Journal of Information Systems and Management Research
Bilişim Sistemleri ve Yönetim Araştırmaları Dergisi

http://dergipark.gov.tr/jismar

Research Article / Araştırma Makalesi

Can Law Deter in Cyberspace? Türkiye's Experience in the Context of the Turkish Penal Code

Mehmet Onur ÖZER*[a], Mehmet KAHRAMAN [b]

[a,*] *Unıversity of Missouri, Truman School of Government and Public Affairs, Political Science, Columbia, 65211, UNITED STATES of AMERICA*
[b] *Hatay Mustafa Kemal University, Faculty of Economical and Administrative Sciences, Political Science and Public Administration, Hatay, 31060, TÜRKİYE*

ARTICLE INFO

Received: 09.05.2025
Accepted: 18.06.2025

Keywords: Cyberspace, cyber security, cyber deterrence, Turkish Penal Code

Corresponding Authors
e-mail: ozermehmetonur@gmail.com

ABSTRACT

The widespread use of cyberspace has significantly transformed the concept of security, introducing complex and novel threats to both individuals and states. This article explores the idea of deterrence in cyberspace, particularly focusing on its legal dimensions within Türkiye's regulatory framework. It starts by tracing the historical shift in security from physical protection to cyber defence and discusses how the digital domain, now regarded as the fifth domain of warfare, presents unique challenges to traditional deterrence models. Drawing on theoretical frameworks, particularly those proposed by Libicki and Nye, the article examines the feasibility of cyber deterrence along with the challenges posed by attribution, asymmetry, and cost dynamics. It further investigates the role of legal deterrence, emphasizing that effective deterrence in cyberspace requires more than just severe penalties; it also depends on the certainty, promptness, and enforceability of legal consequences. The article reviews Türkiye's legal and institutional responses, from early reforms to the Penal Code to contemporary laws aligned with international conventions like the Budapest Convention. Despite Türkiye's significant progress in regulating cybercrime, practices such as the Postponement of the Announcement of the Verdict (HAGB) and effective remorse reductions pose key weaknesses that undermine the deterrent capacity of the legal system. The study concludes by asserting the importance of coherent national legislation, international cooperation, and the consistent application of legal norms to establish a strong deterrent framework in cyberspace. This article is derived from the doctoral dissertation titled "Digitalization and Cybersecurity Based on National and International Security Policies: A Legal and Administrative Assessment" defended in 2023 at Hatay Mustafa Kemal University, Institute of Social Sciences, Department of Political Science and Public Administration.

DOI: 10.59940/jismar.1695163

Hukuk Siber Uzayda Caydırıcı Olabilir mi? Türk Ceza Kanunu Bağlamında Türkiye'nin Deneyimi

MAKALE BİLGİSİ

Alınma: 09.05.2025
Kabul: 18.06.2025

Anahtar Kelimeler*: Siber uzay, siber güvenlik, siber caydırıcılık, Türk Ceza Kanunu*

ÖZET

Siber uzayın yaygın kullanımı, güvenlik kavramını önemli ölçüde dönüştürerek hem bireyler hem de devletler için karmaşık ve yeni tehditleri beraberinde getirmiştir. Bu makale, özellikle Türkiye'de siber uzayın yasal olarak düzenlenmesi bağlamında caydırıcılık konusunu incelemektedir. Fiziksel korumadan siber savunmaya doğru güvenliğin tarihsel dönüşümünü ele alarak başlayan çalışma, dijital alanın artık savaşın beşinci boyutu olarak kabul edilmesiyle geleneksel caydırıcılık modelleri açısından oluşturduğu zorlukları tartışmaktadır. Libicki ve Nye tarafından önerilen teorik çerçevelerden hareketle, makalede siber caydırıcılığın uygulanabilirliği; atfedilebilirlik, asimetri ve maliyet dinamikleri gibi sorunlar çerçevesinde ele alınmaktadır. Ayrıca hukuki caydırıcılığın rolü incelenmekte ve siber uzayda etkili bir caydırıcılığın yalnızca ağır yaptırımlarla değil; aynı zamanda hukuki sonuçların kesinliği, zamanında uygulanabilirliği ve icra edilebilirliği ile mümkün olabileceği vurgulanmaktadır. Makale, Türkiye'nin erken dönem

*Sorumlu Yazar
e-posta: ozermehmetonur@gmail.com

reformlardan başlayarak Ceza Kanunu ile Budapeşte Sözleşmesi gibi uluslararası düzenlemelere uyumlu çağdaş kanunlara uzanan hukuki ve kurumsal tepkilerini değerlendirmektedir. Türkiye, siber suçların düzenlenmesi konusunda önemli ilerlemeler kaydetmiş olsa da hükmün açıklanmasının geri bırakılması (HAGB) ve etkin pişmanlık gibi uygulamalar, hukuki sistemin caydırıcılık kapasitesini zayıflatan temel sorunlar arasında yer almaktadır. Çalışma, siber uzayda güçlü bir caydırıcılık çerçevesi oluşturmak için tutarlı ulusal mevzuat, uluslararası iş birliği ve hukuki normların istikrarlı şekilde uygulanmasının önemine dikkat çekerek son bulmaktadır. Bu makale 2023 yılında Hatay Mustafa Kemal Üniversitesi, Sosyal Bilimler Enstitüsü, Siyaset Bilimi ve Kamu Yönetimi Ana Bilim Dalında savunulan "Ulusal ve Uluslararası Güvenlik Politikaları Temelinde Dijitalleşme ve Siber Güvenlik: Hukuksal ve Yönetsel Bir Değerlendirme" başlıklı doktora tezinden türetilmiştir.

DOI: 10.59940/jismar.1695163

1. INTRODUCTION (GİRİŞ)

The concept and perception of security have evolved throughout history according to the social, economic, and political conditions of the era in which humanity has lived. Before the emergence of the first cities, the perception of security was based primarily on protection from natural disasters and wild animals in the natural environment. However, with the rise of human communities and the formation of the first cities, driven by the tendency of people to live together, this perception evolved from a struggle against nature to one based on human interactions. The concept of security, like many other concepts in the social sciences, is one of the contested notions over which no consensus has been reached. The common point among studies on security is that it refers to freedom from threats to fundamental values, both at the individual and societal levels. However, where these studies diverge is the issue of what basis the analysis should rest on [1]. In different regions of the world, struggles among communities for various reasons evolved into inter-state conflicts with the emergence of the first states, and the notion of security began to be addressed on a much broader scale. The rise of nation-states brought the concept of security into sharp focus at national and international levels. Each era's political and economic conditions and consequences have led to semantic shifts in understanding security.

In this context, security has been perceived differently in various historical periods: as national security in the context of military threats between states following the First and Second World Wars, as strategic balances and nuclear deterrence during the Cold War, and as a fight against terrorism after the September 11, 2001 attacks [2]. The significance of technology in ensuring national and international security became even clearer during the two world wars of the twentieth century and the long-standing Cold War between the United States and the Soviet Union. These historical periods demonstrated that technological superiority is far more critical than traditional manpower [3].

With the widespread use of internet technologies in the 21st century, technology has become an indispensable part of daily life. Today, people can conduct banking operations, commerce, and shopping online. Many electronic devices we use at home such as computers, phones, and various digital appliances can also be controlled through internet technology. This shift has given rise to new and distinct security threats. In this regard, through their extensive use of technology, individuals and states generate security threats that states must address.

With the increasing use of information technologies in almost every field, a new virtual realm called "cyberspace", or the "cyber domain" has emerged. In recent years, ensuring this domain's security has become a priority for states and technology-developing private companies. As this artificial digital environment has permeated every aspect of life, its use has become unavoidable and indispensable at both the individual and state levels. As individuals integrate technology into every aspect of their lives and states, digitize many bureaucratic services, and adapt to technology across various domains, new security threats have emerged. The concept of cybersecurity has thus arisen in response to these growing threats. It represents an effort to keep pace with digitalization and ensure security within cyberspace which is a realm that remains relatively new and highly complex, especially for states.

The extensive reach of cyberspace into nearly all aspects of life, the increased use of computer and internet technologies, and the fact that information sharing occurs in digital environments have collectively introduced new security threats. These threats in cyberspace not only individually endanger people, particularly in terms of the security of personal data, but also pose risks to national security through the potential for cyberattacks targeting the operating systems of critical infrastructure within states. As a result, the concept of security has undergone a significant transformation. With cyberspace now recognized as the fifth domain of warfare alongside land, air, sea, and space, security has taken on a new dimension. States and international organizations are

now keenly aware of the importance of securing this artificial domain and are actively developing security policies to address its challenges.

This awareness has not only encouraged states to develop new security policies to address the challenges in cyberspace but also pushed them to develop new technologies to fight against the threats in this new realm. States have started building new offense and defense capabilities to create deterrence in cyberspace. However, even though states have been building these capabilities actively, the complexity of cyberspace threats has grown drastically. Creating a legal framework to regulate this new domain has also become necessary for states. Having defense and offense capabilities in cyberspace could create deterrence for states. Are those capabilities strong enough deterrents to prevent a cyber-attack before it happens? How about the law? Can it deter in cyberspace? This article will focus on creating legal frameworks to regulate cyberspace as a deterrence system by evaluating Türkiye's experience.

2. WHAT IS "DETERRENCE" IN CYBERSPACE? *(SIBER UZAYDA CAYDIRICILIK NEDİR?)*

The concept of deterrence became a significant reality, particularly during the Cold War era, with the emergence of nuclear deterrence as a balancing factor in the arms race between the United States (U.S.) and the Soviet Union (USSR). The concept of nuclear deterrence has not lost its significance in the new world order that emerged after the collapse of the USSR. However, it is fair to say that it has moved away from the kind of "balance of terror" seen during the Cuban Missile Crisis in 1962, in which Türkiye also played a key role. In recent years, many researchers have argued that cyber threats define the 21st century, and these threats are poised to replace nuclear weapons in terms of their strategic importance.

Deterrence theory refers to the idea that an adversary's potential attack can be prevented by convincing them that such an action would either have no chance of success or would result in unacceptable costs, especially when measured in terms of cost-benefit analysis. Therefore, the capacity to carry out a retaliatory response to a potential attack is critically important [4]. However, whether states can achieve a deterrent power in cyberspace through conventional capabilities remains debatable.

Martin Libicki (2009) argues that cyber deterrence fundamentally differs from nuclear deterrence, making it less effective as a policy tool. While nuclear deterrence relies on symmetry, where adversaries understand each other's capabilities and consequences, cyber operations often lack this clarity. In nuclear strategy, mutual awareness enables rational cost-benefit analysis, and the threat of catastrophic retaliation discourages attacks. Cyberspace, by contrast, obscures attribution and scale, weakening the logic of predictable deterrence. Cyber deterrence, however, diverges at this point. In cyberspace, it may not be possible to identify in advance where the threat is coming from or determine the actors involved in a potential cyberattack. Cyberspace is an environment where states, non-state actors, and sometimes even individuals can effectively operate. Thus, a large-scale cyberattack may originate from a single state, a non-state actor, or a coalition of multiple actors, making attribution and response far more complex [5].

Based on the data obtained during the period of nuclear tension between the United States and the Soviet Union throughout the Cold War, it is possible to have cyber deterrence. In this context, Libicki poses three core and six supporting questions highlighting the differences between nuclear and cyber deterrence. The first core question he asks is: "*Do we know who did it?*" [5]. This question is crucial because in the concept of deterrence, particularly when it comes to retaliation, it is essential to know who launched the attack and against whom a response should be directed. From this perspective, it is often extremely difficult to identify the source of cyber-attacks in cyberspace, which stands out as one of the main factors that makes cyber deterrence problematic.

The other two core questions Libicki poses are: "Can the adversary's assets be held at risk?" and "Can this be repeated?" [5]. Deterrence becomes possible when a potential attack can be prevented through the threat of retaliation before the aggressor acts. Therefore, if a party planning an attack knows that a retaliatory response could put its assets at risk and that the defending side can repeat such retaliation, it may decide not to proceed.

If the damage expected in return outweighs the anticipated harm inflicted by the attack, the attacker will realize that the costs outweigh the benefits, making the attack irrational. In this sense, for cyber deterrence to be credible, the defender must be able to retaliate and repeat that retaliation if necessary.

The other six supporting questions posed by Libicki are as follows:

1. *If retaliation is not a deterrent, can it at least disarm the adversary?*
2. *Will third parties become involved in the conflict?*

3. *Does the retaliation send the right message to our side?*
4. *Do we have a limit to our response?*
5. *Can we avoid escalation?*
6. *Is it worth it for the attacker to respond or launch an attack?* [5]

These are the questions Libicki suggests should be asked in retaliation against a potential cyberattack. When evaluated, it becomes clear that these questions are not fundamentally different from those posed in conventional deterrence. However, what sets cyber deterrence apart is that the cost of conducting a cyberattack is generally much lower than that of a conventional attack, and its effects are quite different from those of a nuclear strike. These differences position the concept of cyber deterrence in a distinct category.

Like Libicki, Joseph Nye (2011) emphasizes that there are significant differences between cyber technology and nuclear technology [3]. Libicki highlights these differences by stating that the damage or disconnection of a cyber system can inflict massive economic harm, while to underscore the devastating effects of nuclear war, he notes that a large-scale nuclear conflict could return humanity to the Stone Age [5]. Unlike nuclear threats, cyber threats are not clearly identifiable. Therefore, deterrence in cyberspace is a highly complex phenomenon and not limited to retaliation alone. The views on deterrence that emerged during the Cold War when the nuclear arms race intensified were relatively simple, centering on the idea that deterrence depended on the ability to retaliate against a nuclear strike.

During the Cold War, retaliatory capacity was the core of the deterrence concept. However, later studies and theories concluded that deterrence, especially in the context of the use of power, is far more complex than originally conceived. Moreover, conventional military forces, clear policy declarations, changes in alert levels, and troop movements supported nuclear deterrence [3].

According to Joseph Nye, the view held by some researchers that deterrence does not work in cyberspace due to its nature is misguided and overly simplistic. Although cyber deterrence may lack the robustness of traditional deterrence, it persists, particularly when considering reciprocity and restraint in interstate relations. In the face of an attack with an uncertain origin, governments may suddenly find themselves caught in a web of interconnected relationships that produce unintended consequences. For instance, during the Cold War, there was a relatively straightforward military dependency between the United States and the Soviet Union. In contrast, today, the United States, China, and other countries exist within complex, overlapping networks. Thus, a large-scale cyberattack that harms the U.S. economy could also cause significant losses for China. The reverse is equally possible. China could be negatively affected by disruptions to interconnected systems that damage its interests [3]. Nye strongly emphasizes the cost advantages of cyberattacks in cyberspace. In contrast to traditional domains of warfare, where achieving dominance and control through conventional military power is highly costly, cyberspace presents a cost-effective environment. This environment allows non-state actors and states with limited conventional capabilities to operate effectively. Nye also argues that, in cyberspace, superiority is more likely to be achieved through offense rather than defence [6, 3].

As highlighted earlier, the technological developments since the 2000s and the advancements in internet technologies have made not only individuals but also states and non-state actors as integral parts of cyberspace. The complexity of cyberspace makes it extremely difficult to detect cyberattacks. Additionally, determining the intent behind such attacks is another significant challenge. In this context, the principle of proportionality becomes increasingly complicated, especially when the source of an attack is unknown. It is often difficult (if not impossible) to determine the level of a cyberattack, whether it was carried out by a state actor, a non-state actor, or an individual [6]. As a result, it becomes very difficult to determine the appropriate nature of the response. If the response does not comply with the principle of proportionality or is directed at the wrong party, the consequences could escalate into an armed conflict.

The uncertainty surrounding attribution and capacity in cyberattacks makes the concept of deterrence in cyberspace both highly complex and sensitive. The logic of deterrence rests on the idea that a potential attacker refrains from acting due to fear of the likely consequences of a retaliatory response based on the perceived capabilities and capacities of the defender. However, the uncertainty and complexity of cyberspace raise serious questions about the feasibility of deterrence in this domain [5].

Cyber deterrence has emerged as states increasingly use cyberspace, particularly for managing critical infrastructures. The issue of securing critical infrastructure in cyberspace, especially given the potentially severe consequences of a possible cyberattack, has become a key national security concern. The fact that critical infrastructures such as

transportation, energy, communications, finance, industry, and health are managed through SCADA (Supervisory Control and Data Acquisition) systems makes these infrastructures vulnerable to potential cyberattacks.

While each state defines critical infrastructures differently, systems whose disruption by a potential attack could threaten national security, hinder vital societal functions, or bring economic activity to a standstill are usually the general description of critical infrastructure structures. The United States defines critical infrastructures as physical or virtual systems so vital that their incapacitation or destruction would have a debilitating impact on physical or economic security or public health [7].

Türkiye defines critical infrastructures based on a regulation issued by the Ministry of Transport, Maritime Affairs, and Communications. In 2013 [8] as “infrastructures that contain information or industrial control systems where the confidentiality, integrity, or availability of processed information, if compromised, could lead to loss of life, large-scale economic damage, national security vulnerabilities, or disruption of public order” [8]. Additionally, in Türkiye’s 2020–2023 National Cybersecurity Strategy and Action Plan, published by the Ministry of Transport and Infrastructure, the designated critical infrastructure sectors are listed as Electronic Communications, Energy, Finance, Transportation, Water Management, and Critical Public Services [9].

The cyber-attacks in Estonia in 2007 and the "Stuxnet Attack" in Iran in 2010 increased the importance of deterrence capabilities for states in cyberspace. Cyberattacks in Estonia were a cornerstone for deterrence studies in cyberspace. Following these large-scale cyberattacks against Estonia in 2007, interest in cyber deterrence and related studies increased significantly both at the level of academic research and in the form of state-level measures and responses. Although the perpetrators and exact origin of the attacks were never definitively identified, it was widely claimed that Russia was behind them [10]. The attacks, which lasted for three weeks, rendered the websites and systems of the presidency, parliament, ministries, political parties, major newspapers, banks, and companies managing inter-institutional communication inoperable, creating a full-blown digital crisis in the country [11]. This massive cyberattack on Estonia caused widespread disruption of services and brought inter-agency communication to a near halt. Just one year later, similar cyberattacks were launched against Georgia, reportedly again by Russia, and produced comparable effects [12]

In 2010, a cyberattack allegedly carried out by the United States with assistance from Israel targeted Iran’s Natanz nuclear facility near Isfahan. The attack reportedly disrupted Iran’s uranium enrichment operations by destroying almost 1,000 centrifuges and even caused the reactors to function dangerously uncontrolled. This attack used a virus called Stuxnet, which has since entered the literature as the "Stuxnet Attack" [13, 14].

2.1. Deterrence in Cyberspace in the Context of Laws and Regulations *(Hukuk ve Mevzuat Bağlamında Siber Uzayda Caydırıcılık)*

The complex nature of cyberspace not only makes it difficult for states to maintain deterrent capabilities in this artificial domain in terms of national security but also complicates the establishment of legal deterrence through the regulation of cyberspace to prevent potential criminal activities. In legal discourse, experts discuss deterrence as an extension of criminal law, and domestic and international literature offers various theories on this issue.

In general, deterrence in the fight against crime is evaluated by the nature of the punishment imposed for a given offense. At this point, legal deterrence is often understood as the deterrent effect of punishment. While the idea that effective deterrence comes from harsh penalties is widespread, legal deterrence should not be viewed solely in terms of punishment severity. It must also be examined in connection with the overall structure and functioning of a country's criminal justice system [15]. Therefore, legal deterrence aimed at preventing crimes in cyberspace through its legal regulation depends on the precise definition of offenses and penalties in law and, more importantly, on their enforceability.

For the criminal justice system to have a preventive and deterrent effect against offenses, certain principles must be in place regarding the enforceability of punishments for clearly defined crimes in law. These principles are certainty, swiftness, and severity of punishment. The principle of certainty means that everyone is judged equally before the law and that if an individual commits a crime, the corresponding punishment will inevitably be applied sooner or later. The principle of swiftness refers to the prompt apprehension of offenders after a crime has occurred, followed by timely investigation, prosecution, and adjudication, leading to the finalization of the sentence. The severity of punishment means that the penalty imposed must be proportionate to the offense committed. If these three principles are absent, punishments lose their deterrent effect [16].

2.2. Deterrence in Cyberspace in International Legal Context *(Uluslararası Hukuk Bağlamında Siber Uzayda Caydırıcılık)*

Cyberspace has become a fundamental domain for most states. In terms of competition, nations seek to deter adversaries from malicious cyber activities through threats of retaliation or denial of benefits. However, creating a deterrence system in cyberspace requires unique legal and practical solutions. Unlike the conventional understanding of deterrence issues such as military attacks, cyber incidents often create a complexity that differentiates the line between crime, espionage, and armed aggression, challenging states to respond within the bounds of international law. Therefore, the international community has gradually recognized that existing international legal norms should be extended to cyberspace.

The international community hasn't been able to create a globally accepted treaty that regulates cyberspace. However, existing international law provides a normative framework for states that cyber deterrence strategies must operate. While no single treaty is dedicated solely to cyber operations by states, various existing legal frameworks regulate state actions in cyberspace. These include the UN Charter's rules on the prohibition of force and the right to self-defence, core international law principles such as sovereignty and non-intervention, and specific agreements like the Budapest Convention on cybercrime. Additionally, non-binding instruments and expert manuals have helped establish norms and guide state behaviour in the digital domain.

2.2.1. International Legal Frameworks Relevant to Cyber Deterrence *(Siber Caydırıcılıkla İlgili Uluslararası Hukuki Çerçeveler)*

Several international legal norms and instruments are relevant to cyber deterrence. Legally binding instruments such as the UN Charter establish core rules prohibiting using force that also applies to cyber operations. At the same time, customary international law addresses areas not covered explicitly, including sovereignty and state responsibility. Additionally, non-binding initiatives like the UN Group of Governmental Experts (GGE) norms and expert analyses like the Tallinn Manual offer additional guidance on appropriate conduct. Collectively, these frameworks create a structured environment that informs how states design cyber deterrence strategies by clarifying unacceptable behaviours and legitimate responses in cyberspace.

Although no single treaty comprehensively regulates state behaviour in cyberspace, several binding and non-binding legal instruments have emerged to shape expectations, responsibilities, and consequences surrounding cyber operations. Together, these frameworks establish the normative foundation upon which states design and implement cyber deterrence strategies.

This framework's core is the UN Charter [17], which applies fully to cyberspace. Article 2(4) prohibits the use of force against the territorial integrity or political independence of any state. In contrast, Article 51 affirms the inherent right of self-defence in the event of an "armed attack." These provisions form the legal bedrock for deterrence by punishment in cyberspace: a sufficiently severe cyber operation—causing death, injury, or significant physical destruction could be interpreted as a use of force, thus justifying a forcible response [17]. However, the Charter offers limited utility for deterring most cyber activities below the armed conflict threshold, creating persistent challenges in addressing so-called "grey zone" operations [18].

Customary international law fills some of these regulatory gaps. The principles of sovereignty**,** non-intervention**,** and state responsibility apply to cyberspace and help delineate acceptable conduct. Sovereignty protects a state’s control over its cyber infrastructure, while non-intervention prohibits coercive interference in domestic affairs, such as election manipulation or fomenting unrest [19]. The doctrine of state responsibility, codified in the Articles on State Responsibility**,** enables using proportionate countermeasures in response to internationally wrongful cyber acts [20]. These principles support deterrence by norms**,** emphasizing that breaches of international obligations, if attributable to a state, can prompt diplomatic, legal, or cyber retaliatory measures. However, the difficulty of attribution remains a critical weakness in operationalizing these norms as effective deterrents [21].

International Humanitarian Law (IHL) becomes applicable in armed conflict. Instruments such as the Geneva Conventions and the Hague Regulations impose obligations to respect the principles of distinction, proportionality, humanity, and necessity, even in cyber warfare [22]. IHL constrains cyber operations targeting civilian infrastructure and reinforces the notion that cyberspace is not exempt from wartime legal constraints. While IHL does little to deter peacetime activities, it plays a vital role in preventing escalatory cyber actions during conflicts by classifying certain cyberattacks as potential war crimes.

On the criminal enforcement side, the Budapest Convention on Cybercrime (2001) strengthens

deterrence through legal accountability. By mandating the criminalization of specific cyber offenses and facilitating international cooperation in cyber investigations, the Convention contributes to deterrence by law enforcement, particularly against non-state actors and proxy groups [23]. Nevertheless, the Convention's normative reach is limited by the absence of key cyber powers such as Russia and China, who reject what they perceive as Western-centric legal standards [24].

A range of non-binding but influential instruments also shape state behaviour in cyberspace. The UN Group of Governmental Experts (GGE) and Open-Ended Working Group (OEWG) processes have produced voluntary norms for responsible state conduct, including commitments to refrain from targeting critical infrastructure or emergency response teams during peacetime [24, 25]. These norms serve as a basis for deterrence through shared expectations**,** enabling collective condemnation and sanctions in response to violations.

The Tallinn Manual 2.0, an expert commentary that analyzes how existing international law applies to cyber operations in peacetime and wartime, provides further interpretive guidance. Although not a binding legal instrument, it has significantly influenced state practice and legal doctrine [18]. The Manual helps states articulate "red lines" by elaborating on when cyber operations might constitute uses of force or armed attacks, thus supporting more credible deterrence postures grounded in legal reasoning.

Lastly, regional and multistakeholder initiatives, including NATO's cyber policy, the EU's Cyber Diplomacy Toolbox**,** and global norms like the Paris Call for Trust and Security in Cyberspace**,** bolster deterrence by signalling collective responses and enhancing resilience [27, 28]. NATO's declaration that a major cyberattack could trigger Article 5 collective defence obligations adds weight to deterrence by alliance commitments**.** Meanwhile, EU-led sanctions and private-sector engagement increase the cost of cyber aggression through diplomatic, economic, and reputational consequences.

3. TÜRKİYE'S EXPERIENCE IN REGULATING CYBERSPACE *(SIBER UZAYIN DÜZENLENMESINDE TÜRKIYE'NIN DENEYIMI)*

Since the early 1990s, Türkiye has undertaken numerous legal and administrative measures to address potential cyber security threats. Although various actors implemented many of these regulations independently, they still represent necessary steps toward ensuring cyberspace security. While the legal regulation of this field through various laws, regulations, circulars, and communiqués has sometimes created inconsistencies, the legal measures introduced remain highly significant in establishing deterrence against potential threats that may arise in cyberspace.

No single law in Türkiye comprehensively regulates crimes committed in cyberspace. Instead, incorporating relevant provisions into existing laws has addressed offenses in the field of information technologies [29]. The first legal regulation regarding cyber-related crimes was introduced on June 6, 1991, through the "Law No. 3756 on the Amendment of Certain Articles of the Turkish Penal Code." By the early 2000s, with the increasing use of cyberspace, Türkiye began to take more concrete and serious steps toward ensuring cybersecurity and establishing deterrence in cyberspace. In this context, a far more comprehensive regulation than the 1991 amendment was enacted in 2004 when the concept of cybercrime was legally defined. Under the heading "Crimes in the Field of Information Technology" Chapter Ten of the Turkish Penal Code No. 5237 included significant legal provisions, particularly focused on offenses committed in the cyber domain.

In Türkiye, the most comprehensive legal regulation of the Internet was enacted in 2007 through Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed Through Such Publications [30]. Another significant legal regulation to ensure cyberspace security was the Electronic Communications Law No. 5809**,** adopted in 2008 [31]. This law intends to prevent unfair competition in the electronic communications sector and to ensure that services in this field are delivered actively and effectively. It was an important step toward safeguarding individuals' freedom and security of communication in cyberspace**,** especially in protecting fundamental rights and freedoms.

In addition to the Electronic Communications Law, another critical piece of legislation for ensuring cybersecurity was Law No. 6698 on the Protection of Personal Data**,** which was submitted to parliament in the same year [32]. Although it took a long time, it was enacted and published on April 7, 2016**.** Today, with the widespread use of e-government applications and the storage of personal data in digital environments across nearly all public institutions, not to mention digital storage on shopping websites and social media platforms, this law serves as an essential deterrent against malicious actors**,** particularly in terms of protecting the privacy of personal life.

3.1. Turkish Penal Code and Deterrence in Cyberspace *(Türk Ceza Kanunu ve Siber Uzayda Caydırıcılık)*

Although several laws regulate cyberspace in Türkiye, the Turkish Penal Code is a key legal framework that creates deterrence. As highlighted earlier, Türkiye is one of the countries that recognized the importance of cyberspace and its security at an early stage and took legislative action accordingly. Aware of the issue's significance as early as the 1990s, Türkiye introduced its first regulation on crimes committed in cyberspace on June 6, 1991, through Law No. 3756 on the Amendment of Certain Articles of the Turkish Penal Code No. 765. Article 20 of this law, titled "Crimes in the Field of Information Technology," made it a criminal offense to unlawfully obtain, use, transmit, or reproduce programs, data, or other elements from an automated data processing system, especially if done with the intent to harm others. The law also set forth the provisions for penalties related to such offenses [33].

In 2004, a far more comprehensive regulation than the 1991 amendment was introduced when the concept of cybercrime was formally defined by law. Under the title "Crimes in the Field of Information Technology" in Chapter Ten of the Turkish Penal Code No. 5237, provisions were made concerning unauthorized access to information systems, obstruction or disruption of systems, deletion or alteration of data, and the misuse of bank and credit cards. These offenses are independently regulated under Articles 243, 244, and 245 of the Turkish Penal Code [34]. Additionally, Türkiye became a party to the Council of Europe Convention on Cybercrime, signed in Budapest in 2001 (commonly referred to as the Budapest Convention) after being ratified by the Grand National Assembly of Türkiye (TBMM) in 2012. Following its ratification, Türkiye amended the Turkish Penal Code to align with the provisions of this international agreement.

Article 20 of Law No. 3756 added a new "Crimes in the Field of Information Technology" section to the Turkish Penal Code No. 765 as "Chapter Eleven" to follow Article 525. Articles 21, 22, 23, and 24 of the same law also introduced Articles 525a, 525b, 525c, and 525d, which were appended to the Penal Code under the same new chapter.

These articles are particularly significant as they represent the first legislative amendments made in Türkiye to ensure cyberspace security. Accordingly, the following provisions are set forth as they appear in the law:

Article 525a:
"Any person who unlawfully obtains programs, data, or any other elements from a system that processes information automatically shall be sentenced to imprisonment from one to three years and a heavy fine ranging from one million to fifteen million Turkish lira. The same penalty shall also apply to any person who uses, transmits, or reproduces a program, data, or any other element in a system that processes information automatically, intending to cause harm to another." [35].

Article 525b:
"Any person who, with the intent to cause harm to another or to obtain benefit for themselves or others, partially or completely destroys, alters, deletes, obstructs the operation of, or causes the incorrect functioning of a system that processes information automatically, or its data or any other element, shall be sentenced to imprisonment from two to six years and a heavy fine ranging from five million to fifty million Turkish lira. Any person who unlawfully obtains a benefit for themselves or others by using a system that processes information automatically shall be sentenced to imprisonment from one to five years and a heavy fine ranging from two million to twenty million Turkish lira." [35].

Article 525c:
"Any person who, for the purpose of creating a forged document to be used as legal evidence, inputs data or other elements into a system that processes information automatically or alters existing data or elements shall be sentenced to imprisonment from one to three years. Those knowingly using the forged or altered data shall be imprisoned for six months to two years." [35].

The amendments to the Turkish Penal Code (TCK) by Law No. 3756 gained further significance in 1993 when Türkiye was introduced to the Internet through initiatives led by Middle East Technical University (METU). In 1991, when the law was enacted, individual computer use in Türkiye was still very limited. Therefore, adopting a legal regulation when internet technology had not yet begun to be widely used aimed at creating deterrence against crimes in cyberspace should be considered a noteworthy development.

Another critical point to emphasize is that this regulation holds great significance within the scope of the principle of legality. This principle was first formulated by German criminal law scholar Anselm von Feuerbach as *"nullum crimen, nulla poena sine lege"*, translated as *"no crime, no punishment without law."* In Türkiye, the principle of legality in crimes

and punishments is guaranteed under Article 13 of the 1982 Constitution, which states:

"Fundamental rights and freedoms may be restricted only by law and solely for the reasons set forth in the relevant articles of the Constitution, without infringing upon their essence. These restrictions shall not violate the letter and spirit of the Constitution, the requirements of the democratic order of society, or the principles of the secular Republic, and shall comply with the principle of proportionality." [36]

This provision represents the constitutional embodiment of the principle of legality. Similarly, Article 38 of the Constitution, titled "Principles Relating to Offenses and Penalties," further reinforces this principle by stating, *"No one shall be punished for any act that was not defined as a crime by law at the time it was committed; nor shall anyone be subjected to a heavier penalty than the one prescribed by law at the time the offense was committed. The provisions of the above paragraph shall also apply to statutes of limitations for offenses and penalties, as well as to the legal consequences of criminal convictions. Criminal penalties and security measures in lieu of penalties may only be imposed by law."* [36]

Therefore, the 1991 amendment to the Turkish Penal Code essentially paved the way for acts committed in cyberspace to be legally recognized as crimes**,** thereby enabling the initiation of investigation and prosecution processes related to such actions.

Instead of terms such as "computer" or "information technology," the law used the phrase "a system that processes information automatically." Considering that the widespread use of computer and software technologies had not yet begun at the time, this definition was intended to encompass all technological devices**,** from the simplest data processing systems to the most advanced computers of the period. Through this regulation, the law established a legal basis for acts committed using or through such devices, assigning them a material and legal meaning. At the time, this regulation was enacted when computer use in Türkiye was still relatively new, and it is true that threats in the context of cybersecurity were quite limited. Therefore, no specific definition was provided regarding the nature of the offense in the regulation. However, with the advent of the internet and its integration into daily life, the concept of crimes committed in cyberspace began to take on real meaning. Thus, this regulation marked an important step for Türkiye in establishing a legal basis for such crimes.

In 2004, Law No. 5252 on the Enforcement and Implementation of the Turkish Penal Code repealed the Turkish Penal Code No. 765, which was replaced by Penal Code No. 5237**.** The new Penal Code addressed crimes committed in cyberspace much more comprehensively than the 1991 regulation. Under the title "*Crimes in the Field of Information Technology*" Chapter Ten of the Turkish Penal Code No. 5237 introduced provisions related to unauthorized access to information systems**,** obstruction or disruption of systems**,** deletion or alteration of data**,** and the misuse of bank and credit cards [37]. These offenses are independently regulated under Articles 243, 244, and 245 of the Penal Code [34].

Article 243 of the Turkish Penal Code (TCK) regulates the offense of unauthorized access to information systems. According to this article, any person who unlawfully accesses all or part of an information system is subject to up to one year of imprisonment or a judicial fine**.** The second paragraph of the same article states that if this act is committed against systems that are available for use in exchange for payment, the penalty shall be reduced by half**.** Finally, the third paragraph stipulates that if, because of this act, the data contained in the system is deleted or altered**,** the offender shall be sentenced to imprisonment from six months to two years [34].

Article 244 of the Turkish Penal Code (TCK) addresses the crimes of obstructing a system, disrupting its functioning, and deleting or altering data. Compared to Article 243, this article provides a more detailed regulation of the offense of interfering with an information system. Article 244 of the Turkish Penal Code states: (1) Any person who obstructs or disrupts the operation of an information system shall be imprisoned for one to five years. (2) Any person who corrupts, deletes, alters, renders inaccessible, inserts data into, or transfers existing data from an information system shall be imprisoned from six months to three years. (3) If the act is committed against an information system belonging to a bank, credit institution, or a public institution or organization, the penalty shall be increased by half. (4) If these acts are committed in such a way as to benefit oneself or another unjustly, and if the act does not constitute another offense, the offender shall be punished with imprisonment from six months to two years and a judicial fine of up to five thousand days." [34]. This provision regulates the offenses of obstructing, disrupting, deleting, or altering a system or its data. The purpose behind defining this offense is to ensure compliance with the "data interference" provision in Article 4 and the "system interference" provision in Article 5 of the Budapest Convention.

Article 245 of the Turkish Penal Code (TCK) regulates the offense of misuse of bank or credit cards. Under this article, acts involving the misuse of bank and credit cards are defined as a distinct crime category, aiming to prevent financial harm to banks or their customers and the unlawful acquisition of benefits through such means. According to the article, any person who uses a bank or credit card belonging to someone else without the consent of the cardholder or the person authorized to possess the card, thereby obtaining a benefit, shall be punished with imprisonment from three to six years and a judicial fine of up to five thousand days. Furthermore, anyone who produces, sells, transfers, purchases, or accepts counterfeit bank or credit cards using fake bank accounts shall be imprisoned for three to seven years and a judicial fine of up to ten thousand days. The third paragraph of this article states that if a counterfeit bank or credit card is used to obtain a benefit, and if this act does not constitute another offense that requires a more severe penalty, the offender shall be sentenced to imprisonment from four to eight years and a judicial fine of up to five thousand days [34].

With the amendment introduced in 2016, Article 245/A, titled "Prohibited Devices and Programs," was added to the section on Crimes in the Field of Information Technology in the Turkish Penal Code. This article established a significant regulation regarding the use and production of devices and software employed to commission offenses regulated under this section. According to the article: *"If a device, computer program, password, or other security code is manufactured or created exclusively for the purpose of committing the offenses outlined in this section or other crimes that can be committed using information systems as tools, any person who manufactures, imports, dispatches, transports, stores, accepts, sells, offers for sale, purchases, distributes to others, or possesses such items shall be punished with imprisonment from one to three years and a judicial fine of up to five thousand days."* [34]. With this regulation, lawmakers introduced criminal sanctions for the hardware and software tools used or produced for the commission of cybercrimes.

In the Turkish Penal Code (TCK), the regulation of cybercrimes within the scope of substantive criminal law is not limited to the section titled "Crimes in the Field of Information Technology." Although not specifically designed for cybercrimes, the Turkish Penal Code addresses offenses committed using or through information technologies in various other contexts. In particular, the entry into force of the Budapest Convention and the obligations arising from this international treaty prompted harmonization efforts in domestic law. Recognizing that traditional crimes can also be committed through information technologies, the TCK incorporates relevant provisions across several articles.

3.1.1. Articles of the Turkish Penal Code Associated with or Potentially Applicable to Crimes Committed Using Information Technologies or Through These Technologies *(Türk Ceza Kanunu'nda Bilişim Teknolojileri Kullanarak veya Bu Teknolojiler Aracılığıyla İşlenen Suçlarla İlişkilendirilen ya da İlişkilendirilebilecek Maddeler)*

In addition to Articles 243, 244, and 245, which specifically address cybercrimes under the category of information technology offenses in the Turkish Penal Code (TCK), numerous other articles are associated with or potentially applicable to crimes committed using or through information technologies. Many of these provisions were introduced or amended after the signing of the Budapest Convention as part of Türkiye 's efforts to harmonize its domestic legislation with the Convention's requirements. The relevant articles can be listed as follows:

Article 123/A – Persistent Stalking *(Added: 12/5/2022 – Law No. 7406, Article 8)*: In the first paragraph of the article, the following provision is introduced: "*Anyone who persistently follows a person physically or attempts to make contact using communication tools, information systems, or third parties in a way that causes serious discomfort to that person or makes them fear for their own or a relative's safety shall be sentenced to imprisonment from six months to two years."* [34]

This regulation considers persistent stalking not only in its physical form but also when carried out through communication tools and information systems. Although it does not provide a detailed definition of stalking via information systems, it encompasses acts of persistent harassment conducted in cyberspace that cause discomfort or create concerns for personal security.

This article was added to the TCK in 2022, reflecting the growing recognition that such behaviours increasingly occur in cyberspace and thus must be addressed through appropriate legal measures.

Article 124 – Obstruction of Communication: This article does not include specific provisions or references to information technologies or cyberspace. Nor does it clarify how or through which means the offense may be committed. Nevertheless, the article defines the offense of obstructing communication as

follows: (1) Anyone who unlawfully obstructs communication between individuals shall be imprisoned for six months to two years or a judicial fine. (2) Anyone who unlawfully obstructs communication between public institutions shall be imprisoned for one to five years. (3) If the unlawful obstruction concerns any form of media or broadcasting outlet, the penalty stated in the second paragraph shall be applied [34].

Although the article does not explicitly mention cyber or digital means, its broad wording allows for interpretation that may include acts committed via information systems, especially as cyber-based disruptions to communication become more prevalent.

Article 132 – Violation of the Confidentiality of Communication: This article sets out the criminal sanctions to be applied in cases where the confidentiality of communication between individuals is violated**,** including the recording of communication content**,** the unlawful disclosure of such content**,** and the unlawful disclosure of communications involving the person themselves**.** Given the widespread use of smartphones and the current level of internet technology, internet-based messaging, and video call applications have become the primary means of communication between individuals. Especially during the COVID-19 pandemic, when curfews restricted people from leaving their homes, internet technology became the most important communication tool, leading to the decline of traditional communication methods. In this context, it becomes evident that the relevant article of the Turkish Penal Code is directly related to the offense of violating the confidentiality of communication as it may occur in cyberspace.

Article 133 – Listening to and Recording Conversations Between Individuals: Although, as in other articles, this provision does not explicitly address the use of information technologies or the commission of such acts through digital means, cyberspace is the primary medium where such offenses are committed or can be committed today. In an era where internet technology is heavily used to communicate, listening to, recording, and disclosing private conversations between individuals increasingly occurs via internet-based platforms, making this a cyber-enabled offense in practice. Smartphones, now used by nearly everyone and always carried, serve as communication devices and tools for audio and video recording. Furthermore, as discussed in the section on cybersecurity threats, unauthorized access to networks for the purpose of illegal surveillance and recording has become a highly probable occurrence. In this context, it can be argued that the relevant article of the Turkish Penal Code is directly related to cybersecurity threats.

Article 134 – Violation of Privacy: This article of the Turkish Penal Code regulates the violation of an individual's right to privacy, specifically when such a violation is committed through the recording of images or audio and the unlawful disclosure of these recordings. The provision refers to privacy infringement by recording visual or auditory content. Still, it does not address whether this is done using information technologies or specify the platforms through which such acts occur. However, the lack of a specific reference to digital means does not prevent the application of this article to offenses committed in cyberspace. There is no legal barrier to interpreting and applying this provision to privacy violations that occur via digital or cyber platforms.

Article 135 – Unlawful Recording of Personal Data: This article of the Turkish Penal Code regulates the offense of unlawfully recording personal data. According to Article 135: (1) Any person who unlawfully records personal data shall be imprisoned for one to three years. (2) If the personal data concerns individuals' political, philosophical, or religious views; racial origins; or their unlawful moral tendencies, sexual lives, health conditions, or trade union affiliations, the penalty under the first paragraph shall be increased by half." [34]

The article does not distinguish whether the offense is committed through information technologies or by other means. However, considering that virtually all types of data, from government institutions to individual users, are now stored in digital environments, the primary medium through which this offense is likely to occur today is cyberspace, particularly through computers and digital systems. Therefore, while the article does not explicitly prescribe a penalty for committing this crime in cyberspace, there is no legal barrier to applying it to cases involving personal data theft in the digital realm.

Article 136 – Unlawful Transfer or Acquisition of Data: As with many other articles that can be associated with the security of cyberspace, this article does not address the use of digital devices or the commission of the offense through information technologies, nor does it provide any specific explanation regarding this issue. The article regulates the unlawful acquisition and transfer of personal data as follows: *"(1) Any person who unlawfully transfers, disseminates, or acquires personal data shall be sentenced to imprisonment from two to four years. (2) If the subject of the offense involves statements and*

recordings made in accordance with the fifth and sixth paragraphs of Article 236 of the Code of Criminal Procedure, the penalty shall be doubled." [34]

As can be seen, the article does not specify the tools used in committing the offense or the environment in which it is carried out. The second paragraph, which was added by an amendment in 2019, refers to statements and recordings taken from child victims during the investigation phase of the offense defined under Article 103 of the Penal Code ("Sexual Abuse of Children"), in accordance with paragraphs five and six of Article 236 of the Code of Criminal Procedure (CMK). Therefore, the "statements and recordings" referred to in the second paragraph of Article 136 pertain specifically to those obtained during investigations related to child sexual abuse cases.

Article 142/2-e – Aggravated Theft: The theft offense, addressed in Chapter Ten of the Turkish Penal Code under "Crimes Against Property," is examined under two categories: theft and aggravated (qualified) theft. According to subparagraph (e) of paragraph 2 in Article 142, if the offense is committed using information systems, the perpetrator shall be sentenced to imprisonment from five to ten years [34]. The Cyber Crimes Department of the Turkish National Police defines aggravated theft as a cybercrime involving unauthorized data acquisition from a system or during data transmission between systems through malicious software. Examples include the theft of in-game characters in online games and the unauthorized transfer of money from one bank account to another [37]. The explicit inclusion in the TCK of the offense of aggravated theft committed using information systems can be considered a preventive legal measure aimed at addressing such crimes committed in cyberspace.

Articles 213–218 – Offenses Against Public Peace: The offenses listed under the section "Crimes Against Public Peace" in the Turkish Penal Code do not explicitly address acts committed in cyberspace or through the use of information technologies. However, if these offenses are carried out via digital technologies, there is no legal obstacle to applying the relevant articles in such cases.
The relevant articles are:

- Article 213: Threat intended to cause fear and panic among the public
- Article 214: Incitement to commit a crime
- Article 215: Praising an offense or offender
- Article 216: Incitement to hatred and hostility or public denigration
- Article 217: Incitement to disobey the law
- Article 217/A: Public dissemination of misleading information

Although the offenses described above are traditionally understood as conventional crimes, each can easily be committed in digital environments. Moreover, social media platforms, now used by nearly everyone, are among the primary digital spaces where such crimes can occur. On these platforms, where each individual can act like a personal media outlet, a single post can reach massive audiences within minutes.

Therefore, the crimes addressed in Chapter Five of the Turkish Penal Code can be committed easily through such channels. In this context, clearly defined penalties for these offenses in the law can be seen as a deterrent factor. However, cyberspace's complex, vast, and borderless nature makes it increasingly difficult to identify and apprehend perpetrators of such crimes.

The borderless nature of cyberspace allows these offenses to be committed from beyond national jurisdictions. As a result, although relevant provisions exist in the Turkish Penal Code, they sometimes fail to function effectively as deterrents. For this reason, international cooperation is critical in combating cross-border cyber offenses and establishing effective deterrence mechanisms in cyberspace.

Article 226 – Obscenity: The offense of obscenity, addressed in the section "Crimes Against Public Morality" of the Turkish Penal Code, is particularly significant in cyberspace due to the ease with which this offense can be committed online. Although the article does not explicitly address the commission of the offense using or through information technologies, it does define as a criminal act the sale, rental, distribution, publication via press and media, or facilitation of the distribution of obscene images, texts, or expressions, and prescribes a prison sentence of six months to five years, depending on the method of commission.

When considered within the scope of Article 9 of the Budapest Convention, which deals with Offenses Related to Child Pornography [38], the importance of Article 226 increases. The provision criminalizes the display, reading, distribution, or provision of obscene materials in places accessible to children or directly to children. More importantly, it foresees a prison sentence of five to ten years and a judicial fine of up to five thousand days for individuals who use children, child-like representations, or persons made to look like children in the production of such materials.

Given the current capabilities of AI, deepfake, and animation technologies, the criminalization of obscene images featuring persons made to appear as

children in digital environments is a crucial measure for preventing such crimes in cyberspace. Although the explicit criminalization of virtual child pornography remains a significant gap in the law, there is no legal barrier to prosecuting such acts under the existing provisions of this regulation.

Article 228 – Providing a Place and Opportunity for Gambling: This article prescribes imprisonment from one to three years and a judicial fine of no less than two hundred days for individuals who provide a place or opportunity for gambling. The increasing use of information and internet technologies creates gambling environments in virtual spaces. has become much easier.

In 2017, an amendment was made to this article specifying that if the offense is committed through the use of information systems, the penalty shall be three to five years of imprisonment and a judicial fine of one thousand to ten thousand days. However, as emphasized earlier, the borderless nature of cyberspace makes it very difficult to apprehend individuals committing this offense.

In cases where online gambling is facilitated through websites hosted on servers located abroad, apprehension and prosecution of the offenders are impossible without international cooperation. In such instances, the most that authorities can do is restrict access to the website. Thus, even though this offense is addressed in the legislation, there is a clear need for stronger international collaboration to combat it effectively.

Articles 209–301 – Offenses Against the Symbols of State Sovereignty and the Dignity of State Institutions: This section of the Turkish Penal Code addresses offenses such as insulting the President (Article 299), denigrating the symbols of state sovereignty (Article 300), and insulting the Turkish Nation, the State of the Republic of Türkiye, or its institutions and organs (Article 301). Although these articles do not include specific provisions for cases where such offenses are committed using information technologies, there is no legal obstacle to applying these provisions when such acts occur in cyberspace. Given that these offenses can easily be committed via digital platforms, particularly on social media, these laws can also be enforced in response to online conduct.

Articles 326–339 – Offenses Against State Secrets and Espionage: This section of the Turkish Penal Code addresses offenses such as the acquisition, destruction, forgery, and disclosure of information and documents that relate to the security of the state or its domestic and foreign political interests, and which are required to be kept confidential. Given that today, most information is stored digitally and a significant portion of communication and data exchange between institutions occurs over internet-connected networks, the unauthorized acquisition of such information in virtual environments is highly likely. Although the relevant articles do not specifically reference the commission of these offenses in cyberspace or through information technologies, it is clear in the current information age that a large portion of sensitive data is stored electronically and can potentially be accessed via cyberattacks on these systems.

It is also useful to examine judicial practices and court rulings in assessing the effectiveness of cybercrime provisions in the Turkish Penal Code. However, implementing measures such as the Postponement of the Announcement of the Verdict (HAGB) and the Effective Remorse Reduction has been viewed as a major weakness in preventing cyber offenses.

The Postponement of the Announcement of the Verdict (HAGB) is regulated under Article 231 of the Criminal Procedure Code (CMK). According to paragraph 5 of the article: "*If the sentence imposed upon the defendant because of the trial for the charged crime is imprisonment of two years or less or a judicial fine, the court may decide to postpone the announcement of the verdict. The provisions regarding reconciliation remain reserved. The postponement of the announcement of the verdict means that the judgment will not have legal consequences for the defendant*." [39]

Paragraph 6 outlines the conditions for applying HAGB: "*To decide on the postponement of the announcement of the verdict: a) The defendant must not have been previously convicted of an intentional crime; b) The court must be convinced, based on the defendant's character, behaviour in court, and other personal qualities, that they are unlikely to re-offend; c) The harm caused to the victim or public due to the offense must be fully compensated by restitution, restoration, or reparation. The defendant's consent is required for the decision.*" [39]

In this context, HAGB may be applied to offenses such as:

- Unauthorized Access to Information Systems [34]
- Disruption or Destruction of Systems or Data [34]
- Misuse of Bank or Credit Cards [34]

According to Turkish Penal Code Article 245(5):

"*For the acts listed in the first paragraph, the provisions on effective remorse for crimes against property shall apply*." Thus, under Article 245(1): *"Any person who, by any means, obtains or retains another person's bank or credit card and uses it or has it used without the consent of the cardholder or authorized party, to benefit themselves or another, shall be punished with imprisonment from three to six years and a judicial fine of up to five thousand days."* [34]

If the offender fulfils the conditions set forth in Turkish Penal Code, Article 168 (Effective Remorse), a reduction in the sentence may apply. If the victim's damages are compensated during the investigation phase, the sentence may be reduced by up to two-thirds. If compensation occurs during the prosecution phase (i.e. after the case has been filed), the sentence may be reduced by up to one-half [34].

Although the cybercrime provisions of the TCK may be seen as a legal deterrent against offenses in cyberspace, HAGB and effective remorse reductions weaken this deterrent effect. These practices undermine the enforceability of penalties and diminish the dissuasive power of the legal framework regarding cyber offenses.

4. CONCLUSION and SUGESTIONS (SONUÇ ve ÖNERİLER)

As cyberspace becomes increasingly central to modern life and national security, the concept of deterrence, traditionally rooted in kinetic warfare, must be reinterpreted for the digital age. Cyberspace's characteristics, including anonymity, low cost of entry, and difficulty of attribution, challenge the classical assumptions of deterrence theory. While traditional deterrence relies heavily on the threat of retaliation and visible capabilities, cyber deterrence must also incorporate legal, normative, and institutional mechanisms.

This article has shown that legal frameworks play a critical role in cyber deterrence, particularly when retaliatory action is unfeasible or ineffective. Türkiye's legislative evolution demonstrates an early recognition of this reality, with successive reforms aimed at addressing cyber threats through criminal law. From the initial amendments in 1991 to the more structured provisions of the Turkish Penal Code (TCK) and the country's accession to the Budapest Convention, Türkiye has laid a legal foundation to define, punish, and thus deter cyber offenses.

However, the existence of legal norms alone does not ensure deterrence. The efficacy of deterrent laws depends on their consistent enforcement, the severity and proportionality of penalties, and the elimination of loopholes that undermine punishment, such as the overuse of HAGB and adequate remorse provisions. These practices, though well-intended, often reduce the dissuasive power of the law in the cyber realm, where certainty and swiftness of justice are critical.

Türkiye's experience highlights the need for integrated deterrence strategies that combine legal frameworks with technological capabilities and international collaboration in the face of rapidly evolving cyber threats. Cybersecurity cannot rely solely on reactive measures; it must be supported by proactive legal systems that deter malicious actors before they strike. As the digital domain continues to expand, the challenge for all states will be to ensure that their laws are robust on paper and effective in practice.

To enhance the deterrent effect of legal frameworks, particular attention must be paid to:

Strengthening Enforcement Mechanisms: Beyond merely having laws, the consistent and timely application of these laws is paramount. This requires well-resourced law enforcement agencies, judiciaries with specialized knowledge in cybercrime, and efficient judicial processes to ensure the swiftness of punishment.

Re-evaluating Sentencing Practices: Practices like the Postponement of the Announcement of the Verdict (HAGB) and effective remorse reductions, while aiming for rehabilitation, inadvertently diminish the perceived certainty and severity of punishment for cyber offenses. A critical review of these mechanisms is necessary to ensure they do not undermine the deterrent impact of the law, especially for crimes that can have far-reaching national security and economic consequences.

Fostering International Cooperation: Given the borderless nature of cyberspace, no single nation can effectively combat cyber threats in isolation. Türkiye's experience, particularly with online gambling and other cross-border offenses, highlights the indispensable need for robust international agreements, intelligence sharing, and collaborative law enforcement efforts to identify, apprehend, and prosecute perpetrators operating beyond national jurisdictions. Harmonization of legal standards, as seen with the Budapest Convention, remains crucial, though efforts must continue to bring key global players into consensus.

Developing Dynamic Legal Frameworks: The rapid evolution of technology, including advancements in AI and deepfake technologies, means that legal frameworks must be agile and adaptable. Laws should

be periodically reviewed and updated to address emerging cyber threats, ensuring that new forms of malicious activity are clearly defined and subject to appropriate legal sanctions.

Integrating Legal Deterrence with Broader Cybersecurity Strategies: Legal measures are just one pillar of a comprehensive cybersecurity strategy. They must be seamlessly integrated with technological defense capabilities, offensive measures for deterrence by punishment, and public awareness campaigns to foster a culture of cybersecurity. The goal is to create a layered defense where legal consequences, technological resilience, and international partnerships collectively raise the cost and risk for malicious actors, thereby creating a more formidable deterrent in the digital realm.

Ultimately, the effectiveness of cyber deterrence will not only depend on the strength of a nation's digital defenses or its capacity for retaliation but increasingly on its ability to build and enforce a credible legal infrastructure that resonates both domestically and internationally, fostering accountability and predictability in the inherently unpredictable domain of cyberspace.

REFERENCES *(KAYNAKLAR)*

[1] Baylis, J. (2008). Uluslararası İlişkilerde Güvenlik Kavramı. *Uluslararası İlişkiler*, 5(18): 69-85.

[2] Booth, K. (2007). *Theory of World Security*. University Press. https://doi.org/10.1017/CBO9780511840210

[3] Nye, J. S. (2011a). Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly*, *5*(4), 18-38.

[4] Mazarr, M. J. (2018). Understanding Deterrence. *Rand Corporation Perspective*. https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf [Accessed: April 23, 2025)

[5] Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. The Rand Corporation.

[6] Nye, J. S. (2010). Cyber Power. *Belfer Center for Science and International Affairs. https://apps.dtic.mil/sti/pdfs/ADA522626.pdf* [Accessed: April 20, 2025]

[7] CISA (2022). *Federal Information Security Modernization Act.* https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act [Accessed: April 25, 2025]

[8] Resmi Gazete (2013). *2818 sayılı Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ.* https://www.resmigazete.gov.tr/eskiler/2013/11/20131111-6.htm [Accessed: April 15, 2024]

[9] UAB (2020). *2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı.* https://hgm.uab.gov.tr//uploads/pages/siber-guvenlik/ulusal-siber-guvenlik-stratejisi-ep-2020-2023.pdf [Accessed: July 16, 2023]

[10] Boulos, S. (2017). Cyberspace: Risks and Benefits for Society, Security and Development, Ramírez, J. M., & García-Segura, L. A. (Eds.). *The Talinn Manual and Jus as bellu: Some Critical Notes*, 231-242, Springer International Publishing. https://doi.org/10.1007/978-3-319-54975-0

[11] The Guardian (2007). "*Russia accused of unleashing cyberwar to disable Estonia".* https://www.theguardian.com/world/2007/may/17/topstories3.russia [Accessed: March 25, 2025]

[12] Healy, J. & Jordan, K.T. (2014). *Nato's Cyber Capabilities: Yesterday, Today, and Tomorrow*, Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2014/08/NATOs_Cyber_Capabilities.pdf [Accessed: March 20, 2025]

[13] Singer, P. W. & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.

[14] Holloway, M. (2015). *Stuxnet Worm Attack on Iranian Nuclear Facilities*. Stanford University. http://large.stanford.edu/courses/2015/ph241/holloway1/ [Accessed: April 18, 2025]

[15] Orhan, U. (2021). Cezaları Ağırlaştırmak Caydırıcılığı Artırır mı? (Does Aggravating Penalties Increase Deterrence?). *Türkiye Barolar Birliği Dergisi*, 34(56), 65-85. http://tbbdergisi.barobirlik.org.tr/m2021-156-1997 [Accessed: January 3, 2023]

[16] Dolu, O., Büker, H.& Uludağ, Ş. (2012). *Türk Ceza Adalet Sisteminin Caydırıcılık Kapasitesine İlişkin Eleştirel Bir Değerlendirme,* Ankara Üniversitesi Hukuk Fakültesi Dergisi, 61(1), 69-106. https://doi.org/10.1501/Hukfak_0000001651

[17] United Nations Charter (1945). https://www.un.org/en/about-us/un-charter/full-text [Accessed: March 18, 2025]

[18] Schmitt, M. N., Vihul, L., & NATO Cooperative Cyber Defence Centre of Excellence (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations* (First published 2017). Cambridge University Press.

[19] Tikk, E., Kaska, K. & Vihul, L. (2010). International Cyber Incidents Legal Considerations. NATO Cooperative Cyber Defence Centre of Excellence https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf [Accessed: March 15, 2025]

[20] Moynihan, H. (2020). The vital role of international law in the framework for responsible state behaviour in cyberspace. *Journal of Cyber Policy*, *6*(3), 394–410. https://doi.org/10.1080/23738871.2020.1832550 [Accessed: April 18, 2025]

[21] Nye, J.S. (2017). Deterrence and Dissuasion in Cyberspace. International Securit, Vol. 41, No. 3 (Winter 2016/17). https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/isec_a_00266.pdf [Accessed: April 4, 2025]

[22] International Committee of the Red Cross (ICRC). (2015). *International humanitarian law and the challenges of contemporary armed conflicts*. https://www.icrc.org/en/publication/international-humanitarian-law-and-challenges-contemporary-armed-conflicts-building [Accessed: April 18, 2025]

[23] Council of Europe. (2001). *Convention on Cybercrime* (ETS No. 185). https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 [Accessed: April 23, 2025]

[24] Carr, E.H. (2001). *The Twenty Years' Crisis: An Introduction to the Study of International Relations*, New York: Palgrave.

[25] United Nations. (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/70/174). https://digitallibrary.un.org/record/799853?ln=en&v=pdf [Accessed: April 29, 2025]

[26] United Nations. (2021). *Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security* (A/75/816). https://documents.un.org/doc/undoc/gen/n21/068/72/pdf/n2106872.pdf [Accessed: April 29, 2025]

[27] NATO. (2019). *Cyber defence*. https://www.nato.int/cps/en/natohq/topics_78170.htm [Accessed: April 29, 2025]

[28] European Commission. (2020). *Cyber Diplomacy Toolbox*. https://www.consilium.europa.eu/en/policies/cyber-diplomacy/ [Accessed: April 29, 2025]

[29] BTK (2017). *Siber Güvenlik Kurulu.* https://www.btk.gov.tr/siber-guvenlik-kurulu [Accessed: June 13, 2023]

[30] 5651 Kanun (2004). https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5651.pdf [Accessed: June 13, 2023]

[31] Resmi Gazete (2008*). 5809 sayılı Elektronik Haberleşme Kanunu*. https://www.resmigazete.gov.tr/eskiler/2008/11/20081110M1-3.htm [Accessed: May 12, 2023]

[32] Resmi Gazete (2016*). 6698 Sayılı Kişisel Verilerin Korunması Kanunu.* https://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf [Accessed: April 29, 2023]

[33] Resmi Gazete (1991). *3756 sayılı 765 sayılı Türk Ceza Kanunu'nun Bazı Maddelerinin Değiştirilmesine Dair Kanun.* https://www.resmigazete.gov.tr/arsiv/20901.pdf [Accessed: Feb 2, 2023]

[34] 5237 Sayılı Türk Ceza Kanunu (2004). https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5237.pdf [Accessed: July 12, 2023]

[35] *3756 sayılı 765 sayılı Türk Ceza Kanunu'nun Bazı Maddelerinin Değiştirilmesine Dair Kanun.* https://www.resmigazete.gov.tr/arsiv/20901.pdf [Accessed: Feb 2, 2023]

[36] Türkiye Cumhuriyeti Anayasası (1982) https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2709&MevzuatTur=1&MevzuatTertip=5 [Accessed: Feb 2, 2023]

[37] EGM (2019). *Siber Suç Nedir?*. https://www.egm.gov.tr/siber/sibersucnedir [Accessed: April 2, 2023]

[38] Council of Europe Budapest Convention (2004). *The Budapest Convention (ETS No.185) and its Protocols*.

https://www.coe.int/en/web/cybercrime/the-budapest-convention [Accessed: June 21, 2023]

[39] 5271 Sayılı Ceza Muhakemesi Kanunu (2004). https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5271.pdf [Accessed: June 27, 2023]