Journal of Industrial Policy and Technology Management, 7(1), 2024, 33-44

The Role of Social Media in Combating Cyberterrorism

Afet Çağay[1] Bahattin Gökhan Topal[2]

[1]Ankara Science University, Türkiye

[2]OSTİM Technical University, Türkiye

[1]afet.cagay@ankarabilim.edu.tr, [2]gokhan.topal@ostimteknik.edu.tr

Received: Dec 12, 2023 Accepted: March 14, 2024 Published: June 30, 2024

Abstract: Terrorism has been among the greatest threats to humanity for centuries. With the development of technology, it has changed the tools it uses, and in recent years, it has been using the internet and social media as an important propaganda tool, a method of recruiting sympathizers and for direct attacks. In this study, the concept and history of terrorism was evaluated and information was given about the methods used by terrorist organizations. Data on Cyberterrorism, one of the methods used effectively in recent years, has been conveyed. How terrorist elements influence the area by using social media and how they are used as a propaganda tool are explained.

Keywords: Terrorism, Finance, Social Media, Terrorism and Finance

JEL Classification: G10

1. Introduction

Since the inception of the internet, it has been used for various purposes. Despite its multifaceted technological advancements for positive aims, unfortunately, it has also been employed for malicious purposes. In recent years, the pervasive influence of the concept of social media in our lives has sparked ongoing debates about its negative effects. The public nature of these platforms and the widespread individual use have drawn the attention of terrorist elements. The continuous relationship between internet, social media, and Cyberterrorism is both simple and complex. Its ability to reach broad audiences makes it a tool for both propaganda and warfare.

This article explores how social media is utilized by terrorist elements, defines the concept of Cyberterrorism, and proposes some measures for counteraction. Over the past 50 years, Türkiye has grappled with various elements in the fight against terrorism, extending this struggle into the realm of Cyberterrorism. The shift in terrorist elements utilizing cyber attacks alongside conventional systems has noticeably altered public

measures, with a visible and intense impact. The paradigm of soldier / police = weapon / intelligence is transforming towards civilian / military / police = weapon / intelligence / cybersecurity.

2. Definitions

Before delving into the topic under the heading of Cyberterrorism, the concepts of social media, the definition of Cyberterrorism, the intersection of Cyberterrorism and social media, a categorical explanation of cyber crimes, and an evaluation of types of Cyberterrorism on social media are attempted.

In presenting these topics, to avoid engaging in terrorist propaganda, no visual examples or links are provided, and only the names of example magazines and channels are abbreviated. Additionally, some graphics and descriptions involving public measures are included.

2.1. Social Media

Social media refers to various online platforms and mobile applications where users can create, edit, and share content without the need for technical knowledge or skills, using Web 2.0 technologies. The defining feature that makes social media "social" is its ability to facilitate interaction between users through the content and activities on the applications. Since this relationship is often visible to other users, the social aspect becomes even more pronounced (Gretzel, 2015).

The foundation of social media content lies in written texts, but with today's Web 2.0 technologies, these have been replaced by audio, visual content, and animated short video designs. With the widespread use of the internet and evolving applications, it has become a globally utilized network. Over 4.7 billion people, equivalent to approximately 60% of the world's population, use social media, ranging from Facebook and Instagram to Twitter (formerly X platform) and YouTube. According to the Digital 2023: Global Overview Report from 2023, 94.6% of website or app visitors spend time on social networks, while the educational purpose accounts for 23.8% (Kemp, 2023).

There are various definitions related to the concept of social media, and in this section, some key information is summarized. Boyd and Ellison define social network sites (a subset of social media) as "web-based services that allow individuals to (1) construct a public or semi-public profile, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others

within the system." This definition focuses on profile creation and network building (Boyd & B. Ellison, 2008).

Kaplan and Haenlein offer an important definition in this field. In their article "Users of the World, Unite! The Challenges and Opportunities of Social Media," they provide a widely accepted definition, describing social media as "a group of internet-based applications built on the ideological and technological foundations of Web 2.0, allowing the creation and exchange of user-generated content." Their definition emphasizes user-generated content and the participatory nature of social media (M. Kaplan & Haenlein, 2010).

As the use of these platforms evolves over the years, definitions have changed to reflect the diversification, usage methods, and purposes of social media. After exploring various definitions, one of the most useful seems to be the one presented by Burgess and others in the introduction to "The Sage Handbook of Social Media," titled the "social media paradigm." Recognizing a distinctive moment shaped by the dominance of social media technologies in media and communication history. Burgess and others define social media and social media technologies more specifically as "digital platforms, services, and applications that converge around content sharing, public communication, and interpersonal connection" (Burgess, Marwick, & Poell, 2018).

Considering Burgess and others' definition, we can say that social media encompasses some unique and innovative features. Social media is connected through a network structure and is accessible through internal and/or mobile networks. Users actively participate in the management process by creating content. It exists within the framework of a social network within the current platform, influencing connections between individuals and organizations through interactions such as comments, likes, and messaging. Social media is a form of polymedia and consists of complex products or product systems, and despite various forms, it has a public structure, being visibly interactive. The user and viewer base continues to grow, influenced by innovative technologies.

2.2. Definition of Cyberterrorism and Use of Social Media

As can be understood from the definitions expressed about social media, it is a structure with high interaction power, the ability to appeal to a wide audience, and the instant use of visual and auditory tools. Within this structure, individual users produce content for personal promotion or individual commercial activities, while corporate entities effectively use social media platforms for visibility and commercial purposes. The

inevitable use of such a powerful means of communication by terrorist elements is apparent. This usage is not only for direct propaganda purposes but is also known to be effectively utilized in cyber attacks, messages intended to be loaded into the subconscious, and perception management. Undoubtedly, the methods of cyber attacks conducted through social media are constantly changing, and the measures taken against them are updated in the same proportions. This section discusses efforts related to the definition of Cyberterrorism, types of cyber crimes, categories of Cyberterrorism through social media, and methods to combat Cyberterrorism on social media.

2.2.1. Cyberterrorism

According to a comprehensive study conducted by the organization Compareitech, it has been stated that over 71 million people experience victimization in cybercrime every year. The same study indicates that the number of cyber attacks is increasing from year to year.

The term "Cyberterrorism" was first introduced by Berry Colin, a senior researcher at the Security and Intelligence Institute in California, in the 1980s (Colin, 1997). Pollitt (1998: 9) defined Cyberterrorism as "politically motivated attacks designed by sub-state groups or clandestine organizations on information systems, computer systems, computer programs, and data stores that result in violence against non-combatants" (Çıtak, 2021). Another definition describes a Cyberterrorism act as a digital attack carried out to threaten or coerce individuals, businesses, or governments with the aim of disseminating the attacker's social or political goals (Smith, et al., 2023).

Among the definitions that lack a consensus on scope and definition, Cyberterrorism has become one of the most scrutinized topics in recent years. Considering the principles of causing harm and the concept of where terrorism takes place, we can see that Cyberterrorism has a broad field of influence. The key factor here is that the execution takes place in the cyber world rather than the physical world. The general definition of "Cyberterrorism" seems to focus on two types. The first type involves actions carried out in the virtual environment, affecting many people within a virtual domain. The second type is where the action takes place in the virtual environment, but the consequences result in physical damage. In the first form, harmful actions are directed towards many people within a virtual domain. The second form aims to affect a large population through actions that disrupt industrial facilities' production and control processes, such as water management systems, power grids, telecommunication tools, public transportation systems, and city information and management systems (Gercke & Brunst, 2009).

The second type involves high-intensity activities with a high level of damage. This process falls under the archetype of a "hacker." Initially, it eradicates data belonging to real users; subsequently, it sabotages data protected by a (large-scale) commercial organization or (even larger-scale) government institution. After this stage, it manages an attack on SCADA or critical infrastructure using high technology and data usage. At this final stage, all activities that truly constitute terrorism (structure, principle of harm, elements) are carried out. Here, the issue has evolved from a simple hacking incident to a Cyberterrorism act. If we interpret what hacking exactly means, it can be deduced from this definition that it constitutes Cyberterrorism (Madarie, 2017). When the action is carried out within the cyber realm and encompasses the activities characterizing terrorism, such as necessary structural conditions, the principle of causing harm, and the presence of elements, the concept of Cyberterrorism comes into play. If these requirements have not been technically and practically fulfilled, it may be just a hacking or hacktivism situation.

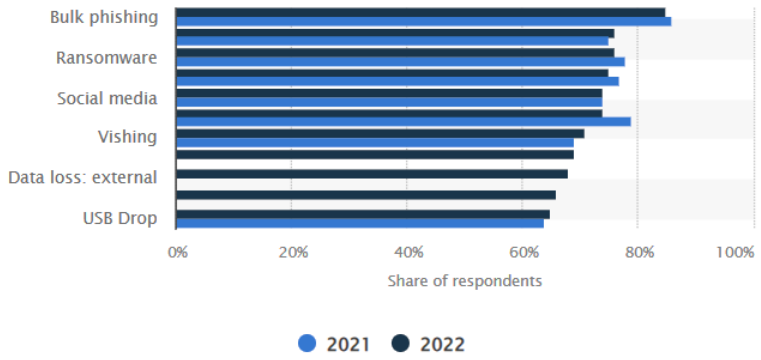

Diagram 1. Percentage of Organizations Worldwide that Experienced Cyber Attacks from 2021 to 2022, by Attack Type

Source: (Statista, 2023)

When looking at the percentage of organizations globally exposed to cyber attacks from 2021 to 2022 based on the type of attack, it is observed that an increase has started between 2021 and 2022, with social media accounting for around 70% of this increase.

According to the United Nations Sustainable Development Goals, by 2030, it is expected that 90% of the world's population, or 7.5 billion people, will be online. This will naturally bring along a security risk, with a particular focus on the intensity of terrorist attacks on cyber platforms (United Nations, 2015).

The Global Cybersecurity Index (GCI) study, conducted by the International Telecommunication Union (ITU) with the participation of 193 member countries and the

State of Palestine, sought answers to 82 questions related to 20 measurement points. The focus of the research was on legal measures, technical measures, organizational measures, capacity-building measures, and collaboration measures. According to the Global Cybersecurity Index 2020 report by ITU, when looking at country profiles, various technical issues are evident. Particularly, the technical capabilities of countries with low development levels are influenced in proportion to this. Examining the graph depicting the situation of countries with sufficient legislation for data protection, it is observed that almost all of Europe has regulation in this regard, while there is a significant deficiency in Africa and Arab countries.

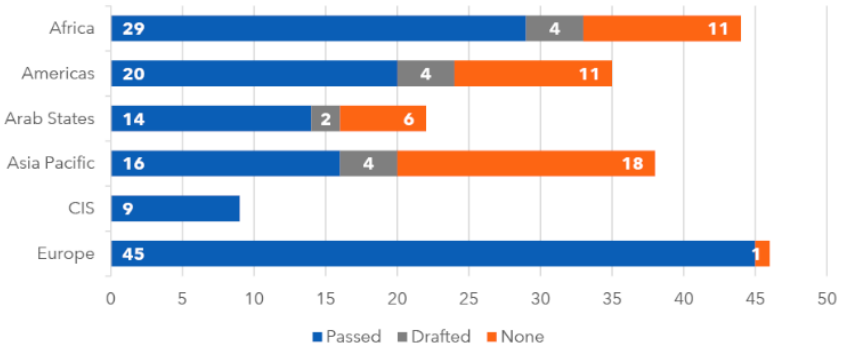

Diagram 2. Countries With Data Protection Legislation

Source: (Global Cybersecurity Index, 2020)

When looking at policies aimed at taking measures during a cyber attack or cyber breach process, it is once again evident that European countries are at the forefront, while the African continent is not in a favorable position on this matter.

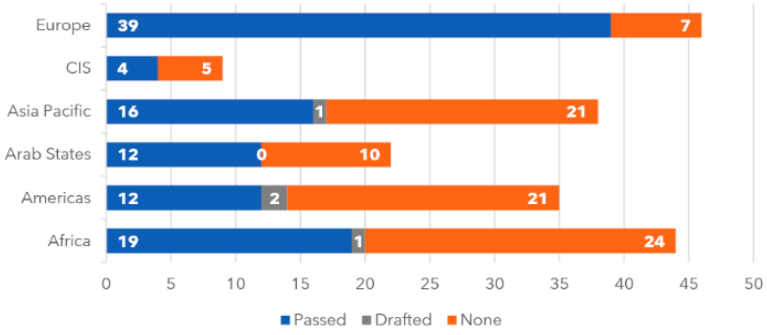

Diagram 3. Countries With Vreach Notification Measures

Source: (Global Cybersecurity Index, 2020)

When looking at the information provided in the report about Türkiye, it is in a strong position in terms of cybersecurity attacks and measures. With an Overall Score of 97.50, it is noted that Türkiye is sufficient in Legal Measures, Capacity Building, and Collaboration Measures, while there is room for improvement in the Technical and Organizational aspects. In the relevant report, Türkiye is ranked 11th with a score of 97.49 in the Global scores and ranking of countries section. Within the Europe Region GCI results, Türkiye ranks 6th among European countries with a score of 97.5.

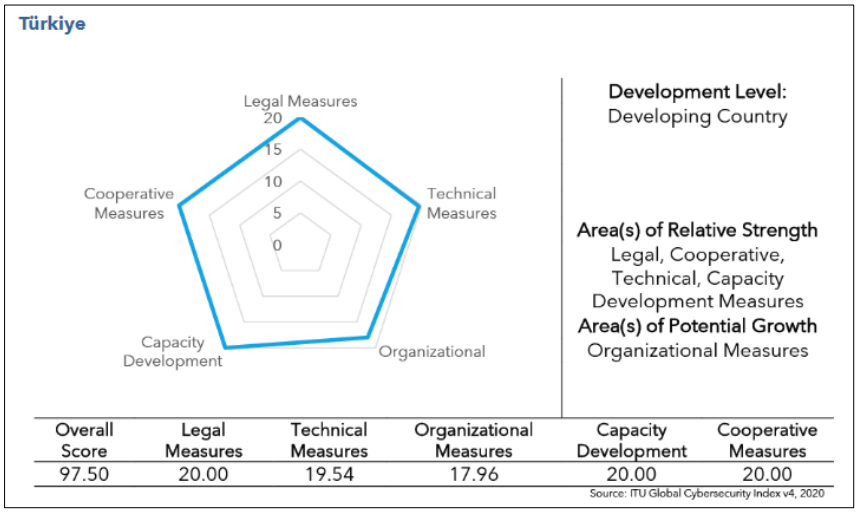

Diagram 4. Global Cybersecurity Index 2020, Country Profiles: Türkiye
Source: (Global Cybersecurity Index, 2020)

2.2.2. Types of Cybercrime

Although cyber attacks generally seem to have a digital purpose of causing harm, their results also aim to target physical attacks. Cybercrimes are usually carried out using public servers and networks. The target is often secure public systems, public networks, and other web networks with limited access. Examples of Cyberterrorism include hacking public websites, unauthorized access, attacking critical infrastructure systems, and cyber espionage. In addition, the main headings in the 2022 Internet Crime Report prepared by the United States Department of Justice Federal Bureau of Investigation are as follows: Phishing, Government Impersonation, Personal Data Breach, Advanced Fee, Non-Payment / Non-Delivery, Extortion, Overpayment, Tech Support, Lottery / Sweepstakes / Inheritance, Investment, Data Breach, Identity Theft, Crimes Against Children, Credit Card / Check Fraud, Ransomware, BEC (Business Email Compromise), Threats of Violence, Spoofing, IPR (Intellectual Property Rights)/Copyright/Counterfeit,

Confidence/Romance, SIM Swap, Employment, Malware, Harassment/Stalking, Botnet, Real Estate.

- **Attack on Public Websites**: The main objective here is to create discomfort for public authorities and society. The attacking group aims to share content expressing their views or disrupt the traffic to the websites.
- **Unauthorized Access**: Those orchestrating cyber attacks often attempt a method of attack that aims to disable communication tools controlled by security elements (police, military, intelligence, etc.) or other critical technologies.
- **Attack on Critical Public Infrastructure Systems**: Attacks are launched on elements crucial to the public, such as electricity, water, purification systems, hospitals, public transportation, and similar necessities. Steps are taken to disable or disrupt these structures, leading to a public health crisis. The attacks target endangering public safety, inducing a state of panic among the people, and even causing fatalities.
- **Cyber Espionage**: Accessing private information, especially belonging to the public, and orchestrating cyber attacks to acquire civilian, military, and intelligence information falls within the priority areas.

2.2.3 Cyberterrorism Categories Through Social Media

Social media has become an open-source tool for the growth and development of organized crime groups and cyberterrorist organizations (Andrews et al., 2018). Along with providing many positive aspects, social media has become a significant factor for cyber attacks. By its nature, social media platforms create a meta-world structure where unrelated individuals interact. It offers the opportunity for individual or corporate promotion and engagement in commercial activities. While its advantageous aspects make it an appealing medium, its structure, allowing interactions among people of varying levels of information, also makes it vulnerable to cyber attacks.

Social media platforms have turned into crucial recruitment points for terrorist groups. Particularly in recent years, the tendency to be influenced by propaganda-sharing by terrorist organizations and to join terrorist elements has increased. Following action-packed and attention-grabbing videos shared by ISIS on YouTube, more than 200 Americans are known to have joined the ranks of ISIS by going to Syria (McDowell-Smith, Spechhard, & Yayla, 2017).

Terrorist organizations operating in the United States have used social media platforms with similar purposes and methods as internationally oriented religious-based terrorist organizations. Groups identified as far-right (advocating white supremacy) use social

media, especially YouTube, to publish extensive messages and use this platform not only to attract attention but also as a tool for recruiting members. Terrorist organizations focus on specific demographic structures to recruit members, especially targeting young people with an average age of 25 in the field of Cyberterrorism.

2.2.4 Combating Cyberterrorism in Social Media

When the use of social media became popular among individuals and groups worldwide, it is evident that various terrorist groups also started using social media for communication with each other and their followers. International terrorist groups such as ISIS, Jabhat al Nusra, Al-Qaeda, and others utilize social media for disseminating their missions and activities under the guise of 'Jihad,' as well as for communicating with other groups (Hossain, 2015).

Terrorist elements do not hesitate to use the cyber world for their actions, often employing it for Education, Planning, Propaganda, Dissemination of False Information, Recruitment and Communication, Cyber Attacks and Provocation, Fundraising and Financial Transactions, and Psychological Warfare purposes.

Education: Social media can serve as a suitable platform for the education of terrorist elements. Especially for training in various areas such as basic weapons use, homemade explosive manufacturing, intelligence gathering, and cyber attacks, these platforms are utilized. Existing members are kept ready for terrorist organizations, and various media outlets are used to be an impressive factor for newcomers. Terrorist organizations like ISIS and Al-Qaeda attempt to gather crowds through publications such as "The Wolves of Manhattan" (ADL, 2023).

Planning: Just as terrorist organizations use social media for recruiting members and education, they also utilize these tools for planning their actions. They gather data such as satellite images, street views, and images shared on social media related to a specific target, transforming them into meaningful data using artificial intelligence. In this way, they can obtain sufficient data for planning purposes to carry out the attack (Parlakkılıç, 2018).

Propaganda: Terrorist organizations use social media to spread extreme ideologies, attract followers, and radicalize individuals. They share propaganda videos, speeches, or written content to introduce their causes and attract sympathizers. For instance, Al-Qaeda launched a campaign titled "They're Back" in 2021 to encourage terrorist attacks, gaining widespread coverage in the American media. They shared videos explaining how

jihadist elements should arm themselves, what steps to take for attacks, engaging in propaganda activities (Goudie & Barb).

Dissemination of False Information: Cyber terrorists can spread false information or fake news to create fear, confusion, or manipulate public opinion. This misinformation can be related to political events, social issues, or even health crises. Terrorist organizations can use false information and propaganda to radicalize people or create bias against a particular community. Spreading untrue or misleading information can influence people's thought patterns, beliefs, and behaviors, leading to changes desired by terrorist organizations. The strategy behind disseminating false news focuses on undermining trust in governments, taking steps that will lead to radicalization and creating a positive impression among followers.

Recruitment and Communication: Terrorist organizations primarily focus on Facebook, Twitter, and YouTube to recruit new members. Social media provides a channel for terrorists to recruit new members, communicate with sympathizers or agents, and coordinate their activities (Adap, 2021). Encrypted or password-protected messaging platforms are often used for secret communications.

Cyber Attacks and Provocation: Social media provides a platform for terrorist organizations to carry out cyber attacks and provocations. Organizations may attempt to harm their adversaries through cyber attacks or aim to create chaos by launching cyber attacks against specific targets. Additionally, they may try to incite community conflicts through provocative messages and shares on social media.

Fundraising and Financial Transactions: Social media can be used as a tool for terrorist organizations to secure funding and collect donations. Organizations may use social media platforms to coordinate and increase their financial resources. This serves as an essential means for organizations to sustain and expand their activities.

Psychological Warfare: Terrorist organizations conduct psychological warfare through social media to intimidate, subdue, and manipulate target communities. Visual content, threatening messages, and propaganda create a psychological impact on target communities, serving the objectives of terrorist organizations.

3. Conclusion

The role of social media in combating Cyberterrorism is becoming increasingly important due to terrorist organizations exploiting these platforms, particularly for planning, propaganda, and communication purposes. As social media becomes an effective tool for the spread of extreme ideologies and the coordination of cyber attacks, collaboration between governments, law enforcement agencies, and technology companies to develop robust strategies against these threats is inevitable.

Efforts to combat Cyberterrorism through social media should encompass various dimensions. Firstly, online security measures, such as advanced algorithms and artificial intelligence, need to be strengthened to rapidly detect and neutralize terrorist content. Additionally, as cyber threats often transcend national borders, encouraging international collaboration is of vital importance. Initiatives for information sharing and cooperation between countries can enhance collective capabilities in combating Cyberterrorism.

Public awareness and digital literacy campaigns are believed to play a crucial role in preventing radicalization and promoting responsible online behavior. Providing education to users about the potential dangers of extremist content and emphasizing the importance of reporting suspicious activities can contribute to creating a safer online environment. Furthermore, the effective enforcement of laws and regulations holding social media platforms accountable for hosting terrorist content is essential. This entails the development and implementation of policies involving close collaboration between governments and technology companies.

In conclusion, the significance of social media in combating Cyberterrorism is critical from both a threat and defense perspective. It is recommended that societies collaborate by leveraging technology, international cooperation, public awareness, and regulatory frameworks to reduce the risks associated with terrorist groups misusing social media. In this way, social media can become a powerful tool contributing to the establishment of a safer and more secure digital environment for everyone.

References

Adap, J. (2021). The Cyber Battleground: An Analysıs On The Use Of Social Media For Terrorist Recruitment. *Rebuplic of the Philippines National Defense Collage of The Philippines*.

ADL. (2023, 12 09). https://www.adl.org/resources/blog/islamists-launch-three-new-magazines-hoping-one-will-inspire adresinden alındı

Andrews, S., Brewster, B., & Day, T. (2018). Organized crime and social media: a system for detecting, corroborating, and visualizing weak signals of organized crime online. Security Informatics, 7(1). https://doi.org/10.1186/s13388-018-0032-8

Boyd, D., & B. Ellison, N. (2008). Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 210-230.

Burgess, J., Marwick, A., & Poell, T. (2018). *The SAGE Handbook of Social Media.* California: SAGE Publications Ltd.

Collin, B. (1997). Future of Cyberterrorism: The Physical and Virtual Worlds Converge. Crime and Justice International, 13(2), 15-18.

Çıtak, E. (2021). Siber Terörizm: Potansiyelin Gerçekçi Tehdidi. Turkuaz Uluslararası Sosyo-Ekonomik Stratejik Araştırmalar Dergisi, 3(1)

Gercke, M., & Brunst, P. (2009). *Praxishandbuch Internetstrafrecht.* Stuttgart: Kohlhammer.

Global Cybersecurity Index. (2020). Geneva: International Telecommunication Union (ITU). Global Cybersecurity Index 2020: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E adresinden alındı

Goudie , C., & Barb, M. (tarih yok). *ABC Chicago.* https://abc7chicago.com/al-qaeda-terrorism-terrorist-attack-inspire-magazine/10918191/ adresinden alındı

Gretzel, U. (2015). Web 2.0 and 3.0. In L. Cantoniand J. A.Danowski (Eds.),Communication and Technology, Handbooks of Communication Science Series, Vol. 5. Berlin: De Gruyter Mouton,pp. 181-192.

Hossain, M. S. (2015). Social media and terrorism: threats and challenges to the modern era. South Asian Survey, 22(2), 136-155.

Kemp, S. (2023, 08 23). *DIGITAL 2023: GLOBAL OVERVIEW REPORT.* www.wearesocial.com: https://wearesocial.com/wp-content/uploads/2023/03/Digital-2023-Global-Overview-Report.pdf adresinden alındı

M.Kaplan, A., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of Social Media. *Kelley School of Business*, 59-68.

Parlakkılıç, A. (2018, 12 30). Cyber Terrorism Through Social Media: A Categorical Based Preventive Approach. *International Journal of Information Security Science*, s. 172-178.

Pollitt, M. M. (1998). Cyberterrorism- Fact or Fancy?, Computer Freud&Security, 8- 10.

Smith, K. T., Smith, L. M., Burger, M., & Boyle, E. S. (2023). Cyber terrorism cases and stock market valuation effects. Information & Computer Security.

Statista. (2023). https://www.statista.com/markets/424/topic/1065/cyber-crime-security/#statistic1 adresinden alındı

United Nations. (2015). *Population 2030, Demographic Challenges and Opportunities for Sustainable Development Planning.* New York: United Nations.