ATATÜRK ÜNİVERSİTESİ YAYINLARI
ATATURK UNIVERSITY PUBLICATIONS

Research Article *Araştırma Makalesi* DOI: 10.62425/jirs.1589559

Evolution of Cyberterrorism: Challenges and Solutions

Siber Terörizmin Evrimi: Tehditler ve Çözüm Önerileri

Mücahit ERGÜN
Ataturk University,
Natural Sciences Institute,
Department of Criminalistics,
Erzurum, Türkiye

Gülşen ŞEKER AYDIN
Ataturk University,
Faculty of Economics and
Administrative Sciences,
Department of International Relations,
Erzurum, Türkiye

ABSTRACT

Cyberterrorism is an important international relations issue as it poses formidable challenges to international security due to its unanimity and easier reach to broad masses. Fighting cyberterrorism necessitates understanding what kinds of actors resort to it, what motivates them, what are their intentions and targets, what kind of means they employ, and what kind of effects their actions cause. This study aims to address the actors, targets, motives, intentions, means, and effects of cyberterrorism and how they have evolved to contribute to providing effective counter-measures and safeguards. To this end, after the introduction, the study first provides a conceptual framework to assess the evolution of cyberterrorism by focusing on its key attributes. Second, it explores the evolution of actors in cyberterrorism. Third, the study focuses on the evolution of motives and intentions in cyberterrorism. Fourth, it examines the evolution of targets, means, and effects in cyberterrorism. The conclusion highlights the transnational nature of cyberterrorism, calls for reciprocating to it in kind and offers solutions.

Keywords: Cyberterrorism, Actors, Motives, Intentions, Targets, Methods, Effects, International Security

ÖZ

Siber terörizm önemli bir uluslararası ilişkiler meselesidir. Teknolojinin teröristlerin kolay bir şekilde çok geniş kitlelere ulaşmalarını sağlaması ve teröristlere kimliklerini saklama imkânı sunması nedeniyle siber terörizm, önemli ve baş edilmesi güç bir uluslararası güvenlik tehdidi haline gelmiştir. Siber terörizmle etkili şekilde mücadele edebilmek için hangi tür aktörlerin buna başvurduğunu, onları neyin motive ettiğini, niyetlerinin ve hedeflerinin ne olduğunu, hangi araçları kullandıklarını ve eylemlerinin ne tür etkiler yarattığını kavramak gerekmektedir. Bu çalışma, siber terörizmin aktörlerini, hedeflerini, güdülerini, niyetlerini, araçlarını ve etkilerini ele almakta ve bunların etkili karşı önlemler ve güvenlik önlemleri sağlamak için nasıl evrildiğini göstermeyi amaçlamaktadır. Bu amaçla, giriş bölümünden sonra, çalışma ilk olarak siber terörizmin evrimini değerlendirmek için temel özelliklerine odaklanan kavramsal bir çerçeve sunmaktadır. İkinci olarak, siber terörizmdeki aktörlerin evrimini değerlendirmektedir. Üçüncü olarak, çalışma siber terörizmin güdüleri ve niyetlerinin evrimine odaklanmaktadır. Dördüncü olarak, siber terörizmin hedeflerinin, araçlarının ve etkilerinin evrimini incelemektedir. Sonuç bölümünde, siber terörizmin ulus ötesi doğasına dikkat çekilmekte, bu tehdide doğasına uygun olarak cevap verilmesi gerektiğinin altı çizilmekte ve önerilerde bulunulmaktadır.

Anahtar Kelimeler: Siber Terörizm, Aktörler, Güdüler, Niyetler, Hedefler, Metotlar, Etkiler, Uluslararası Güvenlik

This study is produced from Mücahit Ergün's master thesis, which he has been writing at the Natural Sciences Institute and Criminalistics Department of Ataturk University. An early version of this article was presented at Social Science Research Conference, which was held in 2024 in Durres, Albania.

Geliş Tarihi/Received 22.11.2024
Kabul Tarihi/Accepted 23.12.2024
Yayın Tarihi/Publication Date 30.12.2024

Corresponding Author/Sorumlu Yazar:
Mücahit ERGÜN
E-mail:: ergunmu2024@gmail.com

Cite this article:
Ergün, M. & Şeker Aydın, G. (2024). Evolution of Cyberterrorism: Challenges and Solutions. *Journal of International Relations Studies, 4*(2), 64-73.

Introduction

The Internet has dramatically transformed communication since its inception in the late 1980s. Technology has enabled communication with comparatively low entrance barriers and a global scope. Thanks to the Internet, people can easily and swiftly connect with an almost unlimited audience across boundaries while maintaining their anonymity to an important extent.

While technology's positive impact on communication is evident, the picture regarding security is more or less blurred. Technology both improved and undermined security. In the positive sense, technology provided new and improved means to detect, mitigate, block, and deter security threats. In the negative sense, new and more sophisticated kinds of security threats that abuse the conducive conditions enabled by technology emerged.

Cyberterrorism clearly illustrates the new and sophisticated threats that technology has been introducing. It is known as the illicit use of the Internet, information channels, and social media to carry out terrorist acts or further terrorist objectives. These acts can take many forms, including distributing false information, stealing or altering data, or interfering with vital infrastructure to cause disruption and harm (Iftikhar, 2024). The unprecedented pace of technological advances has led to the emergence of cyberspace as a new field for criminal activities, including cyberterrorism, which presents a new mode of terrorism. It has become a significant problem due to its negative impact on security at the individual, national, and global levels.

As cyberterrorism undermines international security and international cooperation is essential for fighting it, it has grown in importance in international relations. One needs to have a clear grasp of this new kind of terrorism to have a comprehensive command of the international security environment. While terrorists increasingly find it instrumental in terrorizing the masses, both states and international organizations incorporate the efforts to rein in cyberterrorism in their security agendas. The motivations behind this new face of terrorism are as evil as before, and the means that cyberterrorism uses are unfamiliar. Combining technology with terrorism renders cyberterrorism more complicated compared to the traditional forms of terrorism. Besides providing unanimity, technology enables a cheaper, easier, faster, and broader reach for cyber-attacks.

To make matters worse, rapid technological developments increasingly empower and complicate cyberterrorism. Since cyber threats have become more complicated and wide-ranging, the field of international relations must adapt to address these challenges effectively. Understanding the evolution of cyberterrorism is at the core of gaining such an understanding. It offers insights into the transforming attributes of cyber threats, informs policy formulation, and supports international cooperation. Therefore, policymakers, security staff, and academics must pay close and constant attention to this significant evolution to effectively fight against cyberterrorism and counteract future threats. International relations scholars and practitioners increasingly need to analyze the geopolitical implications of cyber threats, assess the effectiveness of international norms and agreements, and shed light on the dynamics of cyber diplomacy. By integrating cybersecurity into the study of international relations, academics can provide valuable insights into managing the complex landscape of cyberspace and overcoming problems.

In light of the discussion above, this study addresses the evolution of cyberterrorism. As the methodology, it employs content analysis to examine secondary resources on the evolution of cyberterrorism. The study analyzes secondary resources, including news, newspaper articles, academic articles, reports, and case studies, to identify key themes and trends in the evolution of cyberterrorism. While it generally utilizes qualitative analysis to draw meaningful insights from the data, quantitative analysis is also used to measure the severity and impact of cyberterrorism incidents over time. This eclectic approach ensures a comprehensive and thorough understanding of the evolution of cyberterrorism. The study aims to shed light on the evolution of cyberterrorism to guide the efforts to counteract it. To this end, after the introduction, the study first provides a conceptual framework to assess the evolution of cyberterrorism by focusing on its key attributes. Second, it explores the evolution of actors in cyberterrorism. Third, the study focuses on the evolution of motives and intentions in cyberterrorism. Fourth, it examines the evolution of targets, means, and effects in cyberterrorism. The conclusion highlights the transnational nature of cyberterrorism and calls for reacting to it in kind by going beyond the traditional approach to security.

Conceptualizing Cyberterrorism

The concept of cyberterrorism was introduced in the 1980s by Barry Collin, who drew attention to how this kind of terrorism converges the real and virtual worlds (Tafoya, 2011, p. 2). In his seminal study, Collin gives examples of impending cyberterrorist activity to explain this evil convergence. As he argues, cyberterrorists can remotely modify pharmaceutical formulations or deploy numerous digital explosives throughout a metropolis to cause fatalities. They can also remotely interfere with banks, international financial transactions, and stock exchanges. The primary goal is to cause the public to lose trust in the nation's economic structure. The cyber terrorists may remotely alter the pressure in the gas lines to cause valve failures or explosions. By remotely attacking the aircraft's in-cockpit sensors, the terrorists can cause airplane accidents. Trains can also be targets of similar cyber terrorist activity to kill and injure people (Collin, n.d.). As the examination of the following sections reveals, nowadays, cyber terrorism seems to realize almost all the potential examples Collin offered.

At Collin's time of writing, social media did not exist. However, today, terrorists also rely on social media platforms to propagate and wage psychological warfare by inciting public fear, panic, and disinformation (Vilić, 2017, p. 7). For instance, as discussed in more detail below, ISIS has relied on platforms like Twitter and Telegram to appeal to a global audience, instigate lone-wolf attacks, and spread propaganda. The ability to disseminate content directly over the Internet reduces the need for more conventional communication channels, such as news services, which may independently assess the authenticity of the information delivered or get rid of or edit any excessively provocative item (United Nations Office on Drugs and Crime, 2012).

It was in the mid-1990s that the national governments started to pay systematic attention to cyberterrorism. The report titled "Cybercrime, Cyberterrorism, and Cyberwarfare: Averting an Electronic Waterloo" was the first scholarly focus on the issue. It was released in 1998 by the Center for Strategic and International Studies Global Organized Crime Project. The report defined cyberterrorism as a category of information warfare. Since then, cyberterrorism has been seen as an element of offensive information warfare that directly correlates with traditional, physical, non-technology-based classical political terrorism. To put it another way, cyberterrorism has connections to conventional terrorism, but it is a novel approach that utilizes new resources and takes advantage of new vulnerabilities (Conway, 2007, p. 1).

Although there is not a single, generally accepted definition of cyberterrorism, almost all definitions focus on some common elements, including hacking or stealing data, organizing terrorist assaults, inciting violence, and attacks on computer networks and information systems. One critical element that needs to be emphasized is the politically driven use of computers as weapons or as targets by covert actors to cause violence, terrorize the public, or compel a government to reconsider its policies, as Wilson notes (2005, pp. 5-7).

While these elements clarify the concept to some extent, there is still the need for a systematic conceptualization of cyberterrorism. The literature review indicates that two studies offer such a conceptualization by focusing on critical features of cyberterrorism. These studies are Al Mazari et al. (2018) and Plotnek and Slay (2021). The conceptualization of Al Mazari et al. (2018) focuses on five key components: target (military forces, government cyber and physical infrastructures, critical national infrastructures, social and national identity, and private industry or entities), motive (economic, social, cultural, religious, political, ideological), intention (gain political, social, military or ideological advantages), means (computer and communication technologies and networks), and effect (violence, destruction and disruption of services, physical, operational and informational damages, and harm individuals and groups). Plotnek and Slay (2021) add the actor as another component to the five-dimensional taxonomy of Al Mazari et al. (2018). Thus, Plotnek and Slay (2021) define cyberterrorism by focusing on actors, motives, intentions, targets, means, and effects.

Following Plotnek and Slay (2021), this study defines cyberterrorism as a deliberate attack or the threat of such an attack by non-state actors to utilize cyberspace to cause physical, emotional, political, economic, ecological, or other harm. Cybercriminals seek to instill fear or intimidate government or nongovernmental organizations into acting in ways that further their social, economic, or ideological goals. Although cyberterrorism and cyberwarfare use similar strategies, it is necessary to distinguish between them. While non-state actors are responsible for cyberterrorism, states' military forces conduct cyber warfare within the framework of a declared conflict (Denning, 2000). There are cases in which state actors support cyber-terrorist non-state actors. As long as the main instigators are non-state actors, this study will regard these cases as cyberterrorism.

In light of this conceptualization, the study explores the evolution of cyberterrorism in the following sections by meticulously examining actors, motives, intentions, targets, means, and effects.

The Evolution of Actors in Cyberterrorism

The section examines how the actors of cyberterrorism evolved in parallel to technological developments and changing geopolitical circumstances.

Individual hackers and small groups with limited abilities and financial means proved to be the main actors in the initial stages of cyberterrorism. The first cyberterrorists generally acted independently and were driven by personal resentments or ideology. The actors in the following three examples of cyberterrorism meet these criteria. First, a computer hacker connected to the White Supremacist Movement attacked an internet service provider (ISP) in Massachusetts in 1996. The attack heavily damaged the ISP and a portion of its record-keeping system. The ISP had tried to prevent the hacker from using its identity to distribute racist remarks throughout the world. Before signing off, the hacker stated that the world has yet to understand cyberterrorism's real nature. Second, for two weeks in 1998, ethnic Tamil insurgents bombarded Sri Lankan embassies with 800 e-mails every day to disrupt the embassies' communications. Third, individual hacktivists opposing the NATO bombardment launched denial-of-service attacks and e-mail bombs against NATO computers during the 1999 Kosovo war. Some Eastern European nationals also sent political and virus-laden e-mails to corporations, government agencies, and academic institutions. Defacements of websites were also frequent (Denning, 2000).

Hacktivists, people or organizations that employ hacking to further their social or political goals, became prominent cyberterrorism actors as technology developed. These groups generally possessed more advanced equipment and more substantial financial resources. GlobalHell is recognized as one of the first hacker groups to become well-known for website attacks and defacements. The gang stole financial and personal data and caused a $2.5 million loss. Ameritech, the U.S. Army, the U.S. Postal Service, and the White House were all compromised by GlobalHell (Cyber Policy, n.d.). Another group that falls under this scope is Anonymous, which became well-known for its cyberattacks on targets that are thought to be hostile to Internet freedom (Coleman, 2014). Their attacks on the Central Intelligence Agency, the Sun newspaper, the Church of Scientology, and numerous other big corporations led to a worldwide police crackdown. Following Anonymous' lead, LulzSec caused havoc on the Internet during the Wikileaks scandal in 2011. After the American Public Broadcasting Service aired a critical program about Julian Assange, LulzSec penetrated its website and posted fake news on its homepage. Their illegal actions included hacking the Central Intelligence Agency's (CIA) website and Sony's database to release more than a million user names and passwords (Cadwalladr, 2012). The group was also involved in Operation Anti-security in 2012 by mobilizing its supporters to hack and leak banking and governmental data. Although LulzSec was presented to the public as a "revolution" aimed at exposing bribery and fraud, in reality, the group's attacks resulted in financial losses and personal repercussions for the victims (Gregory, 2022). As Olson (2012) argued, their acts created much disturbance and amounted to cyberterrorism.

Terrorist organizations soon adopted cyberterrorism as a tool to achieve their goals. They used the Internet for propaganda, financing, training, planning, communication, and execution (United Nations Office on Drugs and Crime, 2012). Daesh’s or Islamic State of Iraq and ash-Sham’s (ISIS) use of social media platforms, especially Twitter, to recruit supporters and disseminate its ideology is one of the best examples of terrorists' abuse of cyberspace. Utilizing its practical cyber abilities, ISIS has managed to inspire lone-wolf attacks and appeal to a worldwide audience (Berger & Morgan, 2015). The capacity to disseminate content directly over the Internet reduces the need for more conventional communication channels, such as news services, which may independently assess the authenticity of the information offered or remove or censor any excessively provocative content (United Nations Office on Drugs and Crime, 2012). Terrorist organizations also made use of digital means to finance their activities. For instance, Al-Qaeda received cryptocurrency donations from people worldwide, illustrating how the digital age benefited terrorist groups (U.S. Department of Justice, 2020). Terrorist groups often use the Internet for training purposes. The Internet is instrumental in disseminating online audio and video content, online manuals, and information and guidance in different languages. This includes instructions on using weapons and producing explosives (Öğün et al., 2021).

While ISIS expanded its cyber-terrorist activities significantly to the extent that terrorists came to call themselves the Islamic State Electronic Army (Greenberg, 2016), The Global Coalition Against Daesh was involved in an active counter-campaign. The Coalition has sought to impede Daesh's online operations. It aims to challenge the information environment in which Daesh functions and make sure that the group's defeat in cyberspace accompanies its loss of controlled territory. As a result of the Coalition's efforts, Daesh produced 85% less propaganda in October 2017 than it did in August 2015. Additionally, the Coalition is collaborating with the IT sector to curb the internet dissemination of Daesh propaganda. It backs the industry-led Global Internet Forum to Counter Terrorism, which seeks to exchange knowledge on eliminating extremist and terrorist

information from online platforms. In order to increase the scope and influence of the global community's initiatives, the Coalition's Communications Working Group coordinates the communication efforts of Coalition members, boosts international cooperation to weaken Daesh propaganda, and strengthens the resilience of susceptible masses (Global Coalition, 2017). As ISIS has raised money through a variety of internet channels, including bitcoin exchanges, crowdfunding websites, and social media, the Coalition has acted to locate and close these sources of funding. The Coalition has been able to trace and block accounts linked to ISIS fundraising operations by cooperating with financial institutions and social media businesses. The U.S. Department of Justice has filed lawsuits against people and organizations that supplied cryptocurrency to ISIS (Global Coalition, 2019).

The UN has established counter-terrorism mechanisms for research, capacity building, and coordination. It provides guidelines for member countries to anticipate and combat cyberterrorism (Schindler, 2020).

The Evolution of Motives and Intentions in Cyberterrorism

This section questions whether the motives and intentions of cyberterrorism have evolved since the first cyberterrorist attacks. As motives and intentions are connected, the section examines them together.

To start with motives, a preplanned cyberattack has to be motivated by ideological, political, religious, racial, social, and economic drivers to be considered an act of cyberterrorism. While ideological and political motives are considered to be the main drivers from the start, economic motives have recently come to be regarded as relevant (Plotnek & Slay, 2021).

The examination of cyber terrorist attacks so far reveals such an evolution. Ideological, political, and racial reasons have motivated cyber terrorists from the start. As discussed above, racism was the primary motivation behind the attack against the ISP in Massachusetts in 1996. Similarly, in cyberterrorist attacks against the Estonian government in 2007, the motivating reasons were political, and these reasons effectively illustrated why cyberterrorism is a critical issue in international relations and security. The attacks took place against the backdrop of long-term tension between Estonians and the Russian minority of the country. Hundreds of thousands of ethnic Russians were sent to Estonia by the Kremlin after the Soviet Union annexed the Baltic States in 1940. This large-scale immigration aimed at Russifying and controlling Estonia. After the fall of the Union of Soviet Socialist Republics (USSR), the Estonian government implemented policies to lessen Russian leverage on the country. These included the relocation of a monument honoring the Soviet Union's liberation of the nation from the Nazis to a less noticeable spot in Tallinn in April 2007. This relocation led to rioting among the Russian minority and parallel cyberterrorist attacks targeting Estonia's vital political and economic structure (Herzog, 2011). The servers of state institutions, political parties, and major newspapers came under denial-of-service attacks between 25 April and 4 May 2007. Media could not convey the news; government workers could not e-mail one another; and machines for cash and online banking services were intermittently unavailable. While some members of the Estonian government demanded invoking Article 5 of the North Atlantic Treaty Organization during the cyberattack, which stipulates that an attack on one ally nation requires the alliance to fight the aggressor in unity, this demand was not met as there was no loss of life (McGuinness, 2017).

Even though Dmitri Galushkevich, an Estonian student of Russian descent, was found guilty of the attack, its scope suggested that other individuals were probably involved in it. The incident caused the citizens, business people, and investors to lose confidence in the Estonian state. However, in the medium and long term, the defense capacity of Estonia, as well as the other Baltic states and NATO, improved. Formulating a national cyber security strategy by the Estonian Ministry of Defense and establishing the NATO Co-operative Cyber Defense Centre of Excellence in Tallinn, Estonia's capital, in 2008 are essential steps in this respect (Aday et al., 2019). Despite being one of the smallest NATO members, Estonia is among the world's most highly wired nations. From banking to schooling, media access, and casting ballots in municipal elections, practically everything is carried out online. Due to this reliance, Estonian society is highly susceptible to cyberattacks that might block its daily operations. Since the 2007 attacks were not very sophisticated and Estonia is a small country, its cyber professionals were able to install countermeasures quickly. As a result, the country's IT infrastructure was not severely damaged. Still, the strikes served as a real wake-up call for NATO, providing a real-world example of how cyberattacks may devastate a country that depends on IT networks so heavily. Such a scenario poses a new challenge to NATO member nations and the reliability and effective operation of the information networks that are essential to the Organization's primary missions of crisis management and collective defense (Joubert, 2012).

The cyber-attack against the Colonial Pipeline in 2021 exemplifies the evolution of cyberterrorism motives to include economic drivers. This was a ransomware attack, and DarkSide received a Bitcoin payment of $5 million to end the disruption of gasoline supplies to the East Coast of the United States. The attack caused panic, and people rushed to buy gas (Eliaçık,

2022).

Before closing this section, it is necessary to examine the evolution of a related attribute of cyberterrorism: intentions. The conceptual framework of Plotnek and Slay (2021) envisages that cyberterrorism intends to gain political, social, military, or ideological advantages. The examination of the cases of cyberterrorism from the start reveals that there is no crucial evolution of intents. The intention of gaining political, ideological, and social advantages is usually evident. As discussed above, gaining political advantages over the Estonian government was the main intention of the 2007 cyber-attacks against Estonia. In this case and other cases of cyberterrorism, the intention to create chaos and undermine society's confidence in the state has political connotations. The 2017 WannaCry ransomware attack also had political and social intentions, in the sense that it attempted to weaken society's trust in the UK's National Health Service (NHS) (Greenberg, 2018). The intention to gain military advantage is more difficult to identify than other intentions. Still, ISIS's use of social media to recruit people is an example of terrorist attempts to gain military advantage (Schindler, 2020).

The Evolution of Targets, Means and Effects in Cyberterrorism

This section examines the evolution of cyberterrorism's targets, means, and effects. As the discussion further clarifies, these three attributes of cyberterrorism are closely related, so they are analyzed together.

To start with the evolution of targets, this attribute of cyberterrorism covers military forces, government cyber and physical infrastructures, critical national infrastructures, social and national identity, and private industry or entities (Al Mazari et al., 2018). While it is possible to identify cyber terrorist attacks targeting the government's cyber and physical infrastructures, social and national identity, and private industry or entities, state actors seem to be behind the attacks in cases where military capabilities are attacked. The Moonlight Maze and Stuxnet attacks exemplify this phenomenon. In 1998, the Pentagon, NASA, research labs, and universities became the target of the Moonlight Maze cyber espionage attack. The attackers obtained and took significant private data about military systems, setups, and installations. In the 2010 Stuxnet case, the computer attacks compromised Iran's uranium enrichment activities and destroyed its centrifuges. Experts concluded that only nation-states could design and carry out such attacks, even though the suspicions have never been verified in these instances (Haizler, 2017). Therefore, it is necessary to consider Moonlight Maze and Stuxnet attacks as cases of cyber warfare rather than cyberterrorism examples.

Notwithstanding these examples of state involvement in cyberattacks, when technological developments have enabled non-state actors to carry out cyber-terrorist attacks, they have targeted governments' cyber and physical infrastructures. These attacks have had significant implications for national security and public safety. As seen in the previous section, 2007 cyber-attacks on Estonian government bodies highlighted the vulnerability of critical national infrastructures to cyber threats and underscored the need for robust cybersecurity measures. Similarly, the 2015 cyberattack on the U.S. Office of Personnel Management (OPM) demonstrated the potential for cyberterrorism to compromise sensitive information and disrupt government operations. In this attack, hackers gained access to the personal information of millions of federal employees, including social security numbers, fingerprints, and background investigation records (Fruhlinger, 2020). In recent years, attacks targeting civilians have become increasingly prevalent. The WannaCry ransomware attack in 2017 is a notable example. This attack targeted hospitals and ambulance services in England, causing significant disruption to healthcare services. The ransomware encrypted data on infected computers, rendering them unusable until a ransom was paid. The attack led to the cancellation of medical appointments, surgery delays, and a general strain on healthcare resources. It highlighted the potential for cyberterrorism to cause physical harm and endanger public health (Ghafur et al., 2019).

As technology continues to evolve, cyberterrorism targets are likely to become even more diverse and sophisticated. The increasing reliance on digital infrastructure and the rise of the Internet of Things (IoT) present new opportunities for cyber terrorists. Smart cities, autonomous vehicles, and personal devices may become future targets.

As for the means that cyberterrorism has been utilizing, the evolution is quite clear. Initially, cyberterrorists disrupted networks and gained illegal access using simple tools like viruses and worms (Maryville University, 2022). Over time, cyber terrorists started using more advanced forms of malware, such as ransomware and spyware (Montasari, 2024). Moreover, sophisticated means, including phishing campaigns, social engineering, Distributed Denial of Service (DDoS) attacks, deployment of botnets, and Artificial Intelligence, have come to be employed (Montasari, 2024). As a result, the harm that the cyber terrorism increased over time, as the rest of this session argues.

Moving on to how the effects of cyberterrorism evolved, it can be argued that the effect of causing fear and disruption has existed from the beginning. As discussed above, the hacker connected to the White Supremacist Movement disrupting the (ISP) in Massachusetts in 1996 warned about the future potential of cyberterrorism to cause harm. As illustrated by ISIS' use of videos releasing the "kill lists" (Jayakumar, 2020) or showing how people were burnt alive (Ayad & Zerrouky, 2023), instilling fear has remained a consistent theme. So has the disruption. The Serbian hackers' main intention was to disrupt the NATO bombardment of the Federal Republic of Yugoslavia in the Kosovo War (Verton, 1999). As the e-mail bombardment on NATO, the Associated Press and the Washington Post also aimed at forcing NATO to end the bombardment (Denning, 2001); this attack also signified an evolution of cyberterrorism intentions to include forcing policy changes. Diversification of cyberterrorist intentions gained momentum in parallel to technological developments. Social media has provided an invaluable tool for another cyberterrorist intention: furthering the objectives. ISIS' utilization of social media for propaganda and recruitment is a case point (Awan, 2017). Interference is another type of cyberterrorist effect that has grown in significance with technological advances. An incident in 2021 demonstrates how evil this intention may be. In this case, a hacker attempted to poison Florida's water supply by using remote access software. The amount of sodium hydroxide was increased by the hacker-terrorist almost 100 times. While the system operator swiftly lowered the level after noticing the penetration, the incident indicates how some critical infrastructure systems are susceptible to interference (Marquardt,2021).

As technology continues to evolve, the effects of cyberterrorism are likely to become even more severe. The increasing reliance on digital infrastructure and the rise of the Internet of Things (IoT) offer new opportunities for cyber terrorists. Future attacks may target smart cities, autonomous vehicles, and personal devices, causing widespread disruption and fear.

Conclusion

Cyberterrorism poses formidable challenges to international security due to its unanimity and easier reach to broad masses. Fighting cyberterrorism necessitates understanding what kinds of actors resort to it, what motivates them, what their intentions and targets are, what kind of means they employ, and what kind of effects their actions cause. This study has addressed the actors, targets, motives, intentions, means, and effects of cyberterrorism and how they have evolved to contribute to providing effective countermeasures and safeguards.

The analysis of the evolution of cyberterrorism has painted a grim picture. Technological advances have boded ill for individual, national, and international security. As technology has developed, cyber terrorists have seen their means to diversify and sophisticate, their targets to be more vulnerable, their reach to broaden, and the impact of their actions to deteriorate for the victims. While their intentions are as evil as before, they are now more potent due to technology.

This evolution is also at odds with the traditional international relations and security approach. The traditional approach applies to the Cold War period. In this approach, nation-states are thought to be the main actors and threatened by other nation-states. Moreover, they are envisaged to have conflicting interests. The post-Cold War international security makeup is quite different than the Cold War security structure. As these new conditions of the post-Cold War environment are reflected in cyberterrorism, the traditional understanding of international security remains short of understanding and counteracting it effectively. In this formidable kind of terrorism, the main actors are non-state. As cyberterrorism is truly transnational, state actors must react in kind. States need to educate the public about cyberterrorism and raise awareness. They also need to focus on educating more experts in this field. States also must cooperate with universities and research centers to formulate effective countermeasures. Keeping up with technological developments is vital. Academic institutions are crucial in promoting cybersecurity research, developing new technologies, and training the next generation of cybersecurity experts. Joint research projects can lay the ground for innovative solutions and strategies to fight cyberterrorism. As this research has shown, private entities (critical infrastructures, banks, and newspapers) are common targets of cyberterrorism. Therefore, states need to cooperate with non-state actors to identify threats, share intelligence, and formulate effective strategies. Public-private partnerships can enhance the overall cybersecurity structure by creating synergy and boosting the expertise and resources of both sectors.

Having highlighted the need to take the non-state dimension of cyberterrorism into account, it is also necessary to underline that international cooperation is indispensable for effectively fighting cyberterrorism. States need to share intelligence, formulate common policies, and intensify cross-border cooperation. International organizations, including NATO and the UN, are critical in increasing and coordinating international cooperation. For instance, the establishment of the NATO Cooperative Cyber Defense Centre of Excellence in Estonia, which has been discussed in this study, has proved to be a crucial step. While

the UN has turned out to be paralyzed in interstate conflicts where a veto-holding power is involved, including the Russian-Ukrainian and Israeli-Palestinian conflict, it proves to be more effective in attacks orchestrated by non-state actors. The study also has driven attention to the curtailment of ISIS-related cyber-terrorist activities as a result of the counter-campaign of Global Coalition, an interstate coalition.

Cyberterrorism is a highly fertile ground for research, and the study ends by offering new venues for future research. One such venue is examining whether and how states and international organizations' fight against cyberterrorism evolved parallel to the evolution of different attributes of cyberterrorism. As another venue, future studies can assess the effectiveness of national cybersecurity strategies in preventing and responding to cyberterrorism and identify best practices and areas for improvement. Related to effectiveness, new research can also compare and contrast the anti-cyberterrorism strategies of international organizations.

***Yazar Katkıları**: Fikir- M.E.-G.Ş.A.; Tasarım- M.E.- G.Ş.A.; Denetleme- G.Ş.A.; Kaynaklar- M.E.- G.Ş.A.; Veri Toplanması ve/veya İşlemesi-M.E.- G.Ş.A.; Analiz ve/ veya Yorum- M.E.; Literatür Taraması- M.E.; Yazıyı Yazan- M.E.- G.Ş.A.; Eleştirel İnceleme- G.Ş.A.*
***Hakem Değerlendirmesi:** Dış bağımsız.*
***Çıkar Çatışması:** Yazarlar, çıkar çatışması olmadığını beyan etmiştir.*
***Finansal Destek:** Yazarlar, bu çalışma için finansal destek almadığını beyan etmiştir.*

***Author Contributions:** Concept -M.E.; Design- M.E.; Supervision- G.Ş.A.; Resources- M.E.- G.Ş.A.; Data Collection and/or Processing- M.E.- G.Ş.A.; Analysis and/or Interpretation- M.E.; Literature Search- M.E.; Writing Manuscript- M.E.- G.Ş.A.; Critical Review- G.Ş.A.; Other- G.Ş.A.*
***Peer-review:** Externally peer-reviewed.*
***Conflict of Interest:** The authors have no conflicts of interest to declare.*
***Financial Disclosure:** The authors declared that this study has received no financial support.*

References

Aday, S., Andžāns, M., Bērziņa-Čerenkova, U., Granelli, F., Gravelines, J., Hills, M., Holmstrom, M., Klus, A., Martinez-Sanchez, I., Mattiisen, M., Molder, H., Morakabati, Y., Pamment, J., Sari, A., Sazonov, V., Simons, G., & Terra, J. (2019). *Hybrid threats: A strategic communications perspective*. NATO Strategic Communications Centre of Excellence.

Awan, I. (2017). Cyber-extremism: ISIS and the power of social media. *Society*, 54(2), 138-149. https://doi.org/10.1007/s12115-017-0106-6

Ayad, C., & Zerrouky, M. (2023, March 20). Jordanian pilot burned alive by IS in 2015: The story of a failed release. *Le Monde*. https://www.lemonde.fr/en/international/article/2023/03/20/jordanian-pilot-burned-alive-by-is-in-2015-the-story-of-a-failed-release_6027456_4.html

Al Mazari, A., Anjariny, A. H., Habib, S. A., & Nyakwende, E. (2018). Cyber terrorism taxonomies: Definition, targets, patterns, risk factors, and mitigation strategies. In K. Al-Begain, M. Zak, W. Alosaimi, & C. Turyagyenda (Eds.), *Cyber security and threats: Concepts, methodologies, tools, and applications* (pp. 608-621). IGI Global.

Berger, J. M., & Morgan, J. (2015). *The ISIS Twitter census: Defining and describing the population of ISIS supporters on Twitter* (The Brookings Project on U.S. Relations with the Islamic World Analysis Paper, No. 20). Center for Middle East Policy at Brookings.

Cadwalladr, C. (2012, September 8). Anonymous: Behind the masks of the cyber insurgents. *The Guardian*. https://www.theguardian.com/technology/2012/sep/08/anonymous-behind-masks-cyber-insurgents

Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. Verso Books.

Collin, C. B. (n.d.). The future of cyber terrorism: Where the physical and virtual worlds converge. *11th Annual International Symposium on Criminal Justice Issues*. http://www.crime-research.org/library/Cyberter.htm

Conway, M. (2007). *Cyberterrorism: Hype and reality*. Potomac Books, Inc.

Cyber Policy. (n.d.). 5 Cybercrime groups making organizations uneasy. https://www.cyberpolicy.com/cybersecurityeducation/5-cybercrime-groups-making-organizations-uneasy

Denning, D. E. (2000, May 23). *Cyberterrorism*. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives. https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. In J. Arquilla & D. Ronfeldt (Eds.), *Networks and netwars: The future of terror, crime, and militancy* (pp. 239-288). RAND Corporation. http://www.jstor.org/stable/10.7249/mr1382osd.13

Eliaçık, E. (2022, June 17). What is considered cyberterrorism and why does it matter today? *Dataconomy*. https://dataconomy.com/2022/06/17/what-is-cyberterrorism/

Fruhlinger, J. (2020, February 12). The OPM hack explained: Bad security practices meet China's Captain America. *CSO Online*. https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *NPJ Digital Medicine*, 2(1), 98. https://doi.org/10.1038/s41746-019-0098-4

Global Coalition. (2017). Countering Daesh's propaganda. https://theglobalcoalition.org/en/mission/countering-daeshs-propaganda/

Global Coalition Against Daesh. (2019). Dismantling Daesh's illicit financial flows: Tightening the global financial system to stop terror funding. https://theglobalcoalition.org/en/daesh-financial-flows-stop-terror-funding/

Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history. *Wired*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Greenberg, K. J. (2016). Counter-radicalization via the internet. *The ANNALS of the American Academy of Political and Social Science*, 668(1), 165-179. https://doi.org/10.1177/0002716216631194

Gregory, J. (2022, January 26). 10 years later, what did LulzSec mean for cybersecurity? *Security Intelligence*. https://securityintelligence.com/articles/lulzsec-10-years-later-cybersecurity-influence-meaning/

Herzog, S. (2011). Revisiting the Estonian cyber-attacks: Digital threats and multinational responses. *Journal of Strategic Security*, 4(2), 49-60. https://doi.org/10.5038/1944-0472.4.2.2

Haizler, O. (2017). The United States' cyber warfare history: Implications on modern cyber operational structures and policymaking. *Cyber, Intelligence, and Security*, 1(1), 31-45. https://doi.org/10.1080/23802877.2017.1305773

Iftikhar, S. (2024). Cyberterrorism as a global threat: A review on repercussions and countermeasures. *PeerJ Computer Science*, 10, e1772. https://doi.org/10.7717/peerj-cs.1772

Jayakumar, S. (2020). Cyber attacks by terrorists and other malevolent actors: Prevention and preparedness with three case studies on Estonia, Singapore, and the United States. In A. P. Schmid (Ed.), *Handbook of terrorism prevention and preparedness* (pp. 871–925). International Center for Counter-Terrorism.

Joubert, V. (2012). Five years after Estonia's cyber attacks: Lessons learned for NATO. *NATO Defense College Research Paper*, Imprimerie Deltamedia Group.

Marquardt, A., Levenson, E., & Tal, A. (2021, February 10). Florida water treatment facility hack used a dormant remote access software, sheriff says. *CNN*. https://abc17news.com/news/national-world/2021/02/10/florida-water-treatment-facility-hack-used-a-dormant-remote-access-software-sheriff-says/

Maryville University. (2022, January 20). Cyber terrorism: What it is and how it's evolved. *Maryville Online*. https://online.maryville.edu/blog/cyber-terrorism/

McGuinness, D. (2017, April 27). How a cyber-attack transformed Estonia. *BBC News*. https://www.bbc.com/news/39655415

Montasari, R. (2024). *Cyberspace, cyberterrorism and international security in the Fourth Industrial Revolution*. Springer.

Olson, P. (2012). *We are Anonymous: Inside the hacker world of LulzSec, Anonymous, and the global cyber insurgency*. Little, Brown and Company.

Öğün, M. N., Yurtsever, S., Aslan, M., & Elburası, M. (2021). Terrorist use of cyber technology. *Eskişehir Teknik Üniversitesi Bilim ve Teknoloji Dergisi B-Teorik Bilimler*, 9(Iconat Special Issue 2021), 113-128.

Plotnek, J., & Slay, J. (2021). Cyber terrorism: A homogenized taxonomy and definition. *Computers & Security*, 102, 102145. https://doi.org/10.1016/j.cose.2020.102145

Schindler, H.-J. (2020). United Nations and counter-terrorism: Strategy, structure, and prevention of violent extremism conducive to terrorism: A practitioner's view. In S. J. Hansen & S. Lid (Eds.), *Routledge Handbook of Deradicalisation and Disengagement* (pp. 163-179). Routledge.

Tafoya, W. L. (2011). Cyber terror. *FBI Law Enforcement Bulletin*, 80(11), 1-7.

United Nations Office on Drugs and Crime. (2012). *The use of the internet for terrorist purposes*. United Nations. https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

U.S. Department of Justice. (2020, August 13). Global disruption of three terror finance cyber-enabled campaigns. *U.S. Department of Justice*. https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns

Verton, D. (1999, April 4). Serbs launch cyberattack on NATO. *Next Gov*. https://www.nextgov.com/digital-government/1999/04/serbs-launch-cyberattack-on-nato/195288/

Vilić, V. M. (2017). Dark web, cyber terrorism and cyber warfare: Dark side of the cyberspace. *Balkan Social Science Review*, 10(10), 7-25.

Wilson, C. (2005). *Computer attack and cyber terrorism: Vulnerabilities and policy issues for Congress*. CRS Report for Congress. https://fas.org/irp/crs/RL32114.pdf