CYBERTERRORISM IN THE ONLINE MEDIA SPACE

Faton Murseli
University of Tetovo, Tetovo, North Macedonia, faton.murseli@unite.edu.mk

Abstract: Terrorism is present in almost all parts of the world today. We cannot stop this phenomenon, but we can try to prevent it or control it to some extent. Terrorist organizations have different strategies for online terrorism, and they change and advance over time. Before the development of information technology, terrorist attacks were mainly carried out in densely populated areas and the victims were usually civilians, and the primary purpose of these attacks was to intimidate the target group. Today's terrorist attacks are much more sophisticated, and, as a rule, involve the use of advanced information technology. Advances in information technology have also imposed changes within the structures of terrorist organizations. Thus, terrorist groups used to be closed and it was difficult to communicate with them. Meanwhile, today with the help of computer technology they are ubiquitous, members of terrorist groups communicate with each other faster and easier, but at the same time they are also more open to the outside world. Terrorist groups today promote their ideology through various websites and social networks, and publish photos and videos on almost all platforms. With the help of certain systems, they manage to collect information about their targets as well as all the data necessary to carry out a terrorist attack. The motives for joining a terrorist organization are numerous and heterogeneous. Some join motivated by the desire for power or because membership represents self-fulfillment for them, while others are forced or threatened. Thanks to the wide availability of propaganda materials today, members have seen and been influenced by the content of the Internet to join a terrorist group voluntarily, or in other words they self-radicalize. A key factor contributing to the growing propensity for terrorist acts in the virtual world is the anonymity that attackers in cyberwarfare often manage to maintain. Thus, the Internet, in addition to its many undoubted positive social effects, has also brought about the possibilities of simpler and more effective functioning and expansion of terrorist organizations and their propaganda. In addition, there has been an attempt to unify terrorists and guerrillas, and for that reason the comparison between them has often been mentioned. This has resulted in the main difference being that guerrilla wars are more often fought in the mountains, far from cities, while terrorists attack unarmed opponents in the centers of state power. Intimidation of the population is the main goal of terrorists. Bombings, assassinations and kidnappings are among the most common methods practiced by terrorists.
Keywords: Terrorism, online terrorism, information technology, cyberwarfare.

1. INTRODUCTION

The word terrorism comes from the Latin word "terror" which means to cause constant fear to achieve a certain goal. This concept also includes the threat of violence or the use of violence to achieve certain political goals. Many authors have approached the issue of cyber terrorism in two dimensions, namely whether it is an ideology or a strategy to achieve the goal. The most accessible understanding is that cyber terrorism is not an ideology but a strategy used by terrorists, most often motivated by political views, which in most cases are oppositional, that is, political views that do not agree with the leadership of power. In addition, an attempt has been made to unify terrorists and guerrillas, and for that reason the comparison between them has often been mentioned. This has resulted in the main difference being the fact that guerrilla wars are more often fought in the mountains, far from cities, while terrorists attack unarmed opponents in centers of state power. Terrorists' main goal is to intimidate the population. Bombings, assassinations, and kidnappings are among the most common methods terrorists practice. A person does not become a terrorist quickly, but it is a process conditioned by some social or political aspects. Potential members of terrorist organizations usually start by providing support to terrorists and gradually become loyal members. The motivation of a potential terrorist is that he quickly becomes desirable by the organization and meets the conditions of the organization he joins (Bilandzic, 2010, pp. 837-859). First, in a terrorist organization, a sense of acceptance and self-esteem develops in the members and pressure is exerted on them, through which pressure he would be forced to belong to that (terrorist) community and pursue its goals. These organizations, in a psychological spectrum, build a system of thought that dehumanizes its members to the point where even the act of suicide would be considered acceptable. Once members join, they are not allowed to leave the organization and the punishment for doing so is brutal, usually lethal (Bilandzic, 2010, p. 840). Many researchers believe that modern mass terrorism began with the attack on the United States of America on September 11, 2001. After the terrorist attack on the Twin Towers, terrorism in the society we live in was strengthened and American state structures called on the rest of the world to fight together against terrorism (Maric, 2012, p. 89). However, it should be noted that terrorism is a massive phenomenon and has been present even earlier. For example, in the 1960s, there were over

600 organized terrorist groups active in the world. Since then, over 80,000 terrorist crimes have been committed (Bilandzic, 2010, p. 839).

Terrorists are like soldiers, they use a strategy of impersonality, where for them the victims are counted only as numbers and not as human beings. A terrorist also claims the possibility of unintentional (accidental) killing, and this may be either as a justification, or even driven by psychopathological causes (Tomasevski, 1980, pp. 162-166). Terrorist attacks became more frequent during the 20th century, but terrorism on a global scale is increasingly emphasized in the 21st century. Almost all media outlets report on terrorist attacks, and most Internet portals contain sections called "terrorism" (Maric, 2012, p. 91). Among the most famous examples is the media coverage of the terrorist attack on the Twin Towers in the USA on September 11, 2001. The media showed images of the collapse of the so-called "twin towers" all over the world, and many media outlets followed the sequence of this event live (Tomljanovic, 2016, p. 21).

Modern terrorism is strongly linked to the progress of technology, especially information and communication technology, for which reason virtual media (Internet media) that are today increasingly widespread and accessible play an important social role. Another key factor in this whole story is the fact that this factor also increases the arms production industry. Terrorism of the modern era, as we know it, begins at the height of the Cold War and the development of national movements. During this period, many terrorist organizations and groups were created that undertake terrorist acts as their main political action, more precisely through terrorist acts, the realization of their political interests and goals was achieved (Maric, 2012, p. 93).

The first priority of terrorists is to cause as much damage as possible to a certain group of people inside or outside the countries where they operate.

Recently, terrorist organizations have used a non-standard method of warfare. They use information as a weapon of war because information in today's world is valuable and brings much more consequences than standard methods of warfare (Maric, 2012, p. 93). The use of modern technologies has enabled terrorists to exchange information better and faster, to carry out secret communication or even to obtain financing. Financial support is a key element that ensures the survival and functioning of terrorist organizations (Maric, 2012, p. 93). Terrorist groups are also financed with the help of the Internet through voluntary donations and funds that the authorities barely manage to control. An example is Hizb-ut-Tahrir, an international pan-Islamist organization, which uses PayPal to transfer donations (Babic, 2015, p. 17). Terrorist groups today have larger financing systems and are much more complicated to track. The reason for this is that a significant amount of terrorist sponsorship is done under the guise of humanitarian aid (reported as humanitarian organizations) (Maric, 2012, p. 94). Terrorism in its essence has not changed throughout history, but contemporary terrorism is significantly more sophisticated than it was before because they have advanced war techniques by modernizing them. Today we can see news about terrorism and terrorist attacks every day in the media, however suicide attacks are not a form of attack in this era. Today, the suicide method is more present among jihadists (Maric, 2012, p. 95). Mariÿ defines suicide terrorism as "the willingness of an individual to sacrifice his life to destroy or attempt to destroy a goal, in order to achieve another political goal (Maric, 2012, pp. 95-96). The philosopher Jean Baudrillard interprets contemporary terrorism as "terror against terror" and he compares it to a virus, emphasizing that it is everywhere around us and has become part of the culture that is fighting against it. He also calls contemporary terrorism the "fourth world war" and concludes that terrorism does not allow any world order to dominate, but this philosopher even opposes globalization, which, according to him, is as immoral as terrorism itself. Baudrillard sees a key moment in the manifestation of contemporary terrorism in the game of terrorists "with themselves offensively" to serve intuition against an almost perfect system. Terrorism has become a weapon used against the entire state system, even at the cost of the terrorists' lives (Baudrillard, 2023, p. 280). Authors Gayraud and Senat emphasize the excellent adaptability of terrorist organizations to today's modern world, taking into account the unlimited access to the Internet, which allows terrorists to communicate freely.

2. MATERIALS AND METHODS

The method used in this research is the method of analyzing the data content of terrorist organizations and groups, based on previous scientific research on this topic. So, in short, we are presenting the collection of data from terrorist groups. The tool that enables today's terrorists to quickly collect information about the target of the attack, about the people involved in the attack and the like is precisely the Internet. Namely, with the help of search engines such as “Street view” and “Google Maps”, the perpetrators manage to locate the buildings that are in their attack plan, all the roads they need or even air traffic that help and enable a simpler and more efficient attack. When it comes to specific people, social networks are the location of almost all the personal data of the targets, their habits and daily activities, which do not require much time or financial resources for terrorists to find the targeted person or group. To make it more concrete, we are taking the example of a Japanese cult called “Aum Shinrikyo” founded in

1984, which in 2000 monitored the movements of 150 Japanese police vehicles, with the help of GPS[1]. In addition to the GPS method, there are also GSM[2] methods, the world standard for mobile telephony, and GPRS[3], a radio wave data communication service, which are also used by terrorist and anti-terrorist groups (Babic, 2015, p. 16).
When it comes to data collection, attackers gain access to a target's protected data in many ways. Among the most common methods is an illegal system for cracking passwords and stealing virtual identities. Open source intelligence, or OSINT, is a technique used by members of Al-Qaeda, as well as open source Jihad, through which they gathered information and published this type of method publicly in their magazine "Inspire" (Babic, 2015, pp. 16-17). "Inspire" is an English-language online magazine published by the Al-Qaeda organization. The magazine is one of the many ways in which the organization uses the Internet to reach its audience. Many international and domestic extremists have been motivated by the radical interpretations of Islam in this magazine and, in some cases, have used its bomb-making instructions in their attempts to carry out terrorist attacks.
In today's modern world, access to the Internet and electronic technology has enabled almost every person to easily access and afford information about simple and free hacking lessons (Nelson, Choi, Iacobucci, Mitchell, & Gagnon, 1999, pp. 24-30).

3. RESULTS

The word cyber comes from the English word "cyber", which "refers to the visible reality created with the help of a computer" (Croatian Encyclopedia, 2022). Cyberterrorism is an attack for political purposes by individuals or groups focused on computer programs, data systems, i.e. a non-physical war (Vukoviq, 2012, p. 18). Authors Gordon and Loeb state that the possibilities of technology are endless when it comes to cyberterrorism. Theft of confidential data, deletion of data, modification of websites, Website attacks and viruses are the most common examples of cyberattacks, while their targets are government computers, financial networks and power plants (Jazecski & Colarik, 2020, p. 2). Among cyber scientists in the information process, there has been discussion about the beginnings of terrorist attacks, and it is believed that the first attacks began in 1997 on several embassies in Sri Lanka. Namely, an Internet terrorist group in Sri Lanka carried out an attack on electronic mail (E-mail) systems to disable such communication for a certain period of time in protest against the government. The message sent was: "We are the Black Tigers of the Internet and we are doing this to disrupt your communications". This attack is considered the beginning of future forms of cyber terrorism. There are two forms of terrorist attack that can be classified as cyber terrorism. In the first form, the target of the attack is information technology. Terrorists aim to disrupt communication or physically destroy technological devices, which is the ultimate goal. In another form, information technology is understood as a weapon for a specific attack. The most common example would be changing the function of technology to one's advantage (Perešin, 2022, p. 106). In cyberspace, information technology is used both as a strategy and as a target, and almost always as a weapon. Attackers do not necessarily have to be physically present at the location where the attacks are carried out, these attacks require a smaller amount of funds, and there is the possibility of hiding the identity of the attacker himself (Vukoviq, 2012, p. 19). In 1998, the website and email system of the Bhabha Atomic Research Center in India were hacked by three anonymous attackers who in a later online interview explained their action as a sign of protest against the then nuclear explosions (Briere, 2023) (Janczewski & Colarik, 2021, p. 2). More recently, terrorist attacks can also be carried out with the help of drones. Increasingly, world leaders say that there is a fear of the misuse of drones by foreign actors and terrorist groups. Namely, groups could trigger explosions at nuclear power plants, as well as use drones to distribute nuclear materials in large cities, which would lead to widespread panic, and perhaps force a population movement out of fear. Fears also exist because jihadists are buying drones to transport nuclear material (Sovilj & Sovilj, 2017, p. 262). The Islamic State uses drones in its attacks in Syria and Iraq, and it is considered that they plan to use more drones in larger attacks on more people (Sovilj & Sovilj, 2017, p. 257).

4. DISCUSSIONS

In contemporary terrorism, "online" technology is used by terrorists and extremists with the aim of carrying out their actions through a very large number of electronic devices that allow for secret and easy communication. Among the

[1] GPS (Global Positioning System) – The Global Positioning System is a system of 31 satellites that orbit the earth and help locate the movements of all vehicles on earth.
[2] GSM (Global System for Mobile communication) – The Global System for Mobile Communications is a digital cellular network widely used by mobile phone users in Europe and other parts of the world.
[3] GPRS (General Packet Radio Service) – General Packet Radio Service is a mobile communication standard that operates on 2G, 3G, 4G or 5G mobile networks to enable medium-high speed data transfers using radio wave-based technologies.

most common forms of information exchange are SIM cards for mobile devices that are quite affordable and are both legal and easily available. Also with the help of external USB memory cards, large amounts of data can be exchanged without problems. Terrorists also use satellite phones that enable communication in less populated areas. Among the most popular methods is the use of the so-called "bottle" method, which was also used by Osama bin Laden, thus avoiding leaving a digital trace for years. This method is the most common and successful defense to detect future terrorist attacks by communicating through encrypted messages, which means using metaphors in the exchange of SMS messages. One such example is the disclosure of the communication between the two attackers in the Twin Towers in the USA in 2001, who in their communication called the Pentagon "art" and the White House "politics" (Prodan, 2015, p. 115). Virtual communication today also develops through the popularity and accessibility of communication platforms such as "WhatsApp", "Viber" and "Skype" (Babic, 2015, p. 17).

Communication between terrorists also reveals many sophisticated techniques. They communicate through various communication channels, the most important of which is certainly the Internet. Let's assume that there are currently over 4000 countries in the world where plans for future attacks are being devised for "virtual" terrorist warfare. In advance, members of these groups enter their data into forms that can be graphic or audio files without changing either the duration or the structure of the data. But the key to such communication is that only members of the group have access to this data. They have the "key" or certain programs with which they will have access to this information. This is precisely why the problem of detecting terrorist plans by national intelligence services arises (Prodan, 2015, pp. 116-117). In these ways, terrorists use digital technology not only to plan attacks, but also to inform governments, threaten and take responsibility for their actions (Tomić, Musa, & Primorac, 2022). The Internet is very popular nowadays because it is extremely cheap. Even a small, newly established terrorist organization can have a large cyber presence and thus become competitive with much larger organizations. Furthermore, with the help of the Internet, it is possible for members of terrorist groups to receive instructions and information on how to assemble a suicide chain, its effect and purpose. Users achieve anonymity in various ways, mostly free of charge, such as registering with anonymous accounts from "Yahoo", "Hotmail" etc. (Prodan, 2015, p. 117). of the negative sides of communication via the Internet, for terrorists, is that intelligence and security forces can appear as part of a group and create suspicion among terrorists. In these cases, confusion is created among terrorists and they no longer know who to trust and who not. For these reasons, terrorists need to be constantly on the lookout, they are also monitored in hard-to-reach forums and in their private conversations. This means that the number of states that have difficulty creating security systems to track terrorists is increasing. Terrorists also use social networks for their needs, for example "Twitter" (Prodan, 2015, pp. 117-118). The most interesting way of communication between modern terrorists is when one person sends a message to another but never presses the "send" button. That is, those data are available to another person (the third person) and available to the first person (the sender, the source), and the second person (the recipient) can see these messages even if the sender of the messages does not press the button to send them. These data are received by the group members from a very specific and modern communication account (Prodan, 2015, pp. 118-119). Also, terrorists often communicate among themselves through folders marked as "drafts". Certain members have user data that allows them to access (access) these folders and leave messages in them, thus creating a communication between each other. In this way, they exchange information, transmit instructions and plan future terrorist attacks (Prodan, 2015, pp. 118-119).

5. CONCLUSIONS

Terrorist attacks became more frequent during the 20th century, but terrorism on a global scale is increasingly emphasized in the 21st century. Almost all media outlets report on terrorist attacks, and most Internet portals contain sections called "terrorism" (Maric, 2012, p. 91). Among the most famous examples is the media coverage of the terrorist attack on the Twin Towers in the USA on September 11, 2001. The media showed images of the collapse of the so-called "twin towers" all over the world, and many media outlets followed the sequence of this event live (Tomljanovic, 2016, p. 21).

Modern terrorism is strongly linked to the progress of technology, especially information and communication technology, for which reason virtual media (Internet media) that are today increasingly widespread and accessible play an important social role. Another key factor in this whole story is the fact that this factor also increases the arms production industry. Terrorism of the modern era, as we know it, begins at the height of the Cold War and the development of national movements. During this period, many terrorist organizations and groups were created that undertake terrorist acts as their main political action, more precisely through terrorist acts, the realization of their political interests and goals was achieved (Maric, 2012, p. 93).

The first priority of terrorists is to cause as much damage as possible to a certain group of people inside or outside the countries where they operate. Recently, terrorist organizations have used a non-standard method of warfare. They use information as a weapon of war because information in today's world is valuable and brings much more

consequences than standard methods of warfare (Maric, 2012, p. 93). The use of modern technologies has enabled terrorists to exchange information better and faster, to carry out secret communication or even to obtain financing. Financial support is a key element that ensures the survival and functioning of terrorist organizations (Maric, 2012, p. 93). Terrorist groups are also financed with the help of the Internet through voluntary donations and funds that the authorities barely manage to control. An example is Hizb-ut-Tahrir, an international pan-Islamist organization, which uses PayPal to transfer donations (Babic, 2015, p. 17). Terrorist groups today have larger financing systems and are much more complicated to track. The reason for this is that a significant amount of terrorist sponsorship is done under the guise of humanitarian aid (reported as humanitarian organizations) (Maric, 2012, p. 94). Terrorism in its essence has not changed throughout history, but contemporary terrorism is significantly more subtle and sophisticated than it was before because they have advanced war techniques by modernizing them. Terrorist organizations and attacks are not random acts. By examining them carefully, we notice that they have several goals through attacks designed to instill fear in people (Maric, 2012, pp. 93-94). Regarding suicides during terrorist attacks, from the eighties of the last century to 2003 only 3% of attacks were suicides, however, after the attack on the USA on September 11, 2001, this percentage increases to 80%. Today we can see news about terrorism and terrorist attacks every day in the media, however suicide attacks are not a form of attack in this era. Today, the suicide method is more present among jihadists (Maric, 2012, p. 95). Maric defines suicide terrorism as "the willingness of an individual to sacrifice his life to destroy or attempt to destroy a goal, in order to achieve another political goal (Maric, 2012, pp. 95-96). The philosopher Jean Baudrillard interprets contemporary terrorism as "terror against terror" and he compares it to a virus, emphasizing that it is everywhere around us and has become part of the culture that is fighting against it. He also calls contemporary terrorism the "fourth world war" and concludes that terrorism does not allow any world order to dominate, but this philosopher even opposes globalization, which, according to him, is as immoral as terrorism itself. Baudrillard sees a key moment in the manifestation of contemporary terrorism in the game of terrorists "with themselves offensively" to serve intuition against an almost perfect system. Terrorism has become a weapon used against the entire state system, even at the cost of the terrorists' lives (Baudrillard, 2023, p. 280). Authors Gayraud and Senat emphasize the excellent adaptability of terrorist organizations to today's modern world, taking into account the unlimited access to the Internet, which allows terrorists to communicate freely.

REFERENCES

Antoliš, K. (2010). Internetska forenzika i cyber terorizam. *19*(1), 121-128.

Babic, V. (2015). New forms of terrorist activity (Cyberterrorism). *International Scientific and Professional Conference 'Police College Research Days In Zagreb*, 23-24.

Baudrillard, J. (2023). *The Spirit of Terrorism And Requiem for the Twin Towers.* London & New York: Verso.

Bilandzic, M. (2010). Terrorism in theory and the perspective of terrorism. *Social Studies Zagreb, 20*(3), 837-859.

Briere, D. (2023). *Wireless network hacks and mods.* Hungry Minds Inc.

Croatian Encyclopedia. (2022, 1 8). *Kibernetika*. Retrieved from https://www.enciklopedija.hr/clanak/cyber

Gayraud, J.-F., & Sénat, D. (2006). *Le terrorisme.* Paris, Francë: https://www.cairn.info/editeur.php?ID_EDITEUR=PUF.

Hsinchun, C., Thoms, C., & Tianjun, F. (2008). *Cyber extremism in Web 2.0: An exploratory study of international Jihadist groups.* Arizona: Arizona Univ. .

Janczewski, L., & Colarik, A. (2021). *Cyber warfare and cyber terrorism.* IGI Global.

Jazecski, L., & Colarik, A. (2020). *Cyber warfare and cyber terrorism.*

Maric, S. (2012). *Terrorizmi si problem global.*

Nelson, B., Choi, R., Iacobucci, M., Mitchell, M., & Gagnon, G. (1999). *Cyberterror Prospects and Implications.*

Perešin, A. (2022). Mass Media and Terrorism. *Medijska istraživanja : znanstveno-stručni časopis za novinarstvo i medije, 13*(1).

Perkov, I. (2013). Evropianizimi i diskursit kroat të sigurisë.

Precht, T. (2007). *Homegrown Terrorism and Islamist Radicalisation in Europe: From Conversion to Terrorism. An Assessment of the Factors Influencing Violent Islamist Extremism and Suggestions for Counter Radicalisation Measures.* Copenhagen: Danish Ministry of Justice.

Prodan, T. (2015). Internet, terrorism, counterterrorism. *National security and the future, 16*(1), 93-143.

Sovilj, D., & Sovilj, P. (2017). Drone terrorism, a new way of war?! *Policia dhe Siguria, 26*(3), 255-266.

Tomasevski, K. (1980). Causes of terrorism. *Journal of Sociology, 10*(3-4), 161-172.

Tomić, Z., Musa, I., & Primorac, M. (2022). Terrorist organizations as actors of political communication. *Medianali, 6*(11).

Tomljanovic, M. (2016). *Two phenomena of contemporary terrorism: the involvement of women in terrorist acts*

and media monitoring of terrorist activity.

Tonkovic, A. (2014). Terorizmi bashkëkohor – kërcënim global i sigurisë dhe/ose një formë veprimi anti-globalizues. *Mostariensia, 18*(1-2), 277-292.

Vukoviq, H. (2012). *Two phenomena of contemporary terrorism: the involvement of women in terrorist acts and media monitoring of terrorist activity.*