież tożsamości. Terroryzm informatyczny,* Wydawnictwo ENETEIA, Warszawa 2013.

Weimann G., Winn C., *The Theater of Terror: Mass Media and International Terrorism,* New York 1994.

Verton D., Brownlow J., *Black Ice: The Invisible Threat of Cyber-Terrorism,* Osborne 2003.