MANAS Sosyal Araştırmalar Dergisi 2025 Cilt: 14 Sayı: 2
MANAS Journal of Social Studies 2025 Volume: 14 No: 2
ISSN: 1694-7215
Research Paper / Araştırma Makalesi

A Prevention Strategy in Combatting the Online Actions of Terrorist Organizations: Cyber Deterrence

Emre ÇITAK[1]

Abstract
This study explores the effectiveness of deterrence against terrorist organizations that use online environments, including cyberattacks, from various perspectives. Addressing the armed wings, financial resources, external aid and support, recruitment methods, and perception management activities of terrorist organizations requires a comprehensive approach. In addition to these aspects, monitoring and countering their activities in cyberspace constitute a complementary side of the struggle. Therefore, keeping terrorist organizations away from the cyber domain, halting their activities, and preventing attacks require a highly nuanced approach. This study will examine the impact of states' cyber power and defense capabilities on terrorist organizations. As the distinctive aspects of cyber deterrence pose a challenge for states, understanding how to deter non-state actors like terrorist groups is a valuable area of investigation. The study will reevaluate deterrence theory in the context of non-state actors and beyond traditional battlefields. The first section of the study will outline the conceptual framework of cyber deterrence. The second section will analyze the cyber threat potential of terrorist organizations and evaluate cyber deterrence through the lenses of denial and punishment. The conclusion will discuss a comprehensive national cyber deterrence strategy. The study aims to make a modest contribution to strategies for combating the online activities of terrorist organizations.

Keywords: Cyber Security, Cyber Deterrence, Counterterrorism, Deterrence Theory, National Security

Terör Örgütlerinin Çevrimiçi Eylemleriyle Mücadelede Bir Önleme Stratejisi: Siber Caydırıcılık

Öz
Bu çalışmada çevrimiçi ortamı siber saldırılar dâhil pek çok amaçla kullanan terör örgütleri üzerinde caydırıcılığın etkililiği farklı yönlerden tartışılmaktadır. Terör örgütlerinin silahlı kanadıyla, finans kaynaklarıyla, dış yardım ve destekleriyle, eleman temin etme yollarıyla ve algı yönetim faaliyetleriyle mücadele edilmesi bütüncül bir yaklaşımı gerektirmektedir. Günümüzde bunların yanı sıra siber alandaki hareketliliklerinin takip edilmesi ve engellenmesi mücadelenin tamamlayıcı etkisini oluşturmaktadır. Bu nedenle terör örgütlerini siber alandan uzak tutmak, buradaki faaliyetlerini durdurmak ve saldırılarını engellemek oldukça hassas bir yaklaşım gerektirmektedir. Çalışmada devletlerin sahip oldukları siber güç ve savunma kabiliyetinin terör örgütleri üzerindeki etkisi ele alınacaktır. Siber caydırıcılığın geleneksel caydırıcılıktan farklılaşan yönleri hâlihazırda devletler için bir meydan okuma oluştururken, bir devlet dışı aktör olarak terör gruplarının nasıl caydırılabileceği incelenmesi fayda sağlayacak konulardandır. Çalışmada caydırıcılık teorisi, bir devlet-dışı aktör üzerinde ve geleneksel mücadele sahasının dışında yeniden değerlendirmeye açılacaktır. Çalışmanın birinci bölümünde siber caydırıcılığın kavramsal çerçevesi çizilecektir. İkinci bölümde ise terör örgütlerinin siber tehdit potansiyeline yer verildikten sonra siber caydırıcılık üzerinden bir analiz yapılacaktır. Burada denial ve punishment kapsamında bir değerlendirme yapılacaktır. Sonuç bölümünde ise kapsamlı ulusal siber caydırıcılık stratejisi hakkında bir tartışma yer alacaktır. Çalışmanın terör örgütlerinin çevrimiçi faaliyetleriyle mücadele stratejilerine mütevazı bir katkı sunması planlanmaktadır.

Anahtar Kelimeler: Siber Güvenlik, Siber Caydırıcılık, Terörizmle Mücadele, Caydırıcılık Teorisi, Ulusal Güvenlik

Atıf İçin / Please Cite As:

Çıtak, E. (2025). A prevention strategy in combatting the online actions of terrorist organizations: Cyber deterrence. *Manas Sosyal Araştırmalar Dergisi, 14* (2), 838-850. doi:10.33206/mjss.1549263

Geliş Tarihi / Received Date: 27.07.2024 **Kabul Tarihi / Accepted Date:** 27.01.2025

[1] Assoc Prof. – Hitit University Department of International Relations, emrecitak@hitit.edu.tr,
ORCID: 0000-0002-8704-6495

Introduction

The cyber domain draws more interaction with every passing minute. Individuals, states, companies, and other actors strive to exist in the virtual world, competing with the real world, and they are forming increasingly intense relationships in this expanding space. Every aspect of daily life, from commercial activity to communication, education to socializing, has been transferred to the cyber domain. While this trend means the simplification and acceleration of many processes, it also brings various problems. On the one hand, it's possible to connect with the world and handle any task with a small mobile phone, but on the other hand, the activities of malicious individuals and groups are a cause for concern.

It is incorrect to define technology in a dichotomous manner such as either a "devil" or an "angel" because, depending on who uses it and for what purpose, technology today has become a phenomenon that brings with it many outcomes. Just as today differs from yesterday due to ongoing developments in various aspects of life, inevitably, tomorrow will not resemble today. In this process, everyone and everything is somehow affected or positioned. Of course, it is necessary to pay special attention to the internet and related systems, which have created a revolutionary change in technological developments. The widespread accessibility of computer networks and systems has led billions of people, along with legal entities, to transfer everything from their personal information to their material assets into this domain. Undoubtedly, this situation is perceived as an opportunity for those with malicious intentions. Hackers, national/transnational crime groups, and terrorist organizations are actors that use the cyber domain for their interests and interfere with other users. It is necessary to note that the terrorist organizations examined in this study have been active in the cyber domain since the internet became publicly accessible in the 1990s.

Undoubtedly, just like any major development that could bring about profound changes, the introduction of the Internet into human life has also launched many concerns. Various ideas have been expressed, ranging from the notion that personal data will never be safe again to the fear that computers will control humans. One of the significant claims has been that the cyber domain will become the new battlefield and that international conflicts will be based on power struggles within this realm (Gartzke, 2013). Advancements in cyberspace have made it both a critical aspect of national security and a necessity to prioritize. In this context, cyber power has become a key factor. Enhancing capabilities within the cyber domain boosts cyber power and reinforces cyber security. (Kuehl, 2009, pp. 38-40). It has not been surprising that security concerns have arisen alongside the development of computer networks and systems and the expansion of their areas of use. The safety of individuals' information, as well as the shift of international struggles into this domain, has made the question of how to ensure cyber security one of the most heated discussions on the agenda. In this context, computer systems protection, network infrastructures, and users form the core approach.

A strategy rooted in the Cold War era has emerged in discussions on ensuring cybersecurity in this sense. During the Cold War, the possession of nuclear weapons created a state of mutually assured destruction, which acted as a deterrent for both sides. In that period the potential devastation caused by a retaliatory strike in response to an attack became a critical factor to consider. In this context, deterrence—preventing conflict without the need for an initial attack—was seen as a key element in maintaining security. Over time, deterrence has evolved into a strategic approach integrated into various aspects of state policy. The belief that aggressors would either be unable to achieve their desired outcome due to defense measures or would face severe consequences from a retaliatory response has often led potential attackers to reconsider their actions. In today's world, where cyberspace has become a central battleground, ensuring security in this domain has become one of the primary concerns for states. As a result, cyber deterrence is increasingly viewed as an effective tool in responding to the malicious activities of both state and non-state actors.

Deterrence, in general, can be described as the will to dissuade an aggressor from attacking by making it avoid the attack. In this context, deterrence can be regarded as a threat to the aggressor that the attack may fail and that a response will follow. Deterrence can be understood as the ability to prevent an attack by convincing potential aggressors that the cost of their actions will outweigh the benefits (Quackenbush, 2011, pp. 2-5). Effective deterrence relies on three main components: capability, credibility, and communication. It requires the ability to counter the aggressor, the general acceptance that this ability will be used immediately, and the proper communication of this capability to the adversary (Chen, 2017). In his work, Michael Quinlan mentions several factors for successful deterrence: the

capacity to retaliate proportionally or in multiple ways, demonstrating that the attack may incur more costs than benefits, showing the will to retaliate, declaring what actions will provoke a response and what extent, and deeply evaluating the probabilities and possibilities (2004, pp. 11-13). Accordingly, capability, credibility, and communication are the core elements of deterrence. Having the capacity to respond appropriately in case of an attack, others' belief that this capacity will be used, and successfully communicating this to all parties form a successful deterrence strategy (Jasper, 2015, p. 65).

Wyn Bowen suggests that a successful deterrence strategy requires several key components: (1) possessing or at least giving the impression of having the necessary capability to support the deterrence message; (2) showing a clear intent and determination to act on the deterrent threat, or at least appearing ready to do so; and (3) effectively communicating this message to adversaries, making it clear what boundaries or limits should not be crossed (2004, pp. 59-60). Robert Jervis discusses the elements necessary for the success of deterrence: the credibility of threats, the calculation of probabilities by the target, the interaction between the parties to anticipate actions and intelligence activities to understand the adversary (2016, pp. 67-69).

Certainly, the concept of cyber deterrence discussed in this study exhibits significantly different characteristics compared to traditional deterrence. The cyber domain is defined by its ambiguous boundaries, the interplay of asymmetric and symmetric relationships, and a state of continuous flux. This domain features a transformation in scales, interests, power, and defenses, with ambiguity pervasive at every stage of engagement. The diversity of actors and the constant evolution of the environment make cyber deterrence distinctively different from traditional deterrence (Sterner, 2011, pp. 65-66). While traditional deterrence aims to prevent a military attack from an emerging aggressive power, cyber deterrence, as will be discussed in the relevant section, takes a different approach. The nature of cyber attacks, the specific characteristics of the cyber domain, and the particularity of defense measures contribute to this distinction.

During the Cold War, the deterrent effect of nuclear weapons held by states had distinct characteristics. The likelihood of suffering damage greater than that which could be inflicted on the adversary strongly contributed to deterrence, often leading potential aggressors to reconsider their intentions. Today, high-level states in the political, military, and economic arenas can also create a deterrent effect, as aggressors may be deterred by the possibility that an attack could fail to achieve the desired outcome or result in severe retaliation. In this context, effectively communicating the capacity for both prevention and punishment can constitute a successful defense strategy. However, when dealing with the virtual domain and non-state actors, deterrence must be considered from different perspectives.

This study explores the effectiveness of deterrence against terrorist organizations that use online environments, including cyberattacks, from various perspectives. It is crucial to recognize that one of the main reasons for the growing capabilities of terrorist organizations is their adaptability to technology. Like other groups that adopt technological advancements and integrate them into their operations, terrorist organizations leverage the cyber domain to enhance their activities. While the online environment presents both opportunities and threats, terrorist groups exploit these opportunities and contribute to the growing cyber threats. As a result, addressing the cyber aspect of terrorism is essential, and this challenge must be approached within the framework of cyber security. This study discusses the necessity of applying a deterrence strategy against the activities of terrorist organizations in the cyber domain. Addressing the armed wings, financial resources, external aid and support, recruitment methods, and perception management activities of terrorist organizations requires a comprehensive approach. In addition to these aspects, monitoring and countering their activities in cyberspace constitute a complementary side of the struggle. Therefore, keeping terrorist organizations away from the cyber domain, halting their activities there, and preventing their attacks require a highly nuanced approach. This study will examine the impact of states' cyber power and defense capabilities on terrorist organizations. As the distinctive aspects of cyber deterrence pose a challenge for states, understanding how to deter non-state actors like terrorist groups is a valuable area of investigation. The study will reevaluate deterrence theory in the context of non-state actors and beyond traditional battlefields. The first section of the study will outline the conceptual framework of cyber deterrence. The second section will analyze the cyber threat potential of terrorist organizations and evaluate cyber deterrence through the lenses of denial and punishment. The conclusion will discuss a comprehensive national cyber deterrence strategy. The study aims to make a modest contribution to strategies for combating the online activities of terrorist organizations.

Deterrence in Cyber Milieu: Basic Traits

It would not be incorrect to assert that the best defense is to avoid being attacked in the first place. Throughout history, receiving an attack has been a major security concern for states and is considered a national issue of existential significance. It is often challenging to ascertain the adequacy of defensive measures in advance, and any vulnerability can pose serious problems. Consequently, states may choose to engage in proactive measures to prevent attacks rather than merely waiting for them. This approach often results in increased levels of insecurity to ensure overall safety. In this context, deterrence appears to be a highly reasonable strategy compared to purely defensive or offensive options. The ability to dissuade an aggressor before they initiate an attack can be regarded as a significant display of power.

The advancement of computer and internet technologies has brought concerns about cyber security. Particularly, with the public availability and widespread use of the internet, the possibilities of cyber attacks and cyber warfare began to be debated almost immediately. These discussions have continued from the 1990s to the present day, with the cyber domain being extensively addressed within security studies through the lens of threats (van Creveld, 1991; Arquilla & Ronfeldt, 1993; Beeson, 1996; Arquilla & Ronfeldt, 1999; Clarke & Knake, 2011). The impact of technological advancement on the transformation of concepts related to warfare, conflict, and security forms the essence of this issue as it is necessary to acknowledge that the cyber environment occupies a unique space within the relationship between technology and security (Langner, 2016; Danky, Maliarchuk & Briggs, 2017).

With the emergence of security concerns in the cyber domain encompassing cyber warfare, cyber terrorism, and cybercrime, discussions naturally extended to relevant defensive and deterrent measures. The success of deterrence capacity during the Cold War as an adequate measure, combined with evaluations suggesting that similar challenges and threats will manifest in the cyber domain, has contributed to the development of the concept of cyber deterrence. In early writings on the subject, the enhancement of defensive capabilities was viewed as part of the broader development in the fields of information, networks, and technology (Der Derian, 1994; Harknett, 1996). Cyber threats do not present a more tolerable aspect compared to traditional attacks. Even though there may not be tangible military damage, situations can arise that lead to more severe or chronic problems. Consequently, ensuring cyber security requires efforts across multiple domains, including political, economic, legal, military, and cyber spheres (Sterner, 2011, pp. 75-76; Cerf, 2011). Cyberspace can be considered an integral part of a state's territory. In this context, cyber sovereignty emerges as a critical issue. However, unlike sovereignty in the physical world, actions or inactions in cyberspace contribute to heightened uncertainty. Consequently, cyber deterrence is a significant and successful strategic approach to addressing the challenges inside (Kolton, 2017).

The primary objective of cyber deterrence is to influence an adversary's decision-making process to dissuade it from conducting any cyber attack. A deterrent effect is achieved when the potential threat, cost, and risks associated with the cyber effort outweigh the perceived benefits, success, or gains anticipated by the attacker (Kugler, 2009, p. 327). The cyber domain is a realm where actors engage in cost-benefit calculations and must operate within the parameters of impact-response and gain-loss assessments (Boghard & Lonergan, 2017, p. 461). The use of cyber instruments or their potential introduces new elements into deterrence; however, it also raises concerns related to uncertainty, ambiguity, and confusion. As technology evolves, these issues continue to change. Particularly notable is the uncertainty regarding the impact levels of cyber attacks and instruments. These tools introduce two major issues. Firstly, targeting an adversary's command systems is both appealing and strategically advantageous but carries the risk of uncontrollable escalation. The threat to these essential networks might provoke either side to launch a preemptive strike or delegate attack authority to lower levels, thereby increasing the number of individuals who could initiate both cyber and physical attacks, which heightens the risk of broader conflict. Secondly, even without direct attacks on critical networks, the use of cyber tools is likely to disrupt communication among national leaders and their field units to some extent (Jervis, 2016, p. 72). Cyber deterrence is thus intertwined with concepts of cyber security and information warfare (Wheatley & Hayes, 1996; Stevens, 2012).

Cyber power is a fundamental component of cyber deterrence. Its increasing influence as a critical factor in international relations, coupled with its ability to both attract and intimidate, highlights its significant role. Unlike traditional forms of power, such as military or economic strength, cyber power can be expressed in various ways by different nations. This creates new dimensions in international relations,

allowing different actors to leverage deterrence capabilities (Kugler, 2009, pp. 317-318). The unique nature of cyber interactions, threats, and capacities also reshapes the concept of power.

The emergence of cyber security and the discussion of cyber warfare threats have underscored the necessity of possessing cyber power for effective conflict management. Just as military power holds significance in traditional warfare, cyber power carries the same level of importance in the online realm (Betz, 2012). Cyber power manifests as both offensive and defensive capacities. Offensive power refers to the arsenal of weapons available for cyber attacks, while defensive power encompasses security measures aimed at protecting the cyber domain. Thus, aggression and resistance become key components of cyber power (Valeriano & Maness, 2015, pp. 25-26). As discussed throughout this study, the offensive and defensive aspects of cyber power are crucial dimensions of cyber deterrence.

Martin Libicki argues that societies focused on enhancing their cyber attack capabilities are more engaged in cyber deterrence compared to those concentrating on traditional response capacities. These states prefer cyber retaliation over conventional hard or soft responses when faced with a cyber attack (2009, pp. 28-29). Cyber deterrence can be seen as a serious threat directed at adversaries. It involves not only defensive measures but also offensive capabilities, aiming to inflict irreparable damage on the opponent. As a result, an adversary contemplating a cyber attack may hesitate if it believes the potential counterattack will be severe. Therefore, states must communicate the extent of their capacity to respond to threats. This ensures that cyber capabilities can generate a deterrent effect, whether against traditional or cyber-initiated threats (Gaycken & Martellini, 2013, pp. 2-6).

Cyber deterrence generally relies on strategies of punishment and denial. In denial, the objective is to minimize or nullify the attacker's gains from their actions, whereas punishment involves imposing sanctions or penalties on the aggressor (Iasiello, 2014, pp. 55-56; Mazaar, 2018, pp. 2-3). When an attacker engages in rational calculation, they always weigh the potential gains against the risks. In this context, if the attacker faces significant resistance and the prospect of a severe counterattack, they may reconsider or delay their actions. Knowing that every attack has a purpose, the possibility that the attacker might not achieve their goals or could suffer significant losses intensifies the deterrent effect.

Chen highlights additional methods in cyber deterrence beyond punishment and denial, specifically engagement and surprise. Techniques such as intelligence collection, information operations, and surprise operations are emphasized as practical applications in this context (2017, pp. 104-106). Soesanto and Smeets provide a comprehensive overview of the literature on cyber deterrence, identifying categories like deterrence by denial, deterrence by punishment, deterrence by entanglement, and deterrence by delegitimization (2021, pp. 392-394). Manuel Fisher offers a broad perspective by categorizing cyber deterrence into four types: deterrence of denial, deterrence of retaliation, deterrence of entanglement, and deterrence by normative taboos. This classification illustrates that in the cyber age, states have developed new qualified deterrence tools that contribute to their national security (2019). In punishment, appropriate tools are used for retaliation, while denial involves creating overall protection through cyber security mechanisms and measures. Advances in cyber technology continue to influence the strategies and effectiveness of deterrence (Denning, 2015, pp. 13-14). Within denial, resilience is a crucial element. The ability to withstand or restore systems after an attack enhances the deterrent effect (Wilner, 2017, pp. 310-311).

Scott Jasper argues that assessing the effectiveness of four deterrent responses—retaliation, denial, entanglement, and active defense—requires addressing four fundamental questions. These questions are: "Can threats of proportionate response realistically achieve deterrence by retaliation?"; "Are defensive measures adequate to achieve deterrence by denial?"; "Will cooperative measures restrain behavior through deterrence by entanglement?"; and "Is the concept of active cyber defense technically and legally viable?" Evaluating these questions helps in determining the practicality of deterrence and the effort required to implement it effectively (2015). Will Goodman identifies eight key elements of cyber deterrence in his study: interest, deterrent declaration, denial measures, penalty measures, credibility, reassurance, fear, and cost-benefit calculation. States develop and announce deterrence strategies to protect their interests. These strategies should include both denial and penalty measures. The declarations made should be perceived as credible and reassuring by others, meaning that everything stated should be believable and provide guarantees that actors not engaging in attacks will not suffer any harm. Actors deterred by potential penalties and preventive measures are likely to be more hesitant to initiate attacks. A cost-benefit calculation is performed within this framework (2010, pp. 105-106). Emilio Iasiello defines

cyber deterrence as a strategy where a state signals its intentions to influence the attacker's decision-making process, aiming to dissuade them from hostile actions through the fear of severe retaliation and by maintaining the status quo (2014, p. 55). When an attacker recognizes that the cost of a cyber attack is high, the likelihood of success is low, and the target is prepared for a counter-operation, the deterrent effect is significantly increased. This understanding can lead to a high probability of deterrence (Elliot, 2011, p. 38).

It is challenging to determine which deterrence strategy is most effective. For instance, retaliation might be more effective when attribution is possible, while in cases where the attacker cannot be precisely identified, denial and active defense may be more practical options. Additionally, strategies may vary depending on the importance of the target (Lindsay, 2015, p. 62). Kristin Heckman et al. argue that the effectiveness of defense in cyberspace depends on the quality of denial and deception practices. This allows for blocking unauthorized access and luring attackers into traps by redirecting them (2013).

Cyber deterrence is not as effective a measure as its more established counterpart, nuclear deterrence. During the Cold War, nuclear threats involved clear lines, identifiable aggressors, predictable damage, likely effective countermeasures, minimal involvement of third parties, and no obligation for individuals or private companies to defend themselves. All parties involved in such conflicts would experience losses, and the threshold for acceptable use of such weapons was well-defined. In this context, the attacking party knew they would face nuclear retaliation if they proceeded. In contrast, today's cyber attacks are relatively simple and inexpensive, whereas cyber defenses are complex and costly, which can motivate attackers. Additionally, the anonymity of attackers and the unpredictability of subsequent actions are significant challenges for deterrence. While the possibility of retaliation may deter cyber attackers to some extent, the risks and uncertainties involved can make direct responses difficult for the affected party. This creates a dual challenge in cyber deterrence: to either respond immediately and accept the risk of misjudgment or to refrain from retaliation, which may undermine the perceived strength of deterrence (Libicki, 2009, pp. 40-74). In nuclear deterrence, the primary factors are the ability of the attacked state to respond and the capacity to inflict significant damage on the aggressor. Assessing cyber deterrence by these criteria is more challenging (Elliot, 2011, p. 37). Kamaal Jabbour and Paul Ratazzi, after evaluating the unique characteristics of the cyber domain, identify the differences between cyber deterrence from traditional deterrence as the lack of attribution, the low cost of aggression with high potential rewards, inconsequentiality, low probability of detection, the risk of losing more than the adversary, and the ability of new technology to rapidly alter the situation (Jabbour & Ratazzi, 2012, pp. 39-40). Moreover, the relationship between cyber deterrence and technology necessitates a more in-depth examination of the issue. While the boundaries of traditional deterrence are well-defined, the constant evolution of cyber attacks and defense tools alters the nature and effectiveness of deterrence. As a result, cyber deterrence is not a clearly defined or easily measurable form of deterrence with observable benefits (Geist, 2015, pp.55-56).

While it is undoubtedly impossible to prevent all cyber attacks, the ability of cyber deterrence to dissuade or delay certain attackers and potential attacks underscores its necessity. Cyber deterrence plays a crucial role in supporting other national defense strategies, providing assurance to allies, and responding to adversaries that might attack through any means. Thus, rather than viewing cyber deterrence as the sole provider of cybersecurity, it is more accurate to consider it as a component that supports broader security efforts with various benefits (Kugler, 2009, pp. 326-328). The prevailing view in the cyber domain is that attacks are often more effective than defenses, leading to questions about the efficacy of deterrence. The main reasons for this skepticism include the inability to completely neutralize an adversary's weapons, issues with attribution, and uncertainties about the effectiveness of defensive capacities against attacks (Gartzke & Lindsay, 2015, pp. 320-323). To establish effective cyber deterrence, several elements must be in place: identifying the adversary and understanding their intentions, directly communicating deterrent messages, providing appropriate responses, and accurately analyzing evolving attack methods with technological capabilities.

The effectiveness of deterrence must be considered alongside its potential shortcomings. Various factors can undermine deterrence, including attribution issues, deception, inadequate response policies, the aggressor's determination, and insufficient communication of deterrent messages. In the cyber domain, where attacks can be easier and less costly than defenses, the success of deterrence hinges on multiple factors and the effective implementation of all elements (Lindsay, 2015). The anonymity, suddenness, and potentially devastating nature of cyber attacks can reduce the likelihood of retaliation, leading to

arguments that deterrence may not be sufficiently effective (Betts, 2013). However, Gartzke and Lindsay argue that complete anonymity in the online world is not guaranteed. Defenders can deploy deceptive traps, such as tracking beacons to trace attackers or silent systems that detect intrusions and provide clues about the attacker's identity. The possibility of identification means that attackers cannot entirely disregard the threat of retaliation. Moreover, adversaries using deception to bypass deterrence may be subject to counter-deception, risking exposure if they protest defensive measures. Even if attackers remain anonymous, the threat of deception can still impose risks, making them cautious and potentially limiting their actions, even if the defensive deception is not fully successful (Gartzke & Lindsay, 2015, p. 339). Lastly, unlike physical attacks, cyber-attacks are often difficult to detect, and some viruses can go unnoticed for years. Deterrence operates between attack and defense, and undetected attacks make it challenging to determine whether an adversary has attacked or not. Consequently, evaluating the success of deterrence is also complex (Wilner, 2017, p. 312). Given that deterrence is effective only when appropriate punishment can be imposed, the difficulty in identifying attackers raises questions about the effectiveness of cyber deterrence (McKenzie, 2017, pp. 7-8).

In conclusion, it is essential that potential attackers understand and recognize the power and capacity of cyber deterrence to dissuade them. The prevailing uncertainties in the cyber domain can not only challenge the effectiveness and persistence of deterrence and punishment but can also motivate potential attackers rather than dissuade them. Thus, a state's cyber response to other states or non-state actors presents a framework that extends beyond traditional reprisals. The effectiveness of cyber deterrence is subject to debate due to the unique characteristics of the cyber domain. Issues such as the lack of awareness or understanding of one's own capacity by others, the ability of attackers to conceal their identities, and the potential for retaliatory measures to lack real-world impact can make responses seem manageable from the perspective of potential attackers (Fischerkeller & Harknett, 2017; Libicki, 2018). Therefore, it is beneficial to consider Nye's emphasis on the importance of the "how, who, and what" questions in evaluating the effectiveness of cyber deterrence (2017, pp. 68-69).

Cyber Deterrence Against Terrorist Groups: How Effective?

Terrorist organizations are pragmatic structures that operate in line with their ultimate goals. They incorporate any methods, techniques, and tools that could benefit them into their strategies. By creating a fearsome and deterrent effect on the targeted society, they seek to extract concessions. These illegal groups, which do not recognize any rules and can adapt to any conditions to achieve their ultimate goals, pose a significant threat in the cyber world as well. The cyber domain is an area where not only states and individual users, but also non-state actors are actively engaged. Undoubtedly, among these non-state actors, those with malicious intent can become sources of threat in the cyber realm through their activities aligned with their agendas (Valeriano & Maness, 2015). With the general availability of computer networks and systems, the increased interaction and mobility in the cyber domain have opened a process in which terrorist organizations are more intensively involved. Radical groups such as terrorists and criminal organizations have increasingly established a presence in the cyber realm, seeking various benefits. In recent years, it has become evident that terrorist organizations have found ways to use the cyber domain as effectively as the real world. Following the intensification of activities in cyberspace, a series of studies highlighting the shift of terrorist organizations toward this area have been gradually published (Furnell & Warren, 1999; Valari & Knights, 2000; Conway, 2006).

For terrorist organizations, the cyber domain has become a fertile ground for their operations, offering significant advantages. The cyber world, with its continuous activity, anonymity, high interactivity, and ease of access, provides extra benefits for their activities. Terrorist groups not only launch attacks on official institutions and civilian targets using software and viruses but also engage in various online activities. These include diversifying their financial resources, laundering and increasing their income, training members, recruiting new individuals, promoting their ideologies, conducting propaganda, and transmitting messages. The high level of activity on social media platforms particularly attracts terrorist organizations, just as it does other malicious actors (Bieda & Halawi, 2015; Gill et al., 2017; Azani & Liv, 2018).

In current national security policies and strategies, cyber counterterrorism has become a significant focus. On the one hand, the cyber domain has become an increasingly vital part of national borders, while on the other hand, terrorist organizations are intensifying their activities in the cyber realm. Their attacks on the cyberinfrastructure, information systems, and online interactions of targeted societies, or their

potential to do so, pose a realistic threat. Terrorists can inflict damage and also gain financial benefits through cyber attacks (Hua, Chen, & Luo, 2018). The growing importance of cyber security within national policies and strategies has necessitated the development of procedures, resources, and capabilities in this area. The presence of various threats in the cyber domain has made it imperative to establish regulations concerning this aspect of national security (Kuehl, 2009, p. 41).

Despite their intense activities in cyberspace, the capacity and willingness of terrorist groups to engage in cyberattacks remain subjects of debate. The lack of serious examples of such attacks has led to more focus on the potential threat. However, the consequences of cyberattacks by politically motivated groups against civilians, military systems, or institutional structures raise significant concerns (Lachow, 2009; Huey, 2015; Marsili, 2018). Cyberattacks can be more attractive to terrorist groups due to their lower cost compared to traditional attacks, the anonymity of the attack source, the wide variety and number of potential targets, the ability to conduct attacks remotely, and the reduced need for personnel. In some cases, cyberattacks can even affect more people than traditional attacks (Weimann, 2005, p. 137; Macdonald, Jarvis, & Lavis, 2019). Thus, since the proliferation of internet use, terrorist organizations have increasingly engaged in information warfare and cyber conflict. Besides the mentioned advantages gained from cyberspace, they can intensify their harmful activities and exploit the vulnerabilities of their targets more effectively (Libicki, 2007, pp. 47-50).

The deterrence strategy applied to non-state actors differs significantly from that used against states. It is crucial to thoroughly analyze the intentions, goals, and methods of non-state actors, as their agendas often diverge from those of states. Expecting non-state actors to be deterred by elements that typically dissuade states is often misguided. Therefore, deterrence today must be considered within the context of non-state actors' capacities, cost-benefit calculations, and specific agendas (Lowther, 2012, pp. 3-4). Additionally, deterrence theory is based on the assumption that the attacker will analyze the deterrent capacity, clearly perceive the message, and reconsider their intentions after evaluating the costs. This presumes rational behavior. However, expecting rational behavior from all actors at all times is not always feasible, which raises questions about the effectiveness of deterrence (Stein, 2009). Non-state actors' rationality is often influenced by more dynamic factors, and organizations like terrorist groups frequently disregard this filter.

Deterring terrorist organizations, as illegal non-state actors, involves distinct dynamics. Unlike state actors who may determine their actions on a cost-benefit analysis, terrorist groups often operate based on ideological motives rather than a pursuit of tangible gains. Consequently, these groups may place less importance on potential losses or rewards. Additionally, for terrorist organizations, the act of attacking itself and the subsequent message it conveys are often prioritized over the damage caused. Another challenge is that identifying perpetrators of terrorist attacks can be extremely difficult, making retaliation through damage control problematic. These factors render both general deterrence and cyber deterrence against terrorist organizations more complex and contentious.

Deterrence plays a crucial role in combating terrorist organizations. Terrorist activities can be deterred through punishment, coercion, and denial strategies. This deterrence encompasses not only penalties and countermeasures directed at illegal organizations and their members but also extends to those who provide any form of support. Additionally, delegitimizing the terrorists' beliefs is a part of this strategy (Wilner, 2011). Although the specifics of deterring non-state actors like terrorist organizations differ, the fundamental goal remains to prevent potential attacks and maintain the status quo. In this context, strategies involving punishment and denial can be effective. Demonstrating preparedness against terrorist attacks and showing that the likelihood of success is low, as well as the capacity to launch counterattacks against the leaders and structures of terrorist groups can create a deterrent effect (Bowen, 2004, pp. 61-63). Deterrence activities aim to alter the behaviors, plans, and thoughts of terrorists. Given that these organizations use any available methods to achieve their goals and operate without regard to legal or humanitarian constraints, deterrence must be considered on a broad scale. Terrorist groups can target both military and civilian objectives, design small-scale or large-scale operations, exert pressure on physical or non-physical assets, lie dormant, and act unexpectedly, and their ideological commitment can render punishment measures ineffective (Wilner, 2015). Thus, traditional deterrence theory is inadequate in the face of the capabilities and resources of modern terrorist organizations.

Regardless of the actor, the cyber deterrence that must be applied in the face of threats should involve sudden, dynamic, random, and unpredictable responses that will exhaust the attacker virtually,

mentally, morally, and even physically (Chen, 2017). Klein argues that despite all the challenges, deterrence and dissuasion can be effective methods against terrorist organizations' activities and cyberterrorism. He suggests that these approaches create a holistic strategy and are effective alongside other methods in combating terrorism (2015, pp. 35-36).

Terrorist organizations, despite their limited cyber capabilities compared to states, can still pose significant threats in the cyber realm, though these threats are often more constrained in scope. These organizations may seek to maximize the effectiveness of their attacks within their limited capacity. They might delay their actions if they know that states are on high alert and preparing to respond. Effective state measures, such as identifying the methods and targets of a terrorist attack, can mark the beginning of these operations. A state with high capacity, capable of precisely identifying the target, can inflict severe damage on a terrorist organization. This damage can impact not only the organization's cyber attack capabilities but also its other online activities. States can employ effective strategies to undermine terrorist organizations by disrupting their communication channels, shutting down or seizing their propaganda websites and social media accounts, sabotaging their financial acquisition methods, blocking their use of online platforms, and neutralizing their other covert activities in the virtual realm. The potential for such a comprehensive clean-up operation could be a valuable deterrent in keeping terrorist organizations at bay.

As discussed under the general theme of cyber deterrence, attribution is a crucial factor in deterring terrorist organizations. These non-state actors often obscure their identities in attacks on critical infrastructure, making it extremely difficult to trace the source of the attack. The asymmetric nature of terrorist organizations complicates attribution efforts (Wilner, 2017). When terrorist organizations do not openly claim responsibility for their cyber actions, it creates confusion about accountability. Even when the perpetrator is identified, pinpointing a specific adversary for retaliation is challenging. Terrorist groups often use anonymous accounts and constantly change their identity numbers, making direct attribution difficult. Moreover, determining exactly where and to whom retaliation should be directed adds another layer of complexity. Even if the terrorist group responsible for a cyber attack is known, the absence of fixed systems and users that states are obligated to protect can render the punishment process uncertain.

Cyber deterrence strategies targeting terrorist organizations must include robust defense mechanisms and effective retaliation capabilities. Any weakness or failure to deliver on the anticipated response can lead to significant credibility issues. Therefore, cyber capabilities should be tailored to the characteristics of terrorist organizations, which operate as non-state actors employing asymmetric strategies in cyberspace. Additionally, successfully delivering deterrence messages directly to these organizations is a critical factor.

Ultimately, the effectiveness of a deterrence strategy may be evaluated based on whether it prevents attacks by maintaining a credible deterrent image. However, the situation with terrorist organizations remains debatable. While a state's cyber power may cause terrorist groups to reconsider or delay their actions, claiming complete effectiveness is unrealistic. Unlike states, terrorist organizations may not be as deterred by attack failures or retaliatory measures. Nevertheless, by monitoring terrorist activities in cyberspace, tracking their infrastructure, and tracing their members, states can better prepare for and respond swiftly to threats. As states address vulnerabilities and strengthen their capabilities, even terrorist organizations may eventually be deterred from targeting them.

Conclusion and Assessment

National security has always been a primary concern for societies throughout history. While the nature of the threats shaping national security has evolved, the core responsibility of states to ensure security across all dimensions has remained constant. In response to these evolving threats, states have employed a variety of strategies, including bolstering defensive measures, initiating offensive actions, and engaging in international cooperation. As this study highlights, deterrence serves as a strategic alternative by clearly communicating a state's defensive and offensive capabilities to prevent aggression. The scope of deterrence has expanded significantly as national security is increasingly viewed not only in military terms but also through economic, social, and environmental lenses. The rising significance of cyberspace adds a new virtual dimension to these traditionally physical concerns, making cybersecurity a critical pillar of national security and an integral aspect of state security policies.

In the contemporary security paradigm, safeguarding borders from physical incursions is as important as defending against cyberattacks. Thus, investments in cyberspace must not only increase but also diversify and develop continuously. Enhancing both defensive and offensive cyber capabilities

enables states to foster a credible deterrent effect against potential adversaries. Whether cyber deterrence can be as effective as traditional forms of deterrence is still subject to significant debate. Nonetheless, the development of advanced protective mechanisms—coupled with the ability to detect and thwart often elusive cyberattacks—undoubtedly strengthens the security of a state's digital infrastructure.

As states engage in cyber warfare rhetoric and societies become increasingly vulnerable to cybercrime, the growing cyber presence of terrorist groups further complicates the threat landscape. Beyond their organizational activities—such as communication, propaganda, radicalization, and fundraising—terrorist groups also exploit cyberspace to inflict damage. These organizations seek to infiltrate, disrupt, or compromise the computer networks of governments, private entities, and individuals, often resulting in the theft of sensitive data, operational disruptions, financial losses, and threats to critical infrastructure. Therefore, incorporating cyber deterrence into counterterrorism strategies is not only essential but also urgent.

Terrorist organizations are constantly searching for opportunities to exploit vulnerabilities within the computer systems of target societies. As their technical capabilities improve—with external support and the recruitment of members with specialized skills—terrorists are likely to become more adept in cyberspace, yielding greater returns from their activities and escalating the severity of their attacks. Consequently, addressing the cyber capabilities of terrorist organizations must be viewed as a pressing national security concern. Although it remains difficult to predict the precise nature, timing, or methods of terrorist cyberattacks, bolstering national cyber capabilities and implementing robust deterrence strategies offer a pragmatic response to these evolving threats.

While much of the discourse surrounding cyber deterrence focuses on its effectiveness against other states, applying this concept to non-state actors, such as terrorist organizations, presents a unique set of challenges. Terrorist groups are pragmatic entities; they seek to both enhance their offensive cyber capabilities and leverage the benefits of cyberspace to streamline their operations. A comprehensive counterterrorism strategy must, therefore, include a strong cyber component. Given the continuous efforts of terrorist organizations to probe for vulnerabilities in their target societies, it is expected that they will increasingly exploit cyberspace, a domain where absolute security is impossible due to its inherent uncertainties. To mitigate this threat, it is critical to disrupt the visible and covert online activities of terrorist organizations, such as their social media accounts, websites, and other communication channels. Tracking their financial movements and impeding their cyber networks are equally important. Additionally, states must be prepared to neutralize any attacks launched by these groups and respond with decisive retaliatory measures. Although terrorist organizations often act without the calculated rationality seen in state actors, they may reconsider their strategies if they believe their attacks will be ineffective or if they anticipate significant retaliation. Thus, cyber power emerges as a crucial tool for states in deterring terrorist organizations.

However, expecting terrorist organizations to exhibit the same rational behavior as states, which shape their foreign policy under the logic of deterrence—such as during the Cold War era with nuclear deterrence—is unrealistic. Terrorist groups are driven by different incentives and are often more opportunistic and less predictable. Yet, if they perceive that their cyber activities might expose their identities, compromise their networks, or attract debilitating counterattacks, they may limit their operations in cyberspace. To date, while terrorist groups have executed numerous cyberattacks, none have reached the catastrophic scale of paralyzing a society's critical infrastructure. However, discussions on cyberterrorism often revolve around worst-case scenarios, and it is clear that terrorist organizations are striving to increase the scale and impact of their cyber operations. In the near future, vital infrastructure such as energy grids, water supply systems, transportation networks, banking institutions, and military defense systems could become prime targets for cyber terrorists. Therefore, it is imperative that states continue to strengthen their cyber deterrence capabilities to stay ahead of these evolving threats.

Ethical Declaration

During the writing process of the study "*A Prevention Strategy Combating in Combating the Online Actions of Terrorist Organizations: Cyber Deterrence*" scientific rules, ethical and citation rules were followed. No falsification was made on the collected data and this study was not sent to any other academic publication medium for evaluation.

Declaration of Conflict

There is no potential conflict of interest in the study.

References

Arquilla, J. & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, 12(2), 141-165.
Arquilla, J. & Ronfeldt, D. (1999). The advent of netwar: Analytic background. *Studies in Conflict&Terrorism,* 22(3), 193-206.
Azani, E. & Liv, N. (2018). A comprehensive doctrine for an evolving threat: Countering terrorist use of social networks. *Studies in Conflict&Terrorism*, 43(8), 1-25.
Beeson, A. (1996). Top ten threats to civil liberties in cyberspace. *Human Rights*, 23(2), 10-13.
Betts, R. (2013). The lost logic of deterrence: What the strategy that won the Cold War can-and can't-do now. *Foreign Affairs*, 92(2), 87-99.
Betz, D. (2012). Cyberpower in strategic affairs: Neither unthinkable nor blessed. *Journal of Strategic Studies*, 35(5), 689-711.
Bieda, D. & Halawi, L. (2015). Cyberspace: A venue for terrorism. *Issues in International Systems*, 16(3), 33-42.
Borghard, E. D. & Lonergan, S. W. (2017). The logic of coercion in cyberspace. *Security Studies*, 26(3), 452-481.
Bowen, W. Q. (2004). Deterrence and asymmetry: Non-state actors and mass casualty terrorism. *Contemporary Security Policy*, 25(1), 54-70.
Cerf, V. G. (2011). Safety in cyberspace. *Daedalus*, 140(4), 59-69.
Chen, J. (2017). Cyber deterrence by engagement and surprise. *Prism*, 7(2), 100-107.
Clarke, R. A. & Knake, R. K. (2011). *Cyber war: The next threat to national security and what to do about it.* New York: Ecco.
Conway, M. (2006). Terrorists use of the internet and fighting back. *Information and Security*, 19, 9-30.
Danky, Y., Maliarchuk, T. & Briggs, C. (2017). Hybrid war: High-tech, information and cyber conflicts. *Connections*, 16(2), 5-24.
Denning, D. E. (2015). Rethinking the cyber domain and deterrence. *Joint Forces Quarterly,* 77, 8-15.
Der Derian, J. (1994). Cyber-deterrence. *Wired,* 2.09, https://www.wired.com/1994/09/cyber-deter/
Elliott, David. (2011). Deterring strategic cyberattack. *IEEE Security&Pivacy*, 9(5), 36-40.
Fischerkeller, M. P. & Harknett, R. J. (2017). Deterrence is not a credible strategy for cyberspace. *Orbis*, 61(3), 381-393.
Fisher, M. (2019). The concept of deterrence and its applicability in the cyber domain. *Connections*, 18(1-2), 69-92.
Furnell, S. M. & Warren, M. J. (1999). Computer hacking and cyber terrorism: The real threats in the new milenium? *Computer&Security*, 18(1), 28-34.
Gartzke, E. & Lindsay, J.R. (2015). Weaving tangled webs: Offense, defense, and deception in cyberspace. *Security Studies*, 24(2), 316-348.
Gartzke, E. (2013). The myth of cyberwar: Bringing war in cyberspace back down to Earth. *International Security*, 38(2), 41-73.
Gaycken, S. & Martellini, M. (2013). Cyber as deterrent. M. Martellini (Ed.), *Cyber security: Deterrence and IT protection for critical infrastructures* (pp.1-10). Springer.
Geist, E. (2015). Deterrence stability in the cyber age. Strategic Studies Quarterly, 9(4), 44-61.
Gill, P. et al. (2017). Terrorists use of the internet by numbers: Quantifying behaviors, patterns, and process. *Criminology&Public Policy*, 16(1), 99-117.
Goodman, W. (2010). Cyber deterrence: Tougher in theory than in practice. *Strategic Studies Quarterly*, 4(3), 102-135.
Harknett, R. J. (1996). Information warfare and deterrence. *Parameters*, 26(3), 93-107.
Heckmen, K. et al. (2013). Active cyber defense with denial and deception: A cyber-wargame experiment. *Computers&Security*, 35, 72-77.
Hua, J., Chen, Y. & Luo, X. (2018). Are we ready for cyberterrorist attacks? Examining the role of individual resilience. *Information&Management*, 55(7), 928-938.
Huey, L. (2015). This is not your mother's terrorism: Social media, online radicalization and practice of political jamming. *Journal of Terrorism Research*, 6(2), 1-16.
Iasiello, E. (2014). Is cyber deterrence an illusory course of action? *Journal of Strategic Security*, 7(1), 54-67.
Jabbour, K. & Ratazzi, P. (2012). Does the United States need a new model for cyber deterrence? A. B. Lowther (Ed.), *Deterrence: Rising powers, roque regimes, and terrorism in the twenty-first century* (pp. 33-48). Palgrave Macmillian.
Jasper, S. (2015). Deterring malicious behavior in cyberspace. *Strategic Studies Quarterly*, 9(1), 60-85.
Jervis, R. (2016). Some thoughts on deterrence in the cyber era. *Journal of Information Warfare*, 15(2), 66-73.
Kolton, M. (2017). Interpreting China's pursuit of cyber sovereignty and its views on cyber deterrence. The Cyber Defense Review, 2(1), 119-157.
Klein, J.J. (2015). Deterring and dissuading cyberterrorism. *Journal of Strategic Security*, 8(4), 23-38.
Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. F. D. Kramer, S. H. Starr & L. K. Wentz (Eds.), *Cyberpower and national security* (pp.24-42). Potomac Books.
Kugler, R. L. (2009). Deterrence of cyber attacks. F. D. Kramer, S. H. Starr & L. K. Wentz (Eds.), *Cyberpower and national security* (pp.309-342). Potomac Books.

Lachow, I. (2009). Cyber terrorism: Menace or myth? F. D. Kramer, S. H. Starr & L. K. Wentz (Eds.), *Cyberpower and national security* (pp.437-464). Potomac Books.
Langner, R. (2016). Cyber power: An emerging factor in national and international security. *Horizons: Journal of International Relations and Sustainable Development*, 8, 206-2018.
Libicki, M. C. (2007). *Conquest in cyberspace: National security and information warfare*. Cambridge University Press.
Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. RAND.
Libicki, M. C. (2018). Expectation of cyber deterrence. *Strategic Studies Quarterly*, 12(4), 44-57.
Lindsay, J. R. (2015). Tipping the scale: The attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity*, 1(1), 53-67.
Lowther, A. B. (2012). Introduction: How has deterrence evolved? A. B. Lowther (Ed.), *Deterrence: Rising powers, roque regimes, and terrorism in the twenty-first century* (pp.1-16). Palgrave Macmillian.
Macdonald, S., Jarvis, L. & Lavis, S. M. (2019). Cyberterrorism today? Findings from a follow-on survey of researchers. *Studies in Conflict&Terrorism*, 45(8), 1-26.
Marsili, M. (2018). The war on cyberterrorism. *Democracy and Security,* 15(2), 172-199.
Mazaar, M. J. (2018). Understanding deterrence. *Perspective*, RAND Corporation.
McKenzie, T. M. (2017). Is cyber deterrence possible? *Perspectives on Cyber Power*. Air University Press.
Nye Jr., J. S. (2017). Deterrence and dissuasion cyberspace. *International Security*, 41(3), 44-71.
Quackenbush, S. L. (2011). *Understanding general deterrence: Theory and application*. Palgrave Macmillian.
Quinlan, M. (2004). Deterrence and deterrability. *Contemporary Security Policy*, 25(1), 11-17.
Soesanto, S. & Smeets, M. (2021). Cyber deterrence: The past, present, and the future. F. Osinga & T. Sweijs (Eds.), *NL Arms Netherlands annual review of military studies 2020: Deterrence in the 21st century- Insights from theory and practice*. Asser Press&Springer.
Stein, J. G. (2009). Rational deterrence against 'irrational' adverseries? No common knowledge. T. V. Paul, P. M. Morgan & J. J. Wirtz (Eds.), *Complex deterrence: Strategy in the global age* (pp. 58-84). The University of Chicago Press.
Sterner, E. (2011). Retaliatory deterrence in cyberspace. *Strategic Studies Quarterly*, 5(1), 62-80.
Stevens, T. (2012). A cyber war of ideas? Deterrence and norms in cyberspace. *Contemporary Security Policy*, 33(1), 148-170.
Valari, L. & Knights, M. (2000). Affecting trust: Terrorism, internet and offensive information warfare. *Terrorism and Political Violence*, 12(1), 15-36.
Valeriano, B. & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press.
van Creveld, M. (1991). *Technology and war: From 2000 B.C. to the present*. The Free Press.
Weimann, G. (2005). Cyberterrorism: The sum of all fears? *Studies in Conflict&Terrorism*, 28(2), 129-149.
Wheatley, G. F. & Hayes, E. E. (1996). *Information warfare and deterrence*. NDU Press Book.
Wilner, A. (2015). Contemporary deterrence theory and counterterrorism: A bridge too far? *International Law and Politics*, 47, 439-462.
Wilner, A. (2017). Cyber deterrence and critical-infrastructure protection: Expectation, application, and limitation. *Comparative Strategy*, 36(4), 309-318.
Wilner, A. S. (2011). Deterring the undeterrable: Coercion, denial and delegitimization in counterterrorism. *The Journal of Strategic Studies*, 34(1), 3-37.

EXTENDED ABSTRACT

Terör örgütleri nihai amaçları doğrultusunda hareket eden pragmatik yapılanmalardır. Bu doğrultuda uyguladıkları stratejilerin içine fayda sağlayacakları her türlü yöntemi, tekniği ve aracı dâhil etmektedirler. Böylece karşı toplum üzerinde yıldırıcı ve caydırıcı bir etki oluşturarak taviz elde etme arayışındadırlar. Nihai amaçlarına ulaşmak için herhangi bir kural tanımayan ve her türlü koşula uyum sağlayabilen terör örgütleri siber dünya için de dikkate alınması gereken bir tehlikedir. Terör örgütleri için siber alan, adeta rahat hareket kabiliyeti buldukları nimetler bahçesi anlamına gelmiştir. Sürekli aktif, kimliksizliğin yaygın, etkileşimin yoğun ve erişimin oldukça kolay olduğu siber dünya, terör örgütlerinin faaliyetlerinin gerçekleştirilmesi için fazladan avantajlar getirmektedir. Terör örgütleri resmi kurumlara veya sivil hedefleri çeşitli yazılım ve virüslerle saldırılar düzenlemenin yanı sıra farklı amaçlarla çevrimiçi ortamlarda etkin olmaktadırlar. Terör örgütleri çevrimiçi ortamlarda sempatizanlarına ulaşabilmekte, kara propaganda yapabilmekte, finans kaynakları bulabilmekte ve eğitim verebilmektedirler. Bunların yanı sıra askeri ve sivil hedeflerine yönelik siber saldırılar gerçekleştirmektedirler. Bu nedenle terörizmle mücadelenin önemli ayaklarından birini de siber güvenlik oluşturmaktadır. Siber güvenlik stratejileri içinde savunma ve saldırı kapasitelerinin yanı sıra üçün bir yöntem caydırıcılık olarak görünmektedir. Caydırıcılık, düşmanın kazanç-kayıp hesabı yaparak niyetinden vazgeçirilmesi olarak ifade edilebilmektedir. Saldırısı sonunda beklediği sonucu alamayacağını düşünen veya gelecek karşılıktan çekinen düşman saldırısını erteleyebilmekte veya tamamen vazgeçebilmektedir. Ortaya konulan kapasitenin düşmanın geri adım atmasını sağlayacağı yönündeki yaklaşım, caydırıcılık teorisinin temelini oluşturmaktadır. Nükleer silahların oluşturduğu bu etki

ile başlayan caydırıcılık stratejisi, günümüzde farklı açılardan incelenmektedir. Bu çalışmada da ele alındığı üzere günümüzdeki tehditlerin siber alana da yansıması, burada da etkin bir mücadelenin ortaya konulmasını gerektirmektedir. Böylece siber alanda hem savunma yapmak, hem gerektiğinde saldırı düzenlemek hem de caydırıcı etki oluşturmak son derece önemlidir. Devletler kadar siber imkanları olmayan terör örgütlerinin, siber alanda gerçekleştirecekleri saldırılar ciddi bir tehdit oluşturabilse de sınırlı çerçevede gerçekleşebilmektedir. Sınırlı bir çerçevede güce sahip örgütlerin, gerçekleştirecekleri saldırıdan maksimum verim almaları ilk tercihleri olabilmektedir. Devletlerin hareket geçmeleri için teyakkuzda beklediklerini bildiğinde eylemlerini erteleme yoluna gidebilmektedir. Devletlerin aldığı önlemlerle, saldırıyla birlikte terör örgütünün yöntemini belirleyebilmeleri ve saldırının geldiği adresi tespit edebilmeleri sonun başlangıcı olabilmektedir. Hedefini tam olarak belirleyebilen kapasitesi yüksek bir devlet, terör örgütüne ciddi zararlar verebilmektedir. Bu zararlar örgütlerin siber saldırı imkanlarına olduğu kadar, diğer çevrimiçi faaliyetlerine yönelik de olabilmektedir. Devletler etkili bir strateji ile örgütlerin iletişim kanallarını çökertme, propagandaları mecraları olan ağ sayfalarını ve sosyal medya hesaplarını kapatma-ele geçirme, finans elde etme yöntemlerini baltalama, çevrimiçi platformları kullanmalarını engelleme ve sanal alanda yürüttükleri diğer gizli faaliyetlerini etkisiz kılma gibi yaptırımlar uygulayabilmektedirler. Böylesi bir topyekun temizleme operasyonunun gerçekleştirilme ihtimali, terör örgütlerini uzak tutma adına yararlı bir unsur olabilecektir. Terör örgütlerine yönelik oluşturulması gereken siber caydırıcılığın, sağlam bir savunma ve etkili bir karşılık imkanı bulundurması gerekmektedir. Bu noktadaki herhangi bir zaaf veya ifade edilen/beklenen karşılığın içinin doldurulamaması ciddi bir güvenirlik soruna yol açabilecektir. Bu nedenle siber imkanın, devlet-dışı aktör kimliğine sahip ve bu mecrada da asimetrik strateji ortaya koyan terör örgütlerinin özelliklerine göre belirlenmesi gerekmektedir. Ayrıca caydırıcılık mesajının örgütlere başarılı şekilde doğrudan iletilmesi en önemli unsurlardandır. Eklemek gerekir ki eğer caydırıcılık stratejisinin başarısı oluşturulan imaj sayesinde saldırıya maruz kalmamak üzerinden değerlendirilirse, terör örgütlerin durumu tartışmaya açık bir konudur. Her ne kadar devletin siber gücü, terör örgütlerinin niyetlerinden vazgeçmeleri veya farklı yollar bulmak için beklemelerine neden olsa da tamamen etkili olacağını ileri sürmek imkansızdır. Devletlerin aksine terör örgütleri için saldırı başarısızlığı veya karşı saldırının yıkıcılığı kimi zaman anlam ifade etmemektedir. Yine de devletlerin terör örgütlerinin siber alandaki etkinliklerini, sahip oldukları alt yapıyı ve üyelerinin ayak izlerini izlemeleri eylemlere hazırlıklı olmaları ve ani karşılıkla cevap vermeleri olasılığını artıracaktır. Devletler siber alandaki açıklarını kapattıkça ve güçlerini artırdıkça, terör örgütlerinin bile hedefleri olmaktan çıkabilmektedirler. Terör örgütleri fırsat buldukça hedef toplumun bilgisayar ağ ve sistemlerine sızma, yerleşme veya bozma girişimleri yapmaktadırlar. Bu örgütlerin imkanları geliştikçe, dış yardım aldıkça ve teknik bilgiye sahip üyelerinin sayısı arttıkça siber alanda daha etkin olacaklarını, daha çok kazanç elde edeceklerini ve daha ciddi saldırılar düzenleyeceklerini beklemek gerekmektedir. Bu nedenle terör örgütlerinin amaçlarına hizmet edecek siber kabiliyetleriyle mücadele bir ulusal güvenlik meselesi olarak görülmelidir. Terör örgütlerinin siber alanda nasıl, ne zaman, nereye, hangi kimlikle ve yöntemle saldırı yapacaklarını belirlemenin oldukça zor olması bu kapsamdaki mücadeleyi daha meşakkatli bir iş haline getirse de ulusal siber imkânların artırılması ve caydırıcılık stratejisinin uygulanması bir çözüm yolu olacaktır. Günümüze kadar terör örgütlerinin çeşitli zamanlarda siber saldırıları gerçekleşmiş olsa da başa çıkılmaz ve günlük yaşamı tamamen felç edebilen eylemleri gerçekleşmemiştir. Siber terörizm tartışmaları içinde oldukça korkulan senaryolar mevcuttur. Şüphesiz ki terör örgütleri daha ses getirici eylemler yapma arayışındadırlar ve bu doğrultuda da kapasitelerini yükseltme arayışındadırlar. Enerji iletim hatları, temiz su depolama ve dağıtım sistemleri, kent sinyalizasyon sistemleri, bankacılık sistemleri veya askeri silah sistemleri izleyen yıllarda teröristlerin daha net siber saldırı hedefi haline gelecektir. Bu nedenle devletlerin, siber caydırıcılık kapasitelerini maksimumuma çekmek zorundadırlar.