[H]CYBER ATTACKS: ARE THEY THE TERRORISM OF THE FUTURE?

SİBER SALDIRILAR: GELECEĞİN TERÖRÜ MÜ?

Dr. Öğr. Üyesi Kayser (Qaisar) NASRAT [*]

ÖZET

Teknolojik gelişmeler günlük yaşantımızın her alanını kapsayarak büyük avantajlar sağlarken aynı zamanda siber saldırı tehditleri de giderek daha kritik bir endişe haline gelerek terörizmdeki potansiyel rolleri hakkında sorular ortaya çıkarmaktadır. Bu makale, siber saldırılar ve terörizmin kesişimini inceleyerek yeni bir terörizm biçimi olarak siber terörizmin potansiyellerine odaklanmaktadır. Her ne kadar geleneksel terörizm fiziksel şiddet ve zarar ile ilişkilendiriliyor olsa da kritik altyapıların teknolojiye daha da bağımlı hale gelmesiyle birlikte teröristlere fiziksel varlığa ihtiyaç duymadan ve az maliyetle ciddi etkilere sahip siber saldırılar gerçekleştirmesinin yeni yollarını sağlamaktadır. Ayrıca bu makale, kritik altyapı, finansal sistemler ve hükümet kuruluşlarını hedef alan son zamanlardaki yüksek profilli siber saldırıları inceleyerek, geleneksel terör eylemleri ile siber terörizm arasındaki amaç, niyet, etki ve nüfus üzerindeki psikolojik etkiler açısından benzerlikleri vurgulamaktadır. Dolayısıyla, siber terörizm yalnızca politik şiddet için bir araç değil, aynı zamanda ekonomik, sosyal ve psikolojik zarar verme yöntemi olup hükümetler ve küresel güvenlik için önemli zorluklar sunmaktadır. Makale, siber saldırıların bir terörizm biçimi olarak yasal ve etik etkilerini incelemekle birlikte gelecekte ortaya çıkacak eğilimleri, siber tehditlerde yapay zeka (AI) ve makine öğreniminin artan kullanımını da içerecek şekilde araştırmaktadır. Sonuç olarak, siber saldırıların gelecekte terörizmin temel unsurlarından biri haline gelmeye hazır olduğunu ve küresel güvenlik açısından çok önemli sonuçlar doğuracağını ileri sürmekte ve gelecekteki yörüngesine ilişkin önemli içgörüler sunmaktadır.

[H] Eserin Dergimize geliş tarihi: 06.11.2025. İlk hakem raporu tarihi: 04.12.2025. İkinci hakem raporu tarihi: 15.12.2025. Onaylanma tarihi: 15.12.2025

[*] Assistant Prof. Dr., University of Ibn Haldun Faculty of Law, International Law, E-mail: qaisar.nasrat@ihu.edu.tr, Yazarın ORCID Belirleyicisi: 0000-0003-4676-8122

Esere Atıf Şekli: Kayser (Qaisar) Nasrat, *"Cyber Attacks: Are They the Terrorism of the Future?"*, YÜHFD, C.XXIII, 2026/1, s. 243.

Anahtar Kelimeler: *Kritik altyapı, Siber güvenlik, Siber tehditler, Siber terörizm, Ulusal güvenlik.*

ABSTRACT

While technological advances have encompassed every aspect of our daily lives and provided great advantages, cyberattacks have also become an increasingly critical concern, raising questions about their potential role in terrorism. This article examines the intersection of cyberattacks and terrorism, focusing on the potential of cyberterrorism as a new form of terrorism. While traditional terrorism has been associated with physical violence and harm, the increasing reliance on technology in critical infrastructures has provided terrorists with new ways to carry out serious cyberattacks without the need for physical presence and at low cost. In addition, this article examines recent high-profile cyberattacks targeting critical infrastructure, financial systems, and government organizations, highlighting the similarities between traditional terrorist acts and cyberterrorism in terms of purpose, intent, impact, and psychological impact on the population. Thus, cyberterrorism is not only a tool for political violence, but also a method of inflicting economic, social, and psychological harm, presenting significant challenges to governments and global security. The article examines the legal and ethical implications of cyberattacks as a form of terrorism, as well as exploring future trends that include the increasing use of artificial intelligence (AI) and machine learning in cyber threats. It concludes by arguing that cyberattacks are set to become a key element of terrorism in the future, with significant implications for global security, and offers important insights into their future trajectory.

Keywords: *Critical infrastructure, Cybersecurity, Cyberterrorism, Cyber threats, National security.*

EXTENDED SUMMARY

In the technological age we live in, the rapid advancement of technology has brought numerous benefits but also brought critical security threats. The most urgent of these threats is cyberterrorism, a form of terrorism that uses digital technologies to achieve ideological, political, or strategic goals. Unlike traditional terrorism that involves physical violence,

cyberterrorism targets digital infrastructure and can be carried out remotely and anonymously. Due to its efficiency, accessibility, and global reach, it is increasingly seen not only as a complement, but also as a potential replacement for traditional forms of terrorism. The article begins by explaining the emergence and nature of cyberterrorism. Cyberattacks are malicious activities that aim to gain unauthorized access to, damage, or disrupt information systems and networks. These can include malware, phishing, ransomware, Distributed Denial of Service (DDoS) attacks, and Advanced Persistent Threats (APTs). Terrorist groups use these attacks to cause widespread disruption, steal information, and spread fear, often with political or ideological motivations. A notable feature of cyberterrorism is its ability to cross national borders without physical intervention, making it difficult to detect, monitor, and prevent.

The relationship between traditional and cyberterrorism is a central topic of debate. While traditional terrorism often involves physical violence, bombings, and armed attacks, cyberterrorism often targets virtual systems with the intent to cause psychological, economic, or social harm. The lower cost, high levels of anonymity, and remote execution make cyberterrorism attractive to non-state actors and smaller groups. Scholars such as Mark Pollitt and Dorothy Denning define cyberterrorism as politically motivated attacks on digital infrastructure aimed at intimidating societies or governments. Denning emphasizes the ideological purpose behind the attacks and the potential for real-world consequences such as economic collapse, infrastructure failure, or public panic.

Terrorist organizations are increasingly using cyberspace for a variety of purposes beyond direct attacks. The internet serves as a platform for recruitment, radicalization, training, dissemination of propaganda, and financing operations. Online platforms provide anonymity and broad access, allowing terrorist cells to operate effectively across borders. Notable examples include the use of websites to raise funds, train new recruits, and coordinate attacks. The case of the Irish Republican Army (IRA), which used online portals to raise funds, illustrates the practical use of the internet in modern terrorism.

The impact of cyberterrorism on national and global security is significant. Incidents such as the 2007 cyberattack on Estonia, the Stuxnet virus targeting Iranian nuclear facilities, and interference in the 2016 U.S. presidential election highlight the destructive potential of cyberterrorism. These incidents have caused significant economic losses, disrupted essential services, and threatened political stability. Such attacks demonstrate how

digital vulnerabilities can translate into real-world consequences affecting everything from health care to energy supply to public trust in democratic systems.

The article then examines the legal and definitional challenges of cyberterrorism. There is no universally accepted definition, and different scholars and institutions propose different criteria. While Denning discusses ideological motivations and societal intimidation as key elements, others, such as Gabriel Weimann, focus on the disruption of critical infrastructure, independent of physical violence. This definitional ambiguity complicates policy responses and international cooperation as states struggle to agree on what constitutes cyberterrorism.

Moving into the future of cyberterrorism, the article highlights growing concerns about advanced technologies such as artificial intelligence (AI), machine learning (ML), and the Internet of Things (IoT). These technologies increase the potential attack surface and make digital infrastructure more vulnerable. For example, AI can be used to develop self-learning malware that evades detection. Future scenarios that scientists envision include attacks on financial systems, transportation networks, gas pipelines, and pharmaceutical manufacturers—each of which could cause major economic or human losses. Moreover, cyber-physical attacks on infrastructure such as power grids or water supply systems can paralyze cities and even countries.

The concept of cyber-physical warfare is particularly concerning because these attacks connect the digital and physical realms. For example, hackers targeting an air traffic control system can cause fatal plane crashes, while manipulating pressure valves on gas pipelines can lead to deadly explosions. Cyberterrorism, which can infiltrate systems and remain undetected for years, also poses long-term risks to national security.

In summary, it emphasizes that cyberterrorism is rapidly evolving along with technological innovation. The increasing complexity and interconnectedness of global systems magnifies the threat. While traditional terrorism persists, the emergence of cyberterrorism represents a paradigm shift and requires new strategies for prevention, detection, and international cooperation. Cyberterrorism is not just a technical or cybersecurity problem, but also a political, ethical, and legal challenge that requires coordinated responses from governments, private sectors, and international organizations. As a result, cyberterrorism is poised to become one of the most critical security challenges of the 21st century. Its low barriers to entry, global accessibility, and destructive capacity demand urgent action. As technology continues to evolve, so will terrorists' tools and tactics. The fight against

cyberterrorism will require not only technical solutions, but also robust legal frameworks, international agreements, public-private partnerships, and a deep understanding of the political and ideological drivers behind this modern form of warfare.

INTRODUCTION

The rapid development and rise of technology provides many advantages for modern society, but also brings with it some disadvantages and threats. One of the most important of these threats is cyber attacks. These attacks, usually carried out by hackers, terrorist groups or state-sponsored actors, target computer systems, networks and digital infrastructures with the aim of causing damage, disruption and destruction. The increasing dependence of key critical sectors such as government, private sector, healthcare system and military on technology has become a battleground for various forms of conflict, including terrorism and terrorist groups. As a new phenomenon, cyber terrorism has become a significant concern and threat due to its potential to cause serious damage such as widespread chaos and fear, disrupting economies and undermining national security without the need for traditional weapons.

Cyber terrorism, like traditional forms of terrorism, aims to instill fear in society with ideological and political motives, disrupt social order and challenge political or economic structures. However, unlike traditional terrorism, cyber terrorism can cross borders without direct physical conflict, making it difficult to detect, prevent or mitigate attacks. This raises critical questions: Can cyberterrorism replace traditional forms of terrorism in an increasingly digital world?

The emergence of cyberterrorism as a legitimate threat is reflected in the fact that technology has relied on digital systems for nearly every aspect of our lives from our financial transactions and communications to our healthcare and transportation networks. A successful cyberattack on these systems could wreak havoc. For example, a power grid outage could paralyze an entire city, while an attack on critical healthcare infrastructure could endanger countless lives. Terrorist organizations, especially those with a

transnational reach, have adopted cyberattacks as a means of recruiting and propaganda to advance their own agendas, as well as to achieve their terrorist goals.

The importance of this study emphasizes the current and future threat of cyber terrorism as a form of terrorism. Especially with the emergence of advanced technologies such as artificial intelligence, machine learning and the expansion of the Internet of Things (IoT), the potential for cyber threats is increasing. Thus, the risks associated with cyber terrorism continue to increase and require policy makers, cyber security experts and the international community to take urgent measures.

This article consists of three parts. In the first part, a clear definition and information is provided about cyber attacks and their relationship with terrorism and the types of cyber attacks. It will examine the differences between traditional terrorism and cyber terrorism and focus on the impact of cyber attacks. In the second part, it is examined whether cyber attacks constitute terrorism and in which areas cyber terrorism is addressed. In the third part, it is tried to predict the future scenarios of cyber terrorism and the role of advanced technologies such as artificial intelligence in shaping this new form of conflict.

I. TERRORISM IN THE MODERN AGE

Today, with the advancement of technology, terrorism is also evolving. While traditional forms of terrorism such as bombings and armed attacks continue to pose threats, cyber terrorism is emerging as new and more complex threat methods. These new age threats pose extremely serious dangers to states and security institutions and require the development of new strategies to protect against them.

A. Definition and Types of Cyber Attacks

Cyber attacks have become one of the most important threats to the security of individuals, organizations and states. A cyber attack is any malicious attempt or activity designed to compromise, interfere with, prevent access to or destroy information systems or data. Cyber attacks aim to illegally access or damage computers, networks and information processing systems in order to cause harm. Such attacks can disable or take control of digital environments, and can also change, block, delete, manipulate or

expropriate data stored in these frameworks.[654] These attacks can vary in size, impact, complexity, and intent, but they all share the common goal of exploiting weaknesses in technological infrastructure to cause harm and malicious intent.

Cyber attacks are often carried out by hackers, cybercriminals, terrorist organizations, state-sponsored individuals and groups. The reasons behind these attacks include financial gain, espionage, public fear and panic, or political motivations.

Cyber attacks can manifest in many forms, including malware, phishing, ransomware, denial of service (DoS), and distributed denial of service (DDoS) attacks. A denial of service (DoS) attack is a cyber attack that aims to disrupt the services of a connected host, making a machine or network resource inaccessible to its legitimate users. This is usually done by overwhelming the target with excessive requests, causing the system to become overloaded and unable to process valid requests. The goal of a DoS attack is to temporarily or permanently deny service to legitimate users. It can be likened to a group of people blocking the entrance to a store, preventing customers from entering, and disrupting normal operations.[655]

A DDoS attack is a type of DoS attack in which multiple compromised systems, usually infected with a Trojan horse, are used to target a single victim. In a DDoS attack, incoming traffic floods the victim's system from multiple sources, potentially hundreds of thousands or more. This widespread distribution makes it impossible to stop the attack by simply blocking one IP address. It also becomes extremely difficult to distinguish legitimate traffic from attack traffic when it comes from multiple different points. Both the targeted system and the compromised machines used in the attack are considered victims.[656] Ransomware is a type of malware that threatens to release or permanently block access to a person's data unless a ransom is paid. While basic ransomware can lock down a system in a way that can be easily undone by someone with technical knowledge, more sophisticated versions use a method called cryptoviral extortion. This technique encrypts the victim's

[654] Proofpoint, 'What Is a Cyber-Attack?' https://www.proofpoint.com/au/threat-reference/cyber-attack accessed 28 April 2025.

[655] Ahmed Khan, Dipak, Kannan, Kiran, Kulkarni Madunix, Mohamed Iqbal, Nitai, Sagar and Shrikanth, *Attack Types*, https://wentzwu.com/wp-content/uploads/2020/06/All-type-of-attack.pdf, Date of Access: 29.04.2025.

[656] Ibid.

files, making them inaccessible, and demands payment for decryption.[657] Advanced Persistent Threat (APT) is a stealthy and persistent cyber attack targeting specific organizations or governments for commercial or political reasons. It involves sophisticated malware techniques to exploit system vulnerabilities and external command and control systems monitor and extract data over long periods of time. Human participation orchestrates the attack and ensures persistence and stealth throughout the process.[658]

In addition to the above attack types, Phishing attacks use deceptive emails, websites, or messages to trick individuals into disclosing sensitive information such as login credentials, financial details, or personal data. These methods are often employed to collect intelligence or gain unauthorized access to critical systems.[659] Also, Stuxnet-like attacks refer to targeted cyberattacks designed to disrupt industrial control systems, such as those found in nuclear facilities. Cyberterrorists may focus on critical infrastructure systems with the intent to cause physical damage or destruction.[660]

II. Legal and Conceptual Framework of Cyber Terrorism

A. Traditional Terrorism vs. Cyber Terrorism

Terrorism is a term that is difficult to define clearly. In fact, many academic works on the subject include a section, chapter, or even multiple chapters discussing the challenges involved in establishing a precise definition. Therefore, understanding terrorism necessitates establishing a conceptual basis before moving on to the discussion of cyber terrorism.

In his 1998 article "Cyberterrorism: Fact or Fancy?" published in Computer Fraud and Security, Mark M. Pollitt uses the definition of terrorism found in Title 22, Section 2656f(d) of the United States Code. According to that statute, terrorism is defined as: "The term 'terrorism' means premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually

---

[657] Cisco, 'What Is the Difference: Viruses, Worms, Trojans, and Bots?' http://www.cisco.com/c/en/us/about/security-center/virus-differences.html accessed 30 April 2025.

[658] Ibid.

[659] S Iftikhar, 'Cyberterrorism as a Global Threat: A Review on Repercussions and Countermeasures' (2024) 10 *PeerJ Comput. Sci.* e1772 http://doi.org/10.7717/peerj-cs.1772 accessed 23 June 2025.

[660] Ibid.

intended to influence an audience." This definition provides a framework for evaluating cyber terrorism by highlighting the elements of "violence," "political purpose," and "civilian target."

Pollitt merges Collin's definition of cyberspace with the U.S. Department of State's definition of terrorism to create a narrowly focused working definition of cyberterrorism: "Cyberterrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub-national groups or clandestine agents." This unified definition positions cyberterrorism as a version of the classical concept of terrorism adapted to the digital environment.

Traditional terrorism often involves acts of physical violence, such as bombings, armed attacks, or attacks on infrastructure, to instill fear and achieve political goals. In contrast, cyber terrorism operates in the digital realm to achieve similar goals of disruption and intimidation. Thus, while both forms of terror serve similar purposes, they show a clear distinction in terms of their methods of action. The key difference lies in the method: While traditional terrorism targets physical spaces, cyber terrorism focuses on digital infrastructure. However, it is important to note that cyber attacks can also cause significant physical damage. Unlike traditional terrorism, which requires significant physical resources such as conventional weapons and personnel, cyber terrorism can be carried out via the internet by individuals or small groups with limited means. This makes cyber terrorism more attractive than traditional terrorism in terms of both accessibility and cost-effectiveness.

The 2007 DDoS attacks on Estonia and the 2010 Stuxnet operation are considered pivotal moments in the evolution of cyber threat discourse, demonstrating that cyber operations can transcend the digital realm and have real-world consequences. The attacks on Estonia marked the first instance of a cyber operation effectively disrupting the functioning of a sovereign state, temporarily paralyzing essential state functions, including banking, media, and e-government services. Similarly, Stuxnet's targeting and disruption of Iranian nuclear centrifuges demonstrated that malicious code could lead to physical destruction, fundamentally altering the debate about the scope and nature of cyber threats.

However, legally, Stuxnet is not generally classified as cyberterrorism. Since it is understood to be a state-to-state operation causing physical damage to critical infrastructure, academics generally consider it within the framework of Article 2(4) of the UN Charter, which prohibits the

use of force in international relations. The Tallinn Manual 2.0 also confirms that cyber operations that produce physical effects comparable to kinetic attacks can constitute "the use of force".

However, Stuxnet does not meet the criteria for terrorism because it was not perpetrated by non-state actors and did not aim to intimidate a civilian population. This distinction highlights a critical analytical point: while Estonia 2007 and Stuxnet 2010 demonstrate that cyber operations can go beyond mere digital disruption, only attacks carried out by non-state actors acting with coercive intent fall within the definition of cyberterrorism.

Cyber terrorism is attractive to terrorists for the following reasons:

▪ Compared to traditional terrorism methods, cyber terrorism is significantly less costly. A terrorist only needs a personal computer with an internet connection; there is no need to purchase weapons such as guns or explosives.

▪ Cyber attacks offer a level of anonymity that traditional terrorism does not. This makes it difficult for police and military to track cyber terrorists because they often hide behind aliases or access websites as anonymous users.

▪ There are numerous potential targets for cyber terrorism, including government infrastructure, utilities, private companies, airlines, and individuals. Furthermore, critical infrastructures such as emergency services and power grids are particularly at risk due to the complexity of computer systems, making it difficult to secure every possible point of failure.

▪ One of the most appealing features of cyber terrorism is that it can be carried out remotely. It requires minimal physical effort or training, and significantly reduces the risk of injury or death to the perpetrator. This makes it easier for terrorist organizations to recruit and retain members.

▪ Cyber attacks can attract media attention because they cause widespread disruption and damage. This wide visibility is often a key target for terrorist groups because it helps them spread fear and gain visibility.

When these elements are considered together, cyberterrorism presents a more cost-effective, more anonymous, broader targeting, and less risky operational arena than traditional terrorism. Therefore, the appeal of cyberterrorism requires modern states and the international community to take this threat increasingly seriously.

B. Cyber Attacks As A Form of Terrorism

Before cyberattacks can be considered within the scope of terrorism, the legal, political, and theoretical frameworks of the concepts of ‘terror’ and

'terrorism' must first be established. While there is no common definition of terrorism in international law, the UN Security Council, the EU Framework Decision 2002/475/JHA, and US federal legislation recognize political/ideological aims, instilling serious public fear, coercing state authority, and influencing society as common denominators.[661] In Türkiye, the Anti-Terror Law No. 3713 defines terrorism as organized activities aimed at achieving political objectives through force/violence, threats, pressure, and intimidation.[662] The common aspect of these definitions is that they explain terrorism not only through physical violence but also through its capacity to inflict widespread harm targeting state authority and social order. This definition allows digital attacks to be considered the functional equivalent of violence, even if they do not involve classical physical violence, due to the destructive consequences they inflict on critical infrastructures.

Impacts such as the collapse of energy transmission systems, the dysfunction of hospitals, the halting of banking infrastructure, and the disruption of water/transportation networks can be considered the digital form of the element of 'violence'. Therefore, the literature increasingly argues that cyberattacks are a form of 'digital violence'.[663] A similar approach exists in the Turkish academic literature. Oğün & Kaya (2013) emphasize that cyberattacks can affect state security as much as classical terrorism.[664] Gürcan & Erdoğan (2018), on the other hand, argue that due to the fragility of critical infrastructures, cyberterrorism should not be considered a separate category in the definition, but rather a digital variant of terrorism.[665] This framework provides a strong basis for discussing cyberattacks separately in terms of terrorism law.[666] These assessments reveal that cyberattacks have the potential to create social fear, chaos, and security vulnerabilities similar to terrorist acts.

Some argue that "cyber terrorism" doesn't truly exist, that while terrorists may use the Internet, terrorism must involve a tangible, physical attack. I would disagree. In today's world, many aspects of our daily lives

[661] UN Security Council Resolutions 1373, 1566; EU Framework Decision 2002/475/JHA.
[662] 3713 sayılı Terörle Mücadele Kanunu, Kabul: 12 Nisan 1991.
[663] Denning (2010); Weimann (2005).
[664] Oğün, S. & Kaya, Ö., "Siber Güvenliğin Milli Güvenlik Açısından Önemi." Uluslararası Güvenlik ve Terörizm Dergisi, Cilt 4, Sayı 1 (2013): ss. 27–45.
[665] Metin Gürcan & M. Erdoğan, "Siber Terörizm ve Kritik Altyapılar." Güvenlik Bilimleri Dergisi, Cilt 7, Sayı 2 (2018): ss. 65–90.
[666] Duygu Öztürk, "Türkiye'de Siber Terörizm ve Hukuki Boyut." Türkiye Adalet Akademisi Dergisi, 2020/4, ss. 233–260.

depend heavily on cyberspace, creating new avenues for direct terrorist action. These opportunities are growing as our reliance on digital systems increases. Potential cyber attacks include web defacement, the use of malware, data breaches, online training, and Denial of Service (DoS) attacks. With the growing use of SCADA systems to manage critical infrastructure, a successful cyber attack on these systems could have consequences as real and destructive as a conventional bomb.[667] Therefore, considering the condition of physical violence only in its traditional sense narrows the scope of modern digital threats and ignores the real impact of cyberterrorism.

Terrorists use the Internet for many different reasons. It makes terrorists' work much simpler and has a much wider reach than non-electronic means. Cyberspace offers terrorist organizations many potential avenues for exploitation. It provides a means of recruitment, radicalization, propaganda and fundraising, as well as fast and simple command and control.[668] This functionality makes the Internet both an operational tool and a direct attack platform for terrorist organizations.

Threats emerging in cyberspace extend beyond physical damage, information theft, and espionage. The Internet, widely used as a communication tool, can also be exploited for spreading misinformation and propaganda, leading to indirect but significant harm.[669] Therefore, cyber attacks have increasingly begun to be considered a form of terrorism, along with the increasing dependence on digital infrastructure in almost all areas of modern life. The traditional understanding of terrorism generally aims to create fear through physical violence or threats against civilians and to trigger political, religious or ideological changes. However, the tight integration of the digital world into the global infrastructure has made cyber attacks an effective tool for carrying out terrorist acts.

Although many studies have been conducted on cyber terrorism, there is no universally accepted definition of cyber terrorism, as there is for terrorism. Therefore, different academic and institutional definitions of cyber terrorism are made.

The term "cyber terrorism" was first coined in the 1980s by Barry Collin, who argued that it resulted from the merging of two realms: the virtual

---

667 Jpiag CHARVAT, *Cyber Terrorism: A New Dimension in Battlespace*, Centre of Excellence Defence Against Terrorism, 7.

668 Ibid *3.*

669 MN Öğün and A Kaya, 'Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler' (2013) 9(18) *Güvenlik Stratejileri Dergisi* 145–181.

and the physical. This intersection between cyberspace and traditional terrorism is at the core of cyberterrorism. Cyberspace refers to the abstract, digital environment in which computers and networks operate, while the physical world is our tangible, everyday reality. As these two worlds become increasingly interconnected, the resulting complexity gives rise to the phenomenon of cyberterrorism.[670]

Professor Dorothy Denning, who teaches at the Naval Postgraduate School, proposed a widely recognized definition of cyber-terrorism. According to Denning, cyber-terrorism is:

"The convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack 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 cyber-terrorism, 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, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber-terrorism, depending on their impact".[671] This definition recognizes that the violent impact of an act can occur not only through physical destruction but also through the paralysis of critical infrastructure.

Professor Dorothy Denning outlined the following criteria to define cyber-terrorism:

- The participants are non-state actors.
- The attacks are computer-based and target IT infrastructure.
- The victims are societies or governments.
- It is a form of terrorism confined to cyberspace.
- The disruption or destruction is directed at digital assets rather than physical property or individuals.[672]

[670] R Ahmad and Z Yunos, 'A Dynamic Cyber Terrorism Framework' (2012) 30 *International Journal of Computer Science and Information Security* 149–158.

[671] M Nadjib and H Cangara, 'Cyber Terrorism Handling in Indonesia' (2017) 9(2) *The Business and Management Review* 274.

[672] Weimann (11) 129-1.

In contrast to Denning, another leading scholar in this area, Gabriel Weimann, defines cyberterrorism as: "Cyberterrorism is the use of computer network tools to harm or shut down critical national infrastructures (such as energy, transportation, government operations)".[673] There are four key differences between this definition and Denning's. First, unlike Denning's definition, which does not specify that cyberterrorism must be carried out via a computer—only that it involves an attack "against computers, networks, and the information stored therein"[674]—Weimann's definition emphasizes computers as both the means and the target of the attack. Second, Weimann's definition does not provide any information regarding the attackers' motivations, whereas Denning emphasizes the significance of political and social objectives.[675] Third, according to Weimann, cyberterrorism pertains solely to the use of computers as a weapon targeting the networks essential to critical national infrastructures (CNI). Fourth, Weimann's definition does not require that physical violence against people or property, or significant economic damage, must occur for an attack to be classified as cyberterrorism.[676] These differences indicate that there is no consensus at academic and institutional levels in defining cyber terrorism.

There has also been much debate about which actions constitute cyberterrorism. On this issue, Denning states: "cyberterrorism has been used to characterise everything from minor hacks to devastating attacks".[677] Embar-Seddon also rejects the broad range of activities that fall under the term cyberterrorism.[678] According to her, actions such as "hacking" should be classified as "unauthorized access to or use of a computer system" rather than cyberterrorism.[679] Similar to Weimann, she defines cyberterrorism as "acts of terrorism carried out through the use of a computer".[680] Additionally, Embar-Seddon argues that the presence of offline violence is necessary for an act to

[673] Ibid 130.

[674] Denning, "Cyberterrorism: Testimony."

[675] Andrew Whiting, Stuart Macdonald, and Lee Jarvis, Cyberterrorism: Understandings, Debates and Representations , p. 3.

[676] Ibid 4.

[677] D Denning, 'Terror's Web: How the Internet is Transforming Terrorism' in Y Jewkes and M Yar (eds), *Handbook on Internet Crime* (Willan Publishing 2010) 7.

[678] A Embar-Seddon, 'Cyberterrorism: Are We Under Siege?' (2002) 45 *The American Behavioral Scientist* 1035, 1037.

[679] Ibid 1037.

[680] Ibid 1035.

be considered cyberterrorism.[681] This perspective is shared by Heickerö[682] and Maura Conway, who argue that for an attack to be considered cyberterrorism, it must "result in death and/or large-scale destruction".[683] In addition, Maura Conway described cyber-terrorism as the fusion of two anxieties: the fear of technology and the fear of terrorism.[684]

While effects-based definitions focus on the aftermath of cyber-attacks, other definitions emphasize the objectives of the attack's perpetrator. Intent-based definitions, for example, define cyberterrorism as " politically motivated computer attacks [that] are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage".[685] In this view, cyberterrorism is distinguished from other forms of online activity by the perpetrator's underlying intentions. Jerrold Post, Keven Ruby, and Eric Shaw provide a similar perspective, stating that cyberterrorism is characterized by " the degree to which the attack was designed to produce fear and intimidation in the target audience in order to accomplish an ideological goal".[686] These elements of fear and intimidation, aimed at advancing broader political or ideological aims, are common in many general definitions of terrorism.[687]

Some institutional definitions have also been made regarding cyber terrorism. The U.S. Federal Bureau of Investigation (FBI) defines cyber-terrorism as any "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents".[688] As seen in this definition, cyber terrorism is not only a technical attack but also an organized action with political aims. In addition,

[681] Ibid, 1037.

[682] R Heickerö, 'Cyberterrorism: Electronic Jihad' (2014) 38 *Strategic Analysis* 555.

[683] Maura Conway, "Reality Bytes: Cyberterrorism and Terrorist 'use' of the Internet," *First Monday*, (2002) 7.

[684] MN Ogun, S Yurtsever, M Aslan and M Elburasi, 'Terrorist Use of Cyber Technology' (2021) 9 *International Conference on Natural Sciences and Technologies*, 113–128 https://doi.org/10.20290/estubtdb.1021324.

[685] J Hua and S Bapna, 'How Can We Deter Cyber Terrorism?' (2012) 21 *Information Security Journal: A Global Perspective* 104.

[686] JM Post, KG Ruby and ED Shaw, 'From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism' (2000) 12 *Terrorism and Political Violence* 101.

[687] Whiting (20) 5.

[688] Weimann (17) 129-1.

it is implied in this definition of the FBI that the element of "violence" can be evaluated not only physically but also in terms of the indirect results that cyber terrorism can cause. For example, an act of cyber terrorism against a power plant can lead to a great loss of life despite not being a direct physical attack. This also shows that the effects of cyber terrorism can be at least as destructive as traditional terrorism.

The North Atlantic Treaty Organization (NATO) defines cyber terrorism as: "A cyber-attack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal".[689] NATO's definition of cyber terrorism highlights several key points. To be considered cyber terrorism, it is to disrupt services or compromise digital infrastructure by using computer systems or communications networks. The aim of these attacks is not just to cause minor damage; they must be significant enough to cause significant damage, such as physically destroying infrastructure or causing operational disruptions to essential services such as electricity, finance or transportation. The broader aim of cyber terrorism is to create fear or panic among the population for ideological and political reasons.

A publication by the European Council titled *Cyber-terrorism: The Use of the Internet for Terrorist Purposes (Terrorism and Law)* defines cyber-terrorism as encompassing all activities conducted by terrorist cells or individuals via the Internet. Furthermore, the United Nations Office on Drugs and Crime identifies six primary ways in which the Internet can be used for terrorist purposes: spreading propaganda (including recruitment, radicalization, and incitement), financing operations, training, planning (through encrypted communications and open-source intelligence), execution of attacks, and direct cyber attacks.[690]

Cyber terrorism has profound effects on the economy and political stability. In this context, cyber attacks can have profound effects on a country's economy in various ways. One of the most direct consequences is the financial losses that can affect both businesses and governments. Such attacks often disrupt operations, leading to reduced productivity and revenue generation. As a result, organizations can face significant financial setbacks that can hinder economic growth. Cyber attacks can also lead to the theft of critical and sensitive information, such as intellectual property or trade

[689] C o. Terrorism (ed), *Responses to Cyber Terrorism* (1st edn, vol 34, IOS Press 2008).

[690] IG Seissa, 'Cyber-terrorism Definition Patterns and Mitigation Strategies: A Literature Review' (2017) 6(1) *International Journal of Science and Research (IJSR)* 180–186.

secrets, that can provide a competitive advantage to competitors. The loss of valuable data can damage a country's industry and weaken its economic standing.[691]

Another definition of cyberterrorism is that it is the unlawful use of computer technologies and related systems by actors to inflict violence or threaten violence in order to harm critical state infrastructure, individuals, or property, in order to achieve their political, social, or ideological goals.[692] In this context, Özdemir (2020) underlines three key elements that distinguish cyberterrorism from other cyber threats: (1) the act is carried out with an ideological or political objective, (2) it involves the intent to damage digital infrastructure, and (3) it aims to create fear, panic, or chaos in society. These criteria clearly distinguish cyberterrorism from ordinary cybercrimes. For example, a cyber fraud incident aimed at obtaining personal financial gain is considered a cybercrime, while an attack with an ideological aim and targeting energy infrastructure is classified as cyberterrorism.[693]

The impact of cyberterrorism on political stability can significantly affect politics by disrupting elections, spreading misinformation, and compromising state secrets. Cyberattacks targeting election systems or campaigns can sabotage the election process and undermine public confidence in the integrity of elections. Terrorists can use the internet and social media to spread propaganda to influence public opinion and shape political outcomes. Attacks on communications infrastructure, such as email or telephone systems, can disrupt communication between political leaders and organizations and with the public. Cyberattacks that violate privacy can also erode trust in political leaders and institutions.[694]

As a result, cyberterrorism possesses several key elements that distinguish it from ordinary cybercrime or state-sponsored cyber operations. First, the reference to the unlawful use of computer technologies underscores that cyberterrorism is essentially a criminal act encompassing both national and international legal frameworks. Second, by specifying violence or the threat of violence as a core element, the definitions emphasizes that

---

[691] J Hua and S Bapna, 'The Economic Impact of Cyber Terrorism' (2013) 22 *The Journal of Strategic Information Systems* 175–186 https://doi.org/10.1016/j.jsis.2012.10.004.

[692] B Yurtsever, *Küreselleşen Dünyada Terörizm: Siber Terörizm Örneği*. Yüksek Lisans Tezi, Niğde Ömer Halisdemir Üniversitesi, Kasım 2020, s. 82.

[693] E Mücahit, *Bir Siber Suç Olarak Siber Terörizm ve Türkiye* (Yüksek Lisans Tezi, Atatürk Üniversitesi Kriminalistik ABD, 2025), 4.; Ö Burak, "Türkiye'nin Siber Güvenlik Stratejileri," *Journal of National Defense* 12, no. 3 (2020): 100–115.

[694] Weimann (17) 129-149.

cyberterrorism is not limited to data manipulation or digital disruption; it includes actions aimed at creating harm, fear, or coercive pressure in the real world. Third, targeting critical infrastructure, individuals, or property reflects the strategic aim behind cyberterrorist acts, undermining societal stability, government authority, and public trust. Finally, its explicit association with political, social, or ideological aims places cyberterrorism within the broader conceptual family of terrorism, clarifying that the goal is not financial gain or espionage, but establishing coercive influence.

Building upon this distinction, it is also important to differentiate cyberterrorism from cyberattacks carried out by foreign states. Both may employ similar technical methods and target comparable systems, but they are subject to entirely different legal and conceptual regimes. Cyberterrorism is carried out by non-state actors whose primary aim is to instill fear, disrupt public order, or pressure governments through ideologically motivated violence. In contrast, state-sponsored cyber operations are assessed within the framework of interstate relations, state responsibility and depending on the situation, the law of armed conflict. Their motivations are typically strategic or geopolitical, not the psychological coercion of the civilian population. Therefore, attribution, legal characterization, and intended societal impact constitute the key dividing lines between cyberterrorist acts and hostile state cyber operations.

C. How Cyber Attacks are Used in Terrorism

Cyberattacks in the digital age have emerged as a significant tool for expanding terrorists' reach. Ranging from simple website defacements to complex data breaches, attacks on critical infrastructures, and cyber espionage, these attacks are often used to advance terrorist goals by creating fear, causing disruption, and gaining strategic advantage. This situation shows that cyber attacks have become not only a complementary element but also a direct operational tool for modern terrorist organizations.

In terms of the harm principle, cyber terrorism acts are directed at institutional, state or national interests[695] and not individual interests. Cyber terrorism acts that harm individual interests, such as loss of life or property, are only an indirect effect but are not the main target, which is usually directed at democratic environments.[696] Therefore, the main purpose of cyberterrorism

[695] A Gillespie, *Cybercrime: Key Issues and Debates* (Routledge 2016); A Jones, 'Cyber Terrorism: Fact or Fiction' (2005) 6 *Computer Fraud and Security* 4–7.

[696] OGUN (29).

acts is not to cause individual harm, but to target state authority, public order and social stability. In this context, terrorists and terrorist organizations use the Internet to achieve many goals.

Terrorist groups primarily use the Internet to finance themselves, recruit new members, train members of different cells, communicate, coordinate and carry out actions, obtain information, ideologically direct people, promote their organizations, and develop psychological warfare against the enemy.[697] This functional diversity makes the internet an indispensable platform for terrorist organizations' logistical, operational and psychological operations.

One of the primary ways cyberattacks are used in terrorism is to target critical infrastructure. Terrorists and terrorist groups can disrupt essential services such as electricity, water, and healthcare systems, causing widespread chaos and panic. For example, terrorists can disrupt power grids or transportation networks, paralyzing a city, region, or even a country. Such cyberattacks can cause long-term damage to public safety and economic stability, making people more vulnerable to fear and exploitation.

Another fundamental way in which cyberattacks are used in terrorism is through propaganda and psychological warfare. There are countless examples of how terrorists use cyberspace, an uncensored environment, to spread misleading information, make threats or distribute images of attacks. The uncontrolled circulation of images of torture, pleading and/or murder of hostages such as Americans Nicholas Berg, Eugene Armstrong and Jack Hensley, British Kenneth Bigley and Margaret Hassan or South Korean Kim Sun II on numerous internet servers and portals has further reinforced the sense of helplessness in Western societies and questioned the legitimacy and effects of "Operation Iraqi Freedom". In this way, groups manage to convey an image of internal vitality, strength and motivation, and their messages have a global impact. All of this is done to demoralize the US and its allies and strengthen the perception of fragility in these societies.[698] These propaganda and psychological warfare activities have the potential to create social panic, fear and insecurity without the need for physical attack.

In addition, terrorist organizations, like other organizations, use the Internet to finance themselves. In this, they have found a new way to raise

[697] G Weimann, 'How Modern Terrorism Uses the Internet' (2004) http://ics.leeds.ac.uk/papers/vp01.cfm?outfit=pmt&requesttimeout=500&folder=1259&paper=1542.

[698] A Merlos García, 'Internet como instrumento para la yihad' (2006) 8 *Araucaria* 80–99.

funds for the cause. Therefore, terrorists use Internet sites to collect donations from their supporters. For example, the Irish Republican Army (IRA) had a page on its website where visitors could make donations using their credit cards. However, they also use the Internet to extort financial groups, transfer money, make financial transfers through offshore banks, launder and steal money, use electronic money (cyber money) and smart cards, sell counterfeit products or commit various scams through spam emails, etc.[699] These digital financial activities allow terrorist organizations to both diversify their income and evade traditional financial monitoring mechanisms.

Terrorist organizations use the Internet not only as a means of propaganda and financing, but also as a means of education, planning, and communication. The anonymity and global reach offered by the Internet allow terrorist groups to communicate effectively with their members in different geographic areas and share educational materials and strategies. This situation makes it easier for terrorist organizations to organize and conduct operations independently of geographical limitations.

As a result, cyber attacks are becoming the most important element of modern terrorism. For terrorist organizations, the internet has gone beyond being just a means of communication and has become an indispensable platform for strategic planning, education and propaganda. In other words, when all these usage patterns are evaluated together, it is clear that cyber attacks are not only a complementary tool for modern terrorist organizations, but are increasingly becoming an autonomous method of terrorism.

III. THE FUTURE OF CYBER TERRORISM

With the advancement of technology, the world is becoming more and more interconnected and the specter of cyber terrorism is growing larger. Cyber attacks are no longer the sole preserve of hackers seeking financial gain; they are increasingly being used for political and ideological reasons and as a means of war. In parallel with the rise of advanced technology and artificial intelligence, the dependency on cyber digital infrastructure is increasing. This indicates that cyber terrorism will become increasingly prominent in the future. Cyber attacks, especially on critical infrastructures, can lead to major destruction and possible loss of life.

---

[699] G Sánchez Medero, 'Ciberespacio y el Crimen Organizado. Los Nuevos Desafíos del Siglo XXI' (2012) 10(16) *Facultad de Ciencias Políticas y Sociología Universidad Complutense de Madrid* 71–87.

Discussions about new vulnerabilities that could lead to cyberattacks continue, and the increasing number of "software exploits" is a growing concern. One of the biggest fears is that malicious actors, including terrorists, could gain enough technical knowledge to cause significant damage or even create software for government agencies. A major incident occurred in 2000 when Japan's Metropolitan Police Department revealed that the Aum Shinrikyo cult, responsible for the deadly Tokyo subway attacks in 1995 that killed twelve people and injured more than six thousand, was developing software for at least ten government agencies and eight Japanese companies. Members of the cult worked as subcontractors for various firms, making it nearly impossible for end users to identify the original developers of software they purchased.[700]

Collin outlines several terrifying scenarios in his vision of the "Future of Cyberterrorism":[701]

▪ Cyberterrorists disrupt banks, stock exchanges, and internal financial transactions, causing a complete loss of public trust in the economic system. While cyberterrorists are unlikely to target institutions such as the Federal Reserve due to rapid detection, they could shut down an entire country's economic grid from a distance across continents and cause widespread instability.

▪ A cyberterrorist attack on a next-generation air traffic control system could cause a catastrophic collision between two large civilian aircraft. This scenario is realistic because cyberterrorists could also manipulate cockpit sensors on the aircraft. Similar attacks could target rail systems.

▪ Cyberterrorists alter drug formulations at pharmaceutical manufacturers, causing devastating loss of life.

▪ Cyberattacks on pressure-regulating gas lines cause a valve failure, leading to a deadly explosion in a quiet suburban neighborhood. Similarly, the increasing fragility of the electrical grid could be exploited.

While traditional types of cyberattacks, such as data breaches and ransomware attacks, have remained prevalent in recent years, new and more dangerous forms of cyberthreats have emerged. One such threat is "cyber-physical attacks." These attacks can target critical physical infrastructure, such as power grids, water supply systems, and transportation networks, and can have devastating effects on public safety and national security. For

[700] OGUN (39) 113-128.

[701] Weimann (37) 129-1.

example, such an attack on an electrical grid can cause widespread power outages.

Another important type of attack that could pose major threats in the future is "advanced persistent threats" (APTs), which involve long-term, covert cyber espionage operations that infiltrate networks and remain undetected for months or even years. These attacks typically target government agencies, companies, or critical infrastructure.

As artificial intelligence (AI) and machine learning (ML) evolve, their integration into cyberterrorism will become increasingly important. AI could be used to create self-learning malware that helps terrorist groups evade traditional security measures.

In summary, The future of cyber terrorism is directly linked to the extent of rising technology. As technology, artificial intelligence, and machine learning become more complex and widespread, the threat of cyber terrorism will intensify. Therefore, it is clear that cyber terrorism will be one of the most important security problems of the digital age.

CONCLUSION

Cyber attacks have become one of the most critical security threats of our time and are becoming increasingly dangerous. These developments have also added a new dimension to terrorism and have led to the emergence of cyber terrorism. Cyber terrorism has a profound impact on companies, states and the international community. Thus, the increasing prevalence of the threat of cyber terrorism has significantly changed the modern conflict landscape. In other words, with the increasing development of technology, the potential of cyber attacks as a significant tool for terrorism is becoming more of a concern. However, although the question of whether cyber attacks will be the future of terrorism has not yet been clearly answered, it is clear that cyber terrorism will become a reality due to its potential to target critical infrastructure, disrupt economies and endanger national security.

Cyber terrorism is attractive to terrorist groups due to reasons such as anonymity, remote execution, and the secrecy of the perpetrator. It enables terrorists to carry out complex and covert operations. Cyber attacks, in particular, can lead to the collapse of basic services such as power plants, water facilities, health systems, and financial systems. Such attacks can disrupt the economic and social structure of a country and reveal the security weaknesses of the state. In addition, the psychological impact of cyber terrorism can create an environment of fear and uncertainty, undermining

public confidence in the security of digital systems. Although not direct, damage to these critical infrastructures can also lead to injuries and loss of life.

With the development of advanced technologies such as artificial intelligence and machine learning, the future of cyber terrorism is becoming darker. These technologies make attacks more effective and difficult to detect, and require the development of defense strategies and measures. In this context, it is vital for governments, private institutions and the international community to develop robust cyber defense strategies, improve information sharing, and strengthen states' cyber security policies and increase international cooperation. It also requires the creation of a new legal and ethical understanding at national and international levels against cyber terrorism. In addition, more cyber security education and awareness should be created at all levels. Digital networks should be made more proactive in protecting against possible cyber terrorist acts. In order to detect and defend against cyber terrorism threats more quickly, investments should be made in more advanced technologies such as artificial intelligence and machine learning.

In conclusion, although traditional terrorism continues to exist, the rise of cyber attacks is a precursor to a new form of terrorism, cyber terrorism. Therefore, it is vital to take legal and political measures to combat this threat. Although cyber terrorism is seen as a major threat in the future, its impact can be minimized with the right measures.

REFERENCES

Ahmad R and Yunos Z, 'A Dynamic Cyber Terrorism Framework' (2012) 30 *International Journal of Computer Science and Information Security* 149–158.

Ahmed Khan, Dipak, Kannan, Kiran, Kulkarni Madunix, Mohamed Iqbal, Nitai, Sagar and Shrikanth, *Attack Types* https://wentzwu.com/wp-content/uploads/2020/06/All-type-of-attack.pdf accessed 29 April 2025.

Cisco, 'What Is the Difference: Viruses, Worms, Trojans, and Bots?' http://www.cisco.com/c/en/us/about/security-center/virus-differences.html accessed 30 April 2025.

Conway M, 'Cyberterrorism: Hype and Reality' (Dublin City University) 6.

Conway M, 'Reality Bytes: Cyberterrorism and Terrorist "Use" of the Internet' (2002) 7 *First Monday* https://firstmonday.org/article/view/1001/922.

Denning D, 'Cyberterrorism: Testimony'.

Denning D, 'Terror's Web: How the Internet is Transforming Terrorism' in Y Jewkes and M Yar (eds), *Handbook on Internet Crime* (Willan Publishing 2010) 7.

Duygu Öztürk, "Türkiye'de Siber Terörizm ve Hukuki Boyut." Türkiye Adalet Akademisi Dergisi, 2020/4, ss. 233–260.

Embar-Seddon A, 'Cyberterrorism: Are We Under Siege?' (2002) 45 *The American Behavioral Scientist* 1035.

Ergün M. *Bir Siber Suç Olarak Siber Terörizm ve Türkiye.* Yüksek Lisans Tezi, Atatürk Üniversitesi, Kriminalistik Ana Bilim Dalı, 2025.

EU Framework Decision 2002/475/JHA.

Gearty C, *Terror* (Faber & Faber 1998).

Gillespie A, *Cybercrime: Key Issues and Debates* (Routledge 2016).

Guelke A, *The Age of Terrorism and the International Political System* (IB Tauris 1998).

Heickerö R, 'Cyberterrorism: Electronic Jihad' (2014) 38 *Strategic Analysis* 555.

Hoffman B, *Inside Terrorism* (Indigo 1998).

Hua J and Bapna S, 'The Economic Impact of Cyber Terrorism' (2013) 22 *The Journal of Strategic Information Systems* 175–186 https://doi.org/10.1016/j.jsis.2012.10.004.

Hua J and Bapna S, 'How Can We Deter Cyber Terrorism?' (2012) 21 *Information Security Journal: A Global Perspective* 104.

International Conference on Natural Sciences and Technologies, *Terrorist Use of Cyber Technology* (Iconat Special Issue 2021) 9: 113–128 https://doi.org/10.20290/estubtdb.1021324.

Iftikhar S, 'Cyberterrorism as a Global Threat: A Review on Repercussions and Countermeasures' (2024) 10 *PeerJ Comput. Sci.* e1772 http://doi.org/10.7717/peerj-cs.1772 accessed 23 June 2025.

Jones A, 'Cyber Terrorism: Fact or Fiction' (2005) 6 *Computer Fraud and Security* 4–7.

Merlos García A, 'Internet como instrumento para la yihad' (2006) 8 *Araucaria* 80–99.

Metin Gürcan & M. Erdoğan, "Siber Terörizm ve Kritik Altyapılar." Güvenlik Bilimleri Dergisi, Cilt 7, Sayı 2 (2018): ss. 65–90.

OGUN MN and Kaya A, 'Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler' (2013) 9(18) *Güvenlik Stratejileri Dergisi* 145–181.

OGUN MN, YURTSEVER S, ASLAN M and ELBURASI M, 'Terrorist Use of Cyber Technology' (2021) 9 *International Conference on Natural Sciences and Technologies*, 113–128 https://doi.org/10.20290/estubtdb.1021324.

Oğün, S. & Kaya, Ö., "Siber Güvenliğin Milli Güvenlik Açısından Önemi." Uluslararası Güvenlik ve Terörizm Dergisi, Cilt 4, Sayı 1 (2013): ss. 27–45.

Özdemir B. "Türkiye'nin Siber Güvenlik Stratejileri." *Journal of National Defense* 12, no. 3 (2020): 100–115.

Pollitt M, 'Cyberterrorism: Fact or Fancy?' 9.

Post JM, Ruby KG and Shaw ED, 'From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism' (2000) 12 *Terrorism and Political Violence* 101.

Proofpoint, 'What Is a Cyber-Attack?' https://www.proofpoint.com/au/threat-reference/cyber-attack accessed 28 April 2025.

Sánchez Medero G, 'Ciberespacio y el crimen organizado. Los nuevos desafíos del siglo XXI' (2012) 10(16) *Facultad de Ciencias Políticas y Sociología Universidad Complutense de Madrid* 71–87.

Seissa IG, 'Cyber-terrorism Definition Patterns and Mitigation Strategies: A Literature Review' (2017) 6(1) *International Journal of Science and Research (IJSR)* 180–186.

Terrorism C o. (ed), *Responses to Cyber Terrorism* (1st edn, vol 34, IOS Press 2008).

UN Security Council Resolutions 1373, 1566.

Yurtsever B. *Küreselleşen Dünyada Terörizm: Siber Terörizm Örneği*. Yüksek Lisans Tezi, Niğde Ömer Halisdemir Üniversitesi, Kasım 2020, s. 82.

Wardlaw G, *Political Terrorism: Theory, Tactics, and Countermeasures* (Cambridge University Press 1982).

Weimann G, 'Cyberterrorism: The Sum of All Fears' (2005) 28(2) *Studies in Conflict and Terrorism* 129–149 https://doi.org/10.1080/10576100590905110.

Weimann G, 'How Modern Terrorism Uses the Internet' (2004) http://ics.leeds.ac.uk/papers/vp01.cfm?outfit=pmt&requesttimeout=500&folder=1259&paper=1542.

Whiting A, Macdonald S and Jarvis L, *Cyberterrorism: Understandings, Debates and Representations*.