TRIANGLE OF CYBER, TERRORISM AND RADICALIZATION

Sevde KAPU*

ORCID ID: https://orcid.org/0000-0001-7049-7938

Abstract

Cyberspace, called the new field of terrorism, is a transition zone from traditional terrorism to cyber-terrorism. The concept of cyber terrorism created by the combination of the words cyber and terrorism that generates a great risk environment in a world that is increasingly dependent on technology. Terrorist groups that take advantage of the opportunities for unlimited, anonymous and low-cost cyberspace are easily adapted to cyberspace and try to achieve their goals of radicalization through methods such as propaganda and recruitment. In a digitized world, it is possible that terrorist organizations will gain strength and endanger the national security of states by carrying out major cyber attacks.

Key Words: Cyberspace, Cyber Radicalization, Terrorism, ISIS,

Introduction

Cyberspace which is increasingly permeating people's everyday lives with the rise of globalization, is an area of unknown depth and enormity. With the development of information and communication technologies, most of people's lives have become dependent on computers. In this context, cyberspace, which removes borders and distances, has revealed a new dimension of terrorism. The concept of cyber terrorism in this new dimension threatens many targets such as individuals, governments and national critical infrastructure.

The possibilities created by cyberspace for terrorists to achieve their goals are being observed today and pushing the public into a state of fear. The anarchic structure of cyberspace, that is, the lack of a control mechanism, today causes terrorist organizations such as Al-Qaeda and ISIS to use the nature of cyberspace to carry out attacks in order to spread fear in society.

The aim of this study is to explain the concept of cyber terrorism, whose consequences are predicted to be more damaging than traditional terrorism in an increasingly digitized world. In this context, the research questions of the study are as follows. What is the relationship between cyberspace and terrorism? How do terrorists instrumentalize cyberspace in their

radicalization processes? What is the difference between cyber terrorism and traditional terrorism?

In the first part of the study, some concepts related to terrorism, cyberspace, cyber terrorism and cyber will be explained and the confusion of concepts will be tried to be eliminated. It is necessary that these concepts, on which there is no international consensus, that's why it need to be consider from a reasonable, realistic and concrete point of view. In the second part of the study, the difference between the concept of cyber terrorism and other types of terrorism will be revealed and the characteristics of cyber terrorism and the dimension of propaganda will be focused. This study also will examine the cyber capacity that ISIS has established by instrumentalizing cyberspace in its terrorist activities, along with the concepts of cyber radicalization, cyber caliphate and cyber jihadism.

Theoretical Framework

Terrorism, whose historical history dates back to old times, continues to exist from the past to the present with political, religious, social and economic motivations. There is no comprehensive definition agreed upon from the definitions of terrorism made to date. However, these definitions have some in common. A highly controversial concept, terrorism has over a hundred definitions in the literature (Smith, 2020: 223). According to Walter, the concept of terrorism which is derived from the Latin word 'terrorem' in the sense of 'the source of great fear and panic', was later passed into English as 'terror' (Skeat, 2005: 548).

According to the United States, terrorism is defined as pre-planned politically motivated violence against civilians by sub-national groups and secret agents. For the European Union (EU), terrorism is defined as activities aimed at seriously scaring the public, suppressing the government or any organization and destabilizing the constitutional economic and social structure of the country. According to the Arab League, terrorism is defined as acts of violence committed with any intention and purpose, individually or collectively, to damage the environment, public and private property and the government in order to create fear and panic in the people (Smith, 2020: 223). According to the Turkish Penal Code No. 3713, terrorism, algebra, violence, repression, intimidation and similar methods as any action by an individual or part of individuals basic the qualities and characteristics specified in the

Constitution of the Republic of Turkey, against the Republic of Turkey endanger and criminal organisation is defined (Terörle Mücadele Kanunu, 1991).

In this context, the common point of these definitions is violence, creating a state of fear and panic in the target. Finally, to give Conway's definition, the main characteristics of terrorism are the act of using violence against civilians by groups or individuals to influence public perception for political or other purposes (Conway, 2002: 436). In this aspect, with the increase of globalization, the concept of terrorism, which can be applied to cyberspace, which permeates daily lives, has gained a new dimension. The fact that politically or religiously motivated people commit terrorist acts by instrumentalizing information technologies leads to a relationship between digitalization and terrorism (Sundaram&Jaishankar, 2008: 595). In order to understand this relationship, it is necessary to understand cyberspace as a concept.

Cyberspace, in an increasingly digitized world, affects people's lives in multidimensional terms and creates a great risk environment alongside the benefits it brings to humanity (Akyeşilmen, 2018: 53). Human-made cyber space and social relationships that may be more subject to recent and rapid technological developments, social and technological relations, such as cyber attack, cyber crime, cyber terrorism and cyber ethics, including topics such as dynamic and ever-expanding field. (Nye, 2010: 4). Cyberspace, which has no internationally accepted definition, is an information ecosystem created by stored and shared information in its most general sense. Cyberspace is defined as a virtual world based on electronic data, including user, information, software (logical infrastructure), hardware (physical infrastructure) components for an inclusive and realistic definition, not based on geographic boundaries (Akyeşilmen, 2018: 58).

As mentioned above, with the increase of information technologies, cyberspace, which attracts attention, provides new opportunities for terrorist organizations to achieve their goals. Cyber terrorism, a controversial concept, was first described by Collin as a combination of the physical and virtual world (Collin, 1997: 15-18). Although there is no agreed definition of cyber terrorism, Dorothy Denning is the one who has given the literature the broadest and most detailed definition of cyber terrorism:

> *Cyberterrorism refers to 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. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not* (Denning, 1999: 239).

According to Weiman, cyber terrorism is the use of computer network tools to damage critical national infrastructures such as energy, transportation and government operations. With nations' critical infrastructures increasingly computerised, new vulnerabilities and weaknesses in information systems are making cyberspace attractive to terrorists (Weimann, 2005: 130). Another issue as important as definitions of cyber terrorism are cyber-related definitions that are mixed with cyber terrorism. To address this confusion of meaning, it is useful to provide definitions of the concepts of hacktivism, cybercrime and cyber attack.

In this context, Hacktivism is people who are politically or socially motivated and use information technologies and perform actions for the purpose of ideology or belief. Because they are separated with good intentions and malicious intent, they carry out attacks directly on decision-makers, not intended to create a sense of fear in innocent people like cyber terrorism (Çokbildik, 2019: 56). Weiman describes the relationship between cyber terrorism and hacktivism in the words *'hacking marriage with political activism'*. Although the relationship between them is blur, two ways can be explained; terrorist groups recruit hacktivists, or hacktivists decide that states will carry out a critical infrastturcture attack (Weimann, 2005: 130).

Cybercrime covers illegal attacks on the privacy, integrity and accessibility of computers ' data systems by the EU Council, and refers to crimes such as spam, fraud and data theft. The difference between cyber crime and cyber terrorism is its motivation. Cybercrime is done in the form of conscious harm with criminal motivation, while cyber terrorism aims to create a sense of insecurity by containing the element of terror (Giantas&Stergiou, 2018: 4).

A cyber attack is an attack that is considered a cybercrime in the language of law aimed at destroying or damaging information systems. Actors in cyberspace can carry out cyber attacks for their own purposes. In cyber terrorist attacks, the most common types of cyber attacks are: Dos (Denial of Services) and DDos (Distributed Denial of Services) attacks aimed at damaging system service requests, Man in the Middle (MitM) attacks aimed at stopping data

scanning, stealing and filtering, Phishing attacks by email to steal credentials, and malware attacks can be listed as such (Akyeşilmen, 2018: 74-80).

Finally, to mention radicalization as a concept, it is defined by Amoss as a word as revolutionary change on political or social issues (Oz, 2001: 98). Religiously motivated radicalism, on the other hand, has been associated with the Islamic world, especially after the September 9/11 attacks (Laqueur, 1999: 10). But religious radicalization is actually caused by groups that make religion a tool of exploitation and propaganda, and with the expansion of cyberspace's sphere of influence, it is gaining momentum and spreading from regional to global scale.

In this sense, cyber terrorism falls into a type that we can categorize as a new type of terrorism with the same goals as traditional terrorism with the care of its goals, but with the care of its tools and opportunities. It causes social and political and economic distraction with misinformation, spreading fear, and realizing the goals of terrorists. (Giantas&Stergiou, 2018: 5).

Understanding of Cyber Terrorism

There are many reasons why cyber terrorism has become popular among terrorists. According to Weimann, terrorists use information technologies or engage in information technologies for the purpose of finding weapons or targets. In this context, terrorists assist in their activities such as propaganda, recruitment, fund-raising, communicaiton, psychological campaign, coordinate their action, raise fund, virtual training. they use technology for purposes such as radicalization and spread of terror (Weimann, 2005: 133).

In this point, when cyber terrorism and traditional terrorism are compared, the first factor is that cyber attacks for terrorist purposes are less costly in terms of cost. Cyber terrorists could be anyone with access to the internet and modem. The person who will commit cyber terrorism may be the only one, a member or proxy of a group. Without the need for any conventional tools such as weapons, it can perform cyber terrorism with a single button at the desk using virus creation and Denial of Sevice (DoS) methods from cyber attack methods which means that unauthorized person access to information (Sundaram&Jaishankar, 2008: 597).

The second is that attacks aimed at terrorism are carried out with a more anonymous identity than in the real world. At this point, terrorists who can easily hide their identity in the virtual world can share content on websites under the name nickname and guest user and conduct propaganda activities by managing social media accounts (Weimann, 2005: 137).

The third is, the number of targets that can be attacked for the purpose of cyber terrorism is quite large. Cyber terrorists can attack computers, government computer networks, public property and critical infrastructure.

The fourth is, thanks to the remote feature of cyberspace, terrorist groups have no problem hiring and training members. Because there is no risk of death, it is easier to convince individuals equipped with cyber attack and hacking into terrorism (Gürkaynak&İren, 2011: 267). In addition to providing human resources to terrorist groups, cyberspace is another important dimension that the internet is the financing area of terrorist groups. In this context, they use methods such as fund-raising, money laundering and money transfer to provide funds to cyber attacks (Findlay, 2014: 18).

When cyberterrorism activities are viewed from a psychological dimension, an unknown threat is perceived as much more dangerous than a known threat and creates fear in society. Cyber terrorism makes fear of unknown feel more because of its anonymous structure and multitarget structure. For example, after the September 9/11 attacks, in 2003, the Washington Post reported that cyber attacks were carried out by al-Qaeda, increasing the state of fear in society (Weimann, 2005: 131).

As terrorism becomes more involved with cyberspace, cyber attacks that endanger national security are expected to be carried out against national critical infrastructure. For example, attacks against water storage, water supply system, electrical power system, transport, interrupts financial transactions greatly affect national security (Sundaram&Jaishankar, 2008: 603).

The propaganda dimension of cyber-terrorism is deliberate and systemic attempts to shape and manipulate perceptions. Along with cyber developments, the Internet has been a means of inter-terrorist communication and propaganda. The purpose of propaganda is to show terrorist activities/crimes through videos and posts, to find recruitment of people, and finance.

Propaganda is also carried out in order to carry regional visibility terrorism to a global scale and to gain international recognition and to terrorize the masses (Minei&Matusitz, 2011: 1002). At this point, the most important goal of terrorist organizations ' propaganda in cyberspace is to achieve their political goals by managing the perceptions of the masses (Darıcılı, 2020: 102).

Finally, the relationship between cyber terrorism and radicalism is an issue that cannot be ignored today. Modern technologies, especially social media, play an important role in the process of radicalization of religious groups. As terrorists use online platforms, a genre called lone-wolf attack, known as the extermist movement, has emerged alone. Terrorist groups encourage people to commit lone-wolf attacks when there is no spatial proximity to realize their own goals (EFSAS, 2018).

Case of Cyber-Radicalization: Islamic State (IS)

At the beginning of 21st century, ISIS which is the radically influential organizations became more active in cyberspace than other teorist groups. So-called Islamic State (IS) conducts its propaganda activities through social media and has introduced concepts such as cyber caliphate, cyber radicalization and cyber jihadism (Çokbildik, 2019: 73). According to Weimann, ISIS is an organization that has recognized the potential for cyber terrorism.

ISIS was founded in 1999 by Abu Musab al-Zarqawi, the organization was renamed Al-Qaeda in Iraq in 2004, then renamed Islamic State of Iraq and ash-Sham (ISIS) in 2013 and then again renamed Islamic State in 2014 (Bozkurt, 2016: 82).

ISIS which is considered a hybrid in terms of using both physical and virtual methods in its attacks, is not intended to kill as a virtual method, but to create fear and distrust. In this context, recruiting hackers to the computer is seen as an active cyber threat. IS is trying to use cyberspace as a tool to gain new members and radicalize those members (Lillington, 2016). In 2015, when the French satirical newspaper Charlie Hebdo magazine office was attacked by IS, at the same time 19,000 French websites were attacked, creating an state of fear for people with the slogan '*Death to Charlie'* in the French websites (Griffin, 2015). Looking at the cyber structure of ISIS, Cyber Caliphate and Cyber Caliphate Army (CCA) are the first cyber terrorist group to support IS, but they are causing fear in the public with their cyber attacks. The group's founder is a 15-year-old British hacker named Junaid Hussain. The

most significant attack by this group was a cyber attack by the ISIS group against US Central Command (CENTCOM) on youtube and twitter. CENTCOM accounts filled with ISIS slogans this attac such as *American soldiers we are coming to watch your back, Cyber Caliphate, I love You ISIS*. (BBC, 2015). In 2015, the group's effectiveness decreased when Junaid Hussain was killed by an airstrike in Syria (Giantas&Stergiou, 2018: 10).

The Sons of Caliphate Army was founded in 2016 as a subgroup of the Cyber Caliphate and has the potential to carry out more than 15,000 cyber attacks , with more active social media accounts to demonstrate ISIS ' cyber capability. The hacking group, founded in 2016 called Kaslashnikov E-security Team, provides technical support to ISIS's cyberspace activists (Alkhouri, et al., 2016: 3-18). It supports ISIS ' cyber jihadism activities by sharing posts on social media and reporting its successful attacks. (Nance&Sampson, 2017: 69).

United Cyber Caliphate (UCC) is ISIS's most coordinated act in terms of cyber attacks created in 2016 by merging other hacking groups. (Cyber-Caliphate Army, the Kalashkinov E-Security Team and the Sons of Caliphate Army). UCC is very well known for its death lists that it has published in countries such as the United States, Canada, Australia (Alkhouri, et al., 2016: 3-18).

In addition to these organizations, there are hacker groups such as Islamic State Hacking Division (ISHD), Islamic Cyber Army (ICA), Rabitat Al-Ansar, Cyber Team Rox (CTR) that support ISIS propaganda. Although ISIS is a terrorist group that is very active in cyberspace, there are no attacks to be reported as cyber terrorism so far. (Kohlmann, 2006: 121).

The effective use of cyberspace by ISIS and its supporters, spreading their radical and extremist ideology through propaganda, poses an element of risk in a world that is increasingly dependent on cyberspace. Terrorist groups ,which increase visibility in the global context as a potential threat along with the possibilities of cyberspace, are projected to lead to increased examples of international cooperation on cyber security in the future.

Conclusion

Today, technology has a big impact on security paradigms, as well as the amenities it brings, as it exists on all sides of people's lives. As this study shows in this regard, it is inferred that

cyberspace and the phenomenon of terrorism are inevitably connected to each other and will continue to be connected. Terrorism, defined as creating fear in the public for political and social purposes, can move its regional activities to a global scale without causing any deaths, especially by using cyberspace to be an anonymous, multi-targeted, cheap, propaganda tool, recruitment area.

It is observed that a large and destructive attack has not occurred until now from cyber attacks aimed at terrorism. But this does not imply that they will not occur in the future. Cyber terrorists have the potential to attack critical infrastructures of countries, especially airlines, water supplies, energy and electricity suppliers with service providers to achieve their political goals.

Moving a new generation of terrorist activities into cyberspace seems to be a reasonable and logical process for terrorists. In this way, terrorist groups, which have gained greater visibility internationally, are trying to penetrate people's perceptions by instrumentalizing cyberspace in their radicalization processes and jihadism rhetoric. Looking at the example of ISIS, one of the organizations that aims to grow in this way, it seems that it systematically creates cyber infrastructure. ISIS, which has carried out a number of attacks in order to demonstrate its cyber capability, is seen as a very effective terrorist organization in cyberspace.

As a result, cyberspace, which surrounds human life in all its dimensions in terms of social, economic, political and terrorism, requires effective cyber governance at the national and international levels, along with the risks it brings. In this context, countries must conduct their cyber security work on a solid basis against any possible cyber terrorist attack and cooperate in the concession of cyber terrorism, which has devastating consequences for each state.

References

Akyeşilmen, N. (2018). *Disiplinlerarası Bir Yaklaşımla Siber Politika ve Güvenlik.* Ankara: Orion Kitabevi.

Alkhouri, L., Kassirer, A., & Nixon, A. (2016). Hacking for ISIS: The emergent cyber threat landscape. *Flashpoint*, 3-18.

BBC. (2015). *US Centcom Twitter account hacked by pro-IS group.* Retrieved January 23, 2021 from: https://www.bbc.com/news/world-us-canada-30785232.

Bozkurt, A. (2016). Cephet-ul Nusra ve Daeş Çatışması:Radikal bir Karşılaşma. In N. Akyeşilmen & Ö. Afşar (Eds.), *Suriye'de Barışın İmkanları* (pp. 81-104). Ankara:Orion Kitabevi.

Collin, B.C. (1997) The future of cyberterrorism: Where the physical and virtual worlds converge. *Crime and Justice International,* 13(2), 15-18.

Conway, M. (2002). What is cyberterrorism?. *Current History,* 101(659), 436.

Crenshaw, M. (2011). The debate over 'old'vs.'new'terrorism. *Jihadi Terrorism and the Radicalisation Challenge. European and American Experiences,* 57-68.

EFSAS. (2018). Cyber-radicalization:Combating terrorism in the digital era, 1-7. Retrieved January 15, 2021 from https://www.efsas.org/publications/study-papers/cyber-radicalization-combating-terrorism-in-the-digital-era/.

Çokbildik, A. C. (2019). *Siber Terörizm: Radikal/Dini Örgütler*. Unpublished Master's Thesis, Konya: Selçuk Üniversitesi Sosyal Bilimler Enstitüsü.

Darıcılı, A. B. (2020). Küresel Terörün Teknolojik Yönü: Siber Terörizm,. In Hasan A. (Edt). *Küresel Terör ve Güvenlik Politikalar* (pp. 93-106). Nobel Yayınevi.

Denning, D. (1999). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. *Networks and netwars: The future of terror, crime, and militancy*, 239-288.

Findlay, V. (2014). *Cyber-Threats, Terrorism and the Counter-Terror Model.* University of St. Andrew's, The Handa Centre for the Study of Terrorism and Political Violence,

Giantas, D., & Stergiou, D. (2018). *From terrorism to cyber-terrorism: The case of ISIS.* Available at SSRN 3135927.

Griffin, A. (2015). Charlie Hebdo: France hit by 19,000 cyberattacks since Paris shootings in unprecented hacking onsalught. *Independent*, Retrieved January 23, 2021 from: https://www.independent.co.uk/life-style/gadgets-and-tech/news/charlie-hebdo-france-hit-19-000-cyberattacks-paris-shootings-unprecedented-hacking-onslaught-9980634.html.

Gürkaynak, M., & İren, A. A. (2011). Reel dünyada sanal açmaz: Siber alanda uluslararasi ilişkiler. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,* 16(2), 263-279.

Iqbal, Z. (2020). Terrorism in Cyberspace: A Case Study of Terrorist Organizations Operating in Pakistan. *Cyberpolitik Journal,* 5(10), 240-259.

Kohlmann, E. F. (2006). The real online terrorist threat. *Foreign Affairs,* 115-124.

Laqueur, W. (1999). *The new terrorism: Fanaticism and the arms of mass destruction.* Oxford University Press on Demand.

Lillington, K. (2016). How real is the threat of Cyberterrorism?. *The Irish Times,* Retrieved January 27, 2021 from: https://www.irishtimes.com/business/technology/how-real-is-the-threat-of-cyberterrorism-1.2608935.

Madhava, S. S. P., & Jaishankar, K. (2008). Cyber Terrorism: Problems, Perspectives and Prescription. In *Schmallager* F., & Pittaro, M., (Eds.), *Crimes of the Internet,* 593-611.

Minei, E., & Matusitz, J. (2011). Cyberterrorist messages and their effects on targets: A qualitative analysis. *Journal of human behavior in the social environment,* 21(8), 995-1019.

Nance, M., & Sampson, C. (2017). *Hacking ISIS: the war to kill the cyber Jihad*. Skyhorse Publishing Company, Incorporated.

Nye Jr, J. S. (2010). Cyber power. *Harvard Univ Cambridge MA Belfer Center for Science and International Affairs*, 1-31.

Oz, A. (2001). *Fanatizme Karşı Mücadele*. (çev. Mehmet Küçük). İstanbul: Yapı Kredi Yayınları.

Skeat, W. W. (2005). *A Conscise Etymological Dictionary of the English Language. New* York: Cosimo.

Smith, M. (2020). *Uluslararası Güvenlik.* (çev. Ramazan Gözen). Ankara: TED Matbaacılık.

Sundaram, P. M. S., & Jaishankar, K. (2008). Cyber Terrorism: Problems, Perspectives, and Prescription. *Crimes of the Internet; Schmallager,* 593-611.

Terörle Mücadele Kanunu, (12.4.1991). Retrieved January 20, 2021 from https://www.mevzuat.gov.tr/MevzuatMetin/1.5.3713.pdf.

Weimann, G. (2005). Cyberterrorism: The sum of all fears?. *Studies in Conflict & Terrorism*, 28(2), 129-149.

Yılmaz, B. A. (2020). Siber terörizm ve değişen istihbarat anlayışı. *Anadolu Strateji Dergisi*, *2*(1), 65-82.