SELÇUK ÜNİVERSİTESİ
HUKUK FAKÜLTESİ DERGİSİ
Selçuk Law Review

Araştırma Makalesi
Research Article
Gönderim | Received: 16/05/2025
Kabul | Accepted: 16/07/2025
10.15337/suhfd.1700507

TÜRKİYE'NİN SİBER GÜVENLİK YAKLAŞIMI ve 7545 SAYILI SİBER GÜVENLİK KANUNU ÜZERİNE BİR DEĞERLENDİRME

Emir YÜCEL *

Öz

21.yüzyılın ilk çeyreği, küresel ölçekte dijitalleşme sürecinin olağanüstü bir hızla ilerlemesine sahne olmuştur. Dijital teknolojilerin kamu hizmetlerinden finansal işlemlere, askeri yapılardan bireysel mahremiyete kadar her alanda belirleyici hale gelmesi, devletlerin güvenlik politikalarını da kökten değiştirmiştir. Türkiye küresel ölçekte yaşanan bu dönüşümlere sessiz kalmamış ve bu süreçte siber güvenlik alanında hem kurum içi düzenlemeler gerçekleştirmiş hem de stratejik belgeler yayınlamıştır. 2025 yılında yürürlüğe giren 7545 sayılı Siber Güvenlik Kanunu, bu parçalı yapıyı ortadan kaldırmak amacıyla hazırlanmış ve Türkiye'de ilk kez siber güvenliği kapsamlı şekilde tanımlayan yasal bir çerçeve sunmuştur. Bu çalışmada Avrupa Birliği ve Türkiye'nin siber güvenlik alanında gerçekleştirdiği hukuki düzenlemeler ele alınarak Türkiye'nin 7545 Sayılı Siber Güvenlik Kanunu ile oluşturduğu güncel siber güvenlik yaklaşımı ele alınacaktır.

* Yüksek Lisans Öğrencisi, İstanbul Ticaret Üniversitesi, Hukuk Fakültesi, Özel Hukuk Anabilim Dalı, İstanbul, Türkiye | Master's Student, Istanbul Ticaret University, Faculty of Law, Department of Private Law, Istanbul, Türkiye.
emir.yucel@gmail.com • ORCID 0009-0005-9485-246X.

Atıf Şekli | **Cite As**: **YÜCEL,** Emir: "Türkiye'nin Siber Güvenlik Yaklaşımı ve 7545 Sayılı Siber Güvenlik Kanunu Üzerine Bir Değerlendirme", SÜHFD, C. 33, S. 3, Y. 2025, s. 1849-1879.

İntihal | **Plagiarism**: Bu makale intihal programında taranmış ve en az iki hakem incelemesinden geçmiştir. | This article has been scanned via a plagiarism software and reviewed by at least two referees.

Anahtar Kelimeler

Siber Güvenlik • Siber Uzay • Dijital Egemenlik • Avrupa Birliği • 7545 sayılı Siber Güvenlik Kanunu.

AN EVALUATION OF TURKEY'S CYBERSECURITY APPROACH AND CYBERSECURITY LAW NO. 7545

Abstract

The first quarter of the 21st century has witnessed the rapid global rise of digitalization. The growing role of digital technologies in areas from public services and financial systems to military structures and individual privacy has fundamentally reshaped state security policies. Cybersecurity is now a matter of national security, not just a technical issue. Turkey has actively responded to these global shifts by implementing institutional regulations and publishing strategic documents in cybersecurity. The Cybersecurity Law No. 7545, enacted in 2025, was designed to eliminate fragmentation and introduced the first comprehensive legal framework for cybersecurity in Turkey. This study examines the legal frameworks developed by the European Union and Turkey, focusing on Turkey's updated cybersecurity approach through Law No. 7545.

Keywords

Cybersecurity • Cyberspace • Digital Sovereignty • European Union • Cybersecurity Law No. 7545

GİRİŞ

Siber güvenlik, bilgisayar ağları, sistemler ve yazılımları yetkisiz erişim, saldırı ve zarar görme gibi tehditlere karşı koruma amacı taşıyan teknoloji, müdahale ve zarar azaltma yöntemlerinin bütüncül kullanımı olarak ifade edilmektedir.[1]Kavram, bilgisayar sistemlerinin finans, sağlık, enerji ve savunma sanayi alanlarında kullanılmasıyla birlikte yalnızca teknik boyutla açıklanamayacak şekilde çok katmanlı bir yapıya evrilmiştir[2]. Kavramın toplumun birçok kesimini etkileyen çok katmanlı bir yapıya evrilmesiyle birlikte, devletler ulusal güvenliklerini sağlama ihtiyacı

---

1 **CRAIGEN**, Dan, **DIAKUN-THIBAULT,** Nadia & **PURSE,** Randy. (2014). *Defining cybersecurity. Technology Innovation Management Review*, *4*(10), 13–21.

2 **BAYUK**, Jennifer L., HEALEY, Jason., **ROHMEYER**, Paul, **SACHS,** Marcus H., **SCHMIDT**, Jeffrey., & **WEISS**, Joseph. (2012). *Cybersecurity policy guidebook.* John Wiley & Sons..

hissetmiş ve siber güvenliğin sağlanması hedefini ulusal güvenlik stratejilerinin bir parçası haline getirmiştir. [3]

Türkiye'de siber güvenlik kavramı 1990'lı yılların başından itibaren internet bağlantısının kurulmasıyla gündeme gelmiş, bilişim suçları ve bilgi güvenliği meselelerinin tartışılmasıyla gelişim göstermiştir. [4]1991 yılında bilişim suçlarının Türk Ceza Kanunu'na eklenmesi ve 2004 yılında Türk Ceza Kanunu ile bilişim suçlarının daha ayrıntılı bir şekilde suç kategorisi altına alınmasıyla yasal mevzuat temeli oluşturulmuştur.

2012 yılında yayımlanan 2012/3842 sayılı Bakanlar Kurulu Kararı ile Türkiye, siber güvenliğe ilişkin kurumsal stratejisini resmileştirmiştir. Bu karar doğrultusunda, siber tehditlere karşı politikaların belirlenmesi ve koordinasyonunun sağlanması amacıyla Siber Güvenlik Kurulu tesis edilmiştir [5]

2013/4890 sayılı Bakanlar Kurulu Kararı ile Türkiye, Ulusal Siber Güvenlik Stratejisi ve buna bağlı 2013-2014 Eylem Planı'nı uygulamaya koymuştur. Bu kapsamda, siber tehditlere karşı operasyonel yanıt verebilmek amacıyla Bilgi Teknolojileri ve İletişim Kurumu bünyesinde USOM adıyla merkezi bir müdahale birimi kurulmuştur.[6]

Ulusal Siber Güvenlik Stratejisi kapsamında, USOM'un yönlendirmesiyle sektörel düzeyde faaliyet gösterecek SOME'lerin yapılandırılması planlanmıştır. Bu yapılanma, siber güvenlik politikalarında sektörel odaklı bir yaklaşımın tercih edildiğini göstermektedir.

---

3 **LEWIS**, James Andrew. (2011). Cybersecurity: Assessing the immediate threat to the united states. *Testimony Before the US House Oversight and Government Reform Committee, 3*(4), 14. https://www.csis.org/analysis/cybersecurity-assessing-immediate-threat-united-states

4 **AYTEKİN,** Akın. (2015). Türkiye'nin siber güvenlik stratejisi ve eylem planının değerlendirilmesi (Yüksek lisans tezi, Gazi Üniversitesi, Bilişim Enstitüsü). Yükseköğretim Kurulu Ulusal Tez Merkezi. https://tez.yok.gov.tr/

5 T.C. Resmî Gazete. (2012, 20 Ekim). 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının yürütülmesi, yönetilmesi ve koordinasyonuna ilişkin karar. https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm (Erişim tarihi: 08.05.2025).

6 T.C. Resmî Gazete. (2013, 20 Haziran). *2013/4890 sayılı Ulusal Siber Güvenlik Stratejisi ve 2013–2014 Eylem Planı hakkında Bakanlar Kurulu kararı.* https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm

2016 yılında yayımlanan Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı ile gelişen tehdit ortamına uyum sağlanmış, kritik altyapı tesislerinin korunması, siber savunma kapasitesinin artırılması ve insan kaynağı yetiştirilmesi önceliklendirilmiştir[7]. 2020 yılında yaşanan COVID-19 pandemisinin hızlandırdığı dijitalleşme süreciyle birlikte siber güvenlik alanındaki önlemler ciddi şekilde artırılmıştır.[8]

2020-2023 dönemini kapsayan Ulusal Siber Güvenlik Strateji Belgesi ile Türkiye, dijital güvenliğe dair politikalarını güncellemiş ve özellikle eğitim sistemine entegre siber güvenlik içerikleri aracılığıyla bu alanda nitelikli insan kaynağını geliştirmeyi hedeflemiştir.[9]

2024 yılında yayımlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028) ile "*İnsan Odaklı Siber Güvenlik Yaklaşımı*" nı temel alan Türkiye, siber güvenlik alanında öncü ülke olma amacı ve siber diplomasi ile uluslararası alanda ülkemizin tutumunun ifade edilmesinin sağlanması hedeflerini hayata geçirmeyi planlamaktadır.[10] Türkiye, 2025 yılında yürürlüğe giren 7545 sayılı Siber Güvenlik Kanunu ile, dijital alandaki ulusal çıkarlarını korumaya ve siber tehditlere karşı hukuki çerçeveyi güçlendirmeye yönelik önemli bir adım atmıştır.[11] Türkiye, 2025 yılında yürürlüğe giren 7545 sayılı Siber Güvenlik Kanunu ile, dijital alandaki ulusal çıkarlarını korumaya ve siber tehditlere karşı hukuki çerçeveyi güçlendirmeye yönelik önemli bir adım atmıştır

I. KAVRAMSAL ÇERÇEVE

A. Siber Güvenlik

Siber kavramı Yunanca "χυβερνήτης" (kılavuz, dümenci) kelimesinden türemiş olup, 1948 yılında Norbert Wiener tarafından sibernetik (cybernetics) kavramının ortaya atılmasıyla gündeme gelmiştir. Winer'e

---

7 T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. (2016). *Ulusal Siber Güvenlik Stratejisi ve 2016–2019 Eylem Planı*. Ankara.

8 **KOÇAK**, Hüseyin. (2020). Dijital çağda iletişim güvenliği ve toplum. *Journal of Social, Humanities and Administrative Sciences, 6*(34), 2302.

9 T.C. Ulaştırma ve Altyapı Bakanlığı. (2020). *Ulusal Siber Güvenlik Stratejisi ve 2020–2023 Eylem Planı.* Ankara.

10 T.C. Ulaştırma ve Altyapı Bakanlığı. (2024). *Ulusal Siber Güvenlik Stratejisi ve 2024–2028 Eylem Planı*. Ankara.

11 T.C. Resmî Gazete. (2025, 19 Mart). 7545 sayılı Siber Güvenlik Kanunu. Resmî Gazete (Sayı: 32846). https://www.resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm

göre sibernetik, makinelerde ve canlı organizmalarda kontrol ve iletişim ortak bir bilimsel alan içerisinde inceleyen bir disiplin alanıdır. [12]Güvenlik kavramı ise, bir aktörün değerli varlıklarının zarar görmesini önlemek için aldığı önlemler bütünü olarak ifade edilmektedir. [13]

Siber güvenlik, bireylerin, kurumların ve devletlerin kullandığı bilgi sistemlerinin gizliliğini, bütünlüğünü ve erişilebilirliğini korumak amacıyla, insan unsuru, süreç yönetimi ve teknolojik araçlar kullanılarak gerçekleştirilen koruma faaliyetlerinin bütünüdür. [14]

Türkiye açısından siber güvenlik kavramının tanımı Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda yer almıştır. Belgede yer alan tanıma göre siber güvenlik,*" siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen gizlilik, bütünlük ve erişilebilirliğin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini"* ifade etmektedir.[15]

2016-2019 Ulusal Siber Güvenlik Stratejisi belgesinde ise siber güvenlik ve ulusal siber güvenlik olmak üzere iki tanımlamaya yer verilmiştir. Belgede, siber güvenlik "*Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi*" olarak tanımlanmaktadır.

Ulusal siber güvenlik kavramı ise" *Ulusal siber uzayı oluşturan bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmet, işlem, bilgi/verinin ve bunların sunumunda yer alan donanım ve yazılım sistemlerinin ulusal ölçekte*

---

12 **WIENER**, Norbert. (1975*). Emek, sibernetik ve toplum* (İ. Keskin, Çev.). İstanbul: Özgün Yayınları. (Orijinal eser 1948'de yayımlanmıştır).

13 **BALDWIN,** David. A. (1997). The concept of security. *Review of International Studies, 23*(1), 5–26. https://dbaldwin.scholar.princeton.edu/sites/g/files/toruqf4596/files/dbaldwin/files/baldwin_1997_the_concept_of_security.pdf

14 **HEKİM**, Hakan., & **BAŞIBÜYÜK**, Oğuzhan. (2013). Siber suçlar ve Türkiye'nin siber güvenlik politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi, 4*(2), 135–158. https://search.trdizin.gov.tr/tr/yayin/detay/150969/

15 Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. *Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı.* https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm (Erişim tarihi: 08.05.2025).

sağlanan siber güvenliğini "ifade etmektedir.[16]2020-2023 yıllarını kapsayan Ulusal Siber Güvenlik Stratejisi belgesinde ise önceki strateji belgesinden farklı olarak yer alan "*güvenli biçimde işleyen bir siber ortama sahip olmak ve siber güvenlikte uluslararası alanda marka haline gelmek*" vizyonu yer almaktadır. Bu vizyon, 2024-2028 yılları arasını kapsayan Ulusal Siber Güvenlik Stratejisi'nde de yer almaktadır. 2024-2028 yılları arasını kapsayan bu belgede, önceki belgelerden farklı olarak "*Siber Dayanıklılık*" kavramına yer verilmekte, Türkiye'nin hibrit tehditlere karşı koyabilmesi için siber dayanıklılığın sağlanması yolunda adımlar atılacağı ifade edilmektedir.[17]

B. Siber Uzay

Siber uzay; yalnızca bilgisayarlardan ve dijital ortamdan ibaret olmayan, bilgi ve iletişim teknolojilerinin kullanılarak birbirine bağlı ağlar aracılığıyla bilginin oluşturulduğu, paylaşıldığı ve depolandığı alan olarak ifade edilmektedir. [18] NATO, 2016 yılında düzenlenen Varşova Zirvesi sonucunda yayımladığı bildiride siber uzayı; kara, deniz, hava ve uzay alanlarına ek olarak bir harekât alanı olarak kabul etmiş ve böylece dijital ortamları askerî stratejisinin ayrılmaz bir parçası haline getirmiştir.[19]

Siber uzayda egemenlik, klasik sınırlar üzerinden değil; bilgi akışı, ağ trafiği kontrolü ve veri yönetimi üzerinden şekillenmektedir. Siber

---

16 Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. *Ulusal Siber Güvenlik Stratejisi ve 2016–2019 Eylem Planı.* Ankara, 2016. https://www.resmigazete.gov.tr/eskiler/2016/10/20161020-1.htm. Erişim tarihi: 08.05.2025.

17 Ulaştırma ve Altyapı Bakanlığı. *Ulusal Siber Güvenlik Stratejisi ve 2024–2028 Eylem Planı.* Ankara, 2024. https://www.uab.gov.tr/uploads/pages/ulusal-siber-guvenlik-stratejisi/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2024-2028.pdf. Erişim tarihi: 08.05.2025.

[18] **KUEHL** Daniel T, "From Cyberspace to Cyberpower: Defining the Problem", **KRAMER** Franklin D., **STARR** Stuart H. & **WENTZ** Larry K. (Ed.), *Cyberpower and National Security*, Washington DC, 2009, s. 24–42.

19 Kuzey Atlantik Antlaşması Örgütü (NATO). *Warsaw Summit Communiqué, 9 Temmuz 2016*. https://www.nato.int/cps/en/natohq/official_texts_133169.htm. Erişim tarihi: 08.05.2025.

uzayla birlikte ortaya çıkan siber sınır kavramı, verilerin ülke içine girmesini engellemekten çok ülke içinde kalmasını ifade etmektedir. [20]Türkiye'nin bu bağlamda oluşturduğu ulusal güvenlik stratejileri ile attığı adımlar siber uzayda bağımsız hareket etme isteğinin göstergesidir. [21]

Kavramın tanımı 7545 Sayılı Siber Güvenlik Kanunu'nda da yer almaktadır. Bu tanıma göre Siber uzay "*Doğrudan ya da dolaylı olarak internete, elektronik haberleşme veya bilgisayar ağlarına bağlı olan tüm bilişim sistemlerini ve bunları birbirine bağlayan ağlardan oluşan ortamı*" ifade etmektedir.[22] Kanun ile kritik altyapı ve bilişim sistemlerinin korunarak siber saldırıların önlenmesi ve güvenli bir siber uzay oluşturulması hedeflenmektedir. [23]

C. Siber Terör

Siber terör, siyasi, ideolojik veya dini motivasyonlarla, dijital araçlar vasıtasıyla bireyleri, kamu düzenini veya kritik altyapıları tehdit ederek siber uzaya zarar verme amacı taşıyan eylemleri ifade etmektedir.[24]Bu eylemler yalnızca fiziksel zarar vermekle kalmamakta; kamuoyun-da panik oluşturma ve terör duygusunun uyandırılması amacıyla siber şiddet uygulayarak kamu düzenini bozmayı amaçlamaktadır.[25] Estonya'da 2007 yılında yaşanan DDoS saldırıları, İran'daki Stuxnet virüsü ve Ukrayna'nın enerji altyapısına yapılan siber saldırılar, siber terör vakıaları olarak tarihte yerini almaktadır. [26]

7545 Sayılı Kanun, siber terörle mücadele konusunda siber uzayın korunması için gerekli aksiyonların alınmasını öngörmekte ve kamu kurum ve kuruluşları ile özel sektör kuruluşlarına belirli sorumluluklar

---

20 **KUNER**, Christopher, "Data Nationalism and Its Discontents", Emory *Law Journal Online*, 64, 2015, s. 2089. https://scholarlycommons.law.emory.edu/elj-online/25. Erişim tarihi: 08.05.2025.

21 **BOZKURTLAR** Burak, Ulus Devletlerin Siber Güvenlik Stratejileri ve Siber Vatan, *Siber Vatan*, 2021, s. 1–22. https://www.academia.edu/

22 7545 sayılı Siber Güvenlik Kanunu, m. 3/1-i.

23 m.3/1-f, g

24 **ARQUILLA**, John., & **RONFELDT**, David. (Eds.). (2001). Networks and netwars: The future of terror, crime, and militancy. RAND Corporation. https://www.rand.org/pubs/monograph_reports/MR1382.html

25 **SHARMA**, Anuj (2022). "Cyber Terrorism: A Growing Threat to India's Cyber Security". *Indian Journal of Cyber Law (5)*2, s. 61.

26 **STEINER**, Hrafn. (2016). Cyber-attacks as coercive instruments. *Analys & Perspektiv*, (3), 148. https://kkrva.se/artiklar/cyber-attacks-as-coercive-instruments/

yüklemektedir. Yasada yer alan hükümlerle Türkiye'nin ulusal siber güvenliğinin sağlanması hedeflenmektedir.[27]

D. Siber Vatandaşlık

Siber vatandaşlık, bireylerin dijital hak ve sorumluluklarının farkında olarak, belirlenen etik dijital davranış kurallarına uyum sağlayarak dijital ortamlara katılım sağlaması olarak ifade edilmektedir.[28]Türkiye'de siber vatandaşlık özellikle Bilgi Teknoloji ve İletişim Kurumu ve Dijital Dönüşüm Ofisi Başkanlığı [29]gibi kurumların projeleri ile teşvik edilmekte; gençlere yönelik dijital okuryazarlık eğitimleriyle desteklenmektedir.

II. TÜRKİYE'DE SİBER GÜVENLİĞİN TARİHÇESİ VE GELİŞİMİ

A. Bilgi Güvenliğinden Siber Güvenliğe

Türkiye'de siber güvenlik kavramı, ilk yıllarda daha çok *"bilgi güvenliği" ve "bilişim suçları"* çerçevesinde ele alınmıştır. 5237 sayılı Yasa ile siber suçlar ilk kez yasal düzenlemeye dahil edilmiş; *"bilişim sistemine girme", "sistemi engelleme, bozma, verileri yok etme veya değiştirme", banka veya kredi kartlarının kötüye kullanılması"* eylemleri cezai müeyyide altına alınmıştır.[30]Ancak bu dönemde henüz ulusal bir siber güvenlik politikasından söz etmek mümkün değildir.

B. Siber Güvenlik Kurulu ve Ulusal Siber Olaylara Müdahale Merkezi (USOM) 'nin Kuruluşu

2012 yılında Başbakanlık tarafından yayımlanan Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, Türkiye'nin bu alanda gerçekleştirilen resmi bir politika belgesi olarak karşımıza çıkmaktadır. Karar ile Siber Güvenlik Kurulu kurulmuş, Ulaştırma, Denizcilik ve Haberleşme Bakanlığı bu kurulun sekretaryası

---

27 m.3/1-f

28 **RIBBLE**, Mike S., **BAILEY**, Gerald, D., & **ROSS**, Tweed, W. (2004, September). Digital citizenship: Addressing appropriate technology behavior. *Learning & Leading with Technology, 32*(1), 6–9, 11. https://files.eric.ed.gov/fulltext/EJ695788.pdf

29 Dijital Dönüşüm Ofisi, 28 Mart 2025 tarihli 183 sayılı Bazı Cumhurbaşkanlığı Kararnamelerinde Değişiklik Yapılmasına Dair Cumhurbaşkanlığı Kararnamesi ile kaldırılmıştır.

30 **BIÇAKCI** Salih, **ERGUN** Doruk & **ÇELİKPALA** Mitat, "Türkiye'de Siber Güvenlik", EDAM Siber Politika Kağıtları Serisi, *EDAM Yayınları*, 2015, s. 30. https://edam.org.tr/wp-content/uploads/2015/12/EDAM_TR_Siber_Guv_1.pdf. Erişim tarihi: 08.05.2025.

olarak yetkilendirilmiştir. Kurul, "*siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak*" amacıyla kurulmuştur[31].

Kararın 5.maddesinde Siber Güvenlik Kurulu'nun görev ve yetkilerinden bahsedilmektedir:

"*-Ulusal Siber Güvenliğin sağlanması için politika, strateji ve eylem planlarını hazırlamak,*

- Kamu kurum ve kuruluşlarına ait bilgi ve verilerin güvenliği ile mahremiyetinin güvence altına alınmasını sağlamaya yönelik usul ve esasları ha-zırlamak,

- Ulusal Siber Güvenliğin sağlanmasında kamu kurum ve kuruluşlarında teknik alt yapının oluşturulmasını takip etmek, uygulamaların etkinliğinin doğrulanmasını ve test edilmesini sağlamak,

- Ulusal bilgi teknolojileri ve iletişim alt yapısı ve sistemleri ile veri tabanlarının güvenliğini sağlamaya, kritik alt yapıları belirleyerek bunlara yönelik siber tehdit ve saldırı izleme, müdahale ve önleme sistemlerini oluşturmaya, ilgili merkezleri kurmaya, kurdurmaya, bu sistemlerin denetimi, işletimi ve sürekli güçlendirilmesine yönelik çalışmaları yapmak,

- Ulusal Siber Güvenliğin sağlanmasında her türlü milli çözümlerin ve siber saldırılara müdahale araçlarının geliştirilmesi ve üretilmesini teşvik etmek, kullanımım sağlamak,

- Ulusal Siber Güvenlik açısından kritik kurum ve konumlar için gerekli ve yeterli sayıda uzman personelin temini, eğitimi ve gelişimini planlamak, koordine etmek ve yürütmek

- Bu Karar çerçevesinde diğer ülkeler ve uluslararası kuruluşlarla iş birliği yapmak,

- Ulusal Siber Güvenlik konusunda bilinçlendirme, eğitim ve farkındalığı artırma çalışmaları yürütmek

- Bilgi güvenliği alanında eğitim, test ve çözüm üretme alanında çalışan gerçek ve tüzel kişilere usul ve esaslarını belirleyerek güvenlik belgesi vermek

- Siber Güvenlik Kurulunun sekretarya hizmetlerini yürütme"[32]

---

31 T.C. Resmî Gazete. (2012, 20 Ekim). 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının yürütülmesi, yönetilmesi ve koordinasyonuna ilişkin karar. https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm (Erişim tarihi: 08.05.2025).

32 T.C. BAŞBAKANLIK, Ulusal Siber Güvenlik Kararı, m. 5.

Karar'ı takiben 2013 yılında BTK bünyesinde Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuştur. Türkiye'nin siber güvenlik yapısında merkezi bir konuma sahip olan Ulusal Siber Olaylara Müdahale Merkezi (USOM), dijital tehditlerin tespiti, olası saldırıların etkilerinin en aza indirilmesi ve karşı tedbirlerin geliştirilmesi konularında çalışmaktadır. Ayrıca, bu tehdit bilgilerini ilgili kamu ve özel sektör kuruluşlarıyla paylaşarak siber savunma kapasitesinin artırılmasına katkı sağlamaktadır[33]

2016 yılında yayımlanan Ulusal Siber Güvenlik Stratejisi ve 2016–2019 Eylem Planı, Türkiye'nin siber güvenlikte kurumsallaşma yönündeki ikinci strateji belgesi olması açısından önem taşımaktadır. Bu belgeyle birlikte, sektörel SOME'lerin kurulması yasal zorunluluk haline getirilmiştir.[34] 2018 yılında Cumhurbaşkanlığı Hükümet Sistemi'ne geçilmesinin ardından, 1 sayılı Cumhurbaşkanlığı Kararnamesi ile doğrudan Cumhurbaşkanlığı'na bağlı olarak faaliyet gösterecek Dijital Dönüşüm Ofisi kurulmuştur. Bu ofisin görevleri arasında, ülke genelinde bilgi güvenliği ve siber güvenlik alanında proje geliştirmek ve uygulamak gibi işlevler de yer almaktadır. Ofis bünyesinde oluşturulan Siber Güvenlik Dairesi Başkanlığı ise siber güvenliğin sağlanması yönünde çalışmalar yapmakla görevlendirilmiştir[35]. Dijital Türkiye vizyonu kapsamında Dijital dönüşümün sağlanması görevini yürüten Ofis'in e-devlet uygulamalarının geliştirilmesi faaliyetleri ve "BTK'nin Siber Güvenlik, Siber Farkındalık, Dijital Vatandaşlık" eğitimleri ile birlikte siber vatandaşlık bilincinin oluşturulması yönünde çalışıldığı görülmektedir. [36]2019 tarihli "*Bilgi ve İletişim Güvenliği Tedbirleri"* başlıklı Cumhurbaşkanlığı Genelgesi doğ-

---

33 Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm (Erişim tarihi: 08.05.2025).

34 Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. Ulusal Siber Güvenlik Stratejisi ve 2016–2019 Eylem Planı. Ankara, 2016. https://www.resmigazete.gov.tr/eskiler/2016/10/20161020-1.htm. Erişim tarihi: 08.05.2025.

35 T.C. Resmî Gazete,1 Sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi", 10 Temmuz 2018, Sayı: 30474. https://www.resmigazete.gov.tr/eskiler/2018/07/20180710-1.pdf. Erişim tarihi: 08.05.2025.

36 BTK Akademi: BTK Akademi Eğitim Portalı, https://www.btkakademi.gov.tr/portal (Erişim Tarihi: 08.05.2025).

rultusunda Dijital Dönüşüm Ofisi Başkanlığı tarafından 2020 yılında yayımlanan Bilgi ve İletişim Güvenliği Rehberi siber olaylara ilişkin birtakım tedbir ve denetim mekanizmaları öngörmektedir. [37]

2020 yılında Ulusal Siber Güvenlik Strateji ve Eylem Planı (2020-2023) 'ün yayımlanması ve 2024 yılında Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028)'nın yayımlanması ile Türkiye en güncel strateji planını hayata geçirme hedefini taşımaktadır.

C. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028)

İnsan, Savunma, Caydırıcılık ve İş Birliği temalarından yola çıkılarak hazırlanan belgede, Türkiye'nin 2012'den itibaren belirli periyotlarla revize ettiği stratejik yaklaşımlarının somut kazanımlara dönüştürülmesinin hedeflendiği ifade edilmektedir. [38]

1. Belgede Yer Alan Stratejik Amaç ve Hedefler

a. Siber Dayanıklılık

Belgede, Siber dayanıklılığın sağlanmasının risk tespiti ile risk değerlendirmesi yapılması ve risk temelli analiz yaklaşımının uygulanması ile gerçekleştireceği ifade edilmektedir. Qudus'a göre, dijital çağda ortaya çıkan siber terör, siber savaşlar, fidye yazılımı saldırıları gibi siber güvenliği tehlikeye atan durumlara karşı dayanıklı altyapılar oluşturulmalıdır.[39]

b. Proaktif Siber Savunma ve Caydırıcılık

Proaktif siber savunma, belirli yazılımların tanımlı olduğu ağ tabanlı güvenlik duvarlarının kullanılarak, siber saldırının önceden tanımlanması ve tahmin edilmesine dayanan, kritik altyapıların korunmasına yönelik savunma yaklaşımı olarak ifade edilmektedir. [40]Strateji belgesin-

---

37 T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Bilgi ve İletişim Güvenliği Rehberi, Ankara, 2020. https://assets.kpmg.com/content/dam/kpmg/tr/pdf/2020/08/bilgi-iletisim-guvenligi-rehberi.pdf (Erişim tarihi: 08.05.2025).

38 T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Strateji ve Eylem Planı (2024–2028), Ankara, 2024. Erişim tarihi: 08.05.2025.

39 **QUDUS**, Lawal (2025). Resilient Systems: Building Secure Cyber-Physical Infrastructure for Critical Industries Against Emerging Threats. *International Journal of Research Publication and Reviews (6)*1, s. 3330.

40 **ROSHANAEI**, Maryam. (2021). Resilience at the core: Critical infrastructure protection challen-ges, priorities and cybersecurity assessment strategies. *Journal of Computer and Communications, 9*(8), 80–102. https://doi.org/10.4236/jcc.2021.98006

de, SOME'lerin kapasitelerinin artırılması ve olaylara müdahale kabiliyetlerinin artırılmasıyla birlikte siber savunma alanında proaktif yaklaşımın uygulanabileceği hususu yer almaktadır. [41]

c. İnsan Odaklı Siber Güvenlik Yaklaşımı

Belgede, siber güvenlik zafiyetlerinin yaklaşık %80'inin insan unsurunun rol oynadığı ihmallerden kaynaklandığı, kişilerin siber olaylara ilişkin bilinçlendirilmesinin ulusal siber güvenliğin sağlanmasında etkin rol oynayacağı ifade edilmektedir. Doktrinde, insan merkezli yaklaşımla birlikte, siber güvenlik risklerinde gelen olarak bir azalmanın olacağı yönünde görüşler yer almaktadır.

d. Teknolojinin Güvenli Kullanımı ve Siber Güvenliğe Katkısı

Dijitalleşme çağında ortaya çıkan büyük ölçekli teknolojiler karşısında "*sıfır güven (zero trust)"* anlayışını temel alarak dijital dönüşüm ve siber güvenliğin sağlanacağı ifade edilmektedir. [42]Sıfır güven anlayışı, geleneksel güvenlik anlayışının tehditlere karşı koymakta yetersiz kalması nedeniyle, kimlik doğrulaması, denetim ve şifreleme gibi güvenlik yöntemlerin kullanılmasını içermektedir.[43]

e. Siber Tehditlerle Mücadelede Yerli ve Millî Teknolojiler

Yerli ve milli imkanlar ile üretilen teknolojiler, Türkiye'nin siber uzayda güvenliğinin sağlanması yönünde önemli bir adım olarak görülmektedir. Belgede, yerli ve milli imkanlar ile üretilen teknolojiler sayesinde, Türkiye'nin siber savunma ve caydırıcılık hedeflerinin sağlanacağı öngörülmektedir.[44]

AKINTOLA, Adeyemi Samuel (2024). Integrating research testbeds, attack mechanisms, and defence strategies into a holistic framework for cybersecurity. *Journal of Computer Science Review and Engineering*, *8*(2), 1–12. https://doi.org/10.5281/zenodo.14543273

41 **NOGHONDAR**,Elham Rajabian "Importance of Human Factors on Cybersecurity within Organizations", 2023. https://personales.upv.es/thinkmind/dl/conferences/securware/securware_2022/securware_2022_1_10_30004.pdfErişim tarihi: 09.05.2025.

42 T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Strateji ve Eylem Planı (2024–2028), Ankara, 2024. Erişim tarihi: 09.05.2025.

43 **EL-ZUGHAID** ,Aya Issa, **FUNOUSH**, Zuhayr A., **YOUNIS** A. & **ALGHAMDİ** Mohammed Yahya, (2024). "A Zero Trust Framework to Secure IoT Devices", *University of Ha'il – Journal of Science, 5*(2), s. 51.

44 T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Strateji ve Eylem Planı (2024–2028), Ankara, 2024. Erişim tarihi: 09.05.2025.

f. Uluslararası Alanda Türkiye Markası

Siber güvenlik alanında marka haline gelme amacını taşıyan Türkiye, siber diplomasi alanında kabiliyetlerini gerçekleştirerek bu amacına ulaşmayı hedeflemektedir. Türkiye, bu amaç doğrultusunda uluslararası iş birliği ve uyumun sağlanmasını hedeflemektedir.[45] Siber diplomasi, siber uzayda güvenliğin sağlanması amacıyla diplomatik imkanların kullanılması olarak ifade edilmektedir.[46]

III. BÖLÜM: 7545 SAYILI SİBER GÜVENLİK KANUNU'NUN DETAYLI İNCELENMESİ

A. Kanunun Gerekçesi ve Ortaya Çıkış Süreci

Dünyada ve Türkiye'de bilişim teknolojilerinin kullanımının hızla yaygınlaşması ve Türkiye'nin internet kullanımı alanında yaptığı atılım ile birlikte üretilen veri miktarının büyük ölçüde arttığı ifade edilmektedir. Dijitalleşme çağında, konvansiyonel savaşlar yerine hibrit anlayışın hâkim olduğu savaşların yaşandığı, devlet destekli yahut terör örgütleri tarafından yapılan siber saldırılar olduğu görülmektedir.

Uluslararası Telekomünikasyon Birliği'nin (ITU) 2024 yılına ait Küresel Siber Güvenlik Endeksi raporuna göre, Türkiye 20 ülkenin yer aldığı "rol model" [47]ülke kategorisinde konumlandırılmıştır. Ancak bu kategorideki ülkelerin %91'inin ulusal ölçekte çatı niteliğinde bir siber güvenlik mevzuatına sahip olması, Türkiye'de bu alanda yasal bir düzenlemenin gerekli olduğuna işaret etmektedir.[48]9 Mart 2025 tarihinde yürürlüğe giren 7545 Sayılı Kanun, Türkiye'nin dijital dönüşüm yolculuğunda

---

45 T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Strateji ve Eylem Planı (2024–2028), Ankara, 2024, s. 26. Erişim tarihi: 09.05.2025.

46 **BARRINHA** André & **RENARD**, Thomas. (2017). "Cyber-diplomacy: the making of an international society in the digital age", *Global Affairs, (3)*4–5, s. 353–364. https://doi.org/10.1080/23340460.2017.1414924 Erişim tarihi: 12.05.2025.

47 International Telecommunication Union Development Sector, Global Cybersecurity Index 2024 – 5th Edition, Eylül 2024. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx Erişim tarihi: 12.05.2025.

48 Türkiye Büyük Millet Meclisi, 7545 Sayılı Siber Güvenlik Kanunu Teklifi, https://www.tbmm.gov.tr/Yasama/KanunTeklifi/af1dfbdb-e3e3-4820-a493-0194504c63b4 Erişim tarihi: 12.05.2025.

uzun süredir ihtiyaç duyduğu çatı düzenleme olarak 2025 yılında yürürlüğe girmiştir. Bu düzenleme, strateji belgeleri ve yönetmeliklerle yürütülen siber güvenlik çalışmalarını ilk kez bir yasa metnine taşımıştır.[49]

B. Kanunun Amaç ve Kapsamı

7545 sayılı Siber Güvenlik Kanunu incelendiğinde, Kanun'da yer alan hükümlerle ulaşılmak istenen temel amaçların; Türkiye'nin siber uzayda ulusal güvenliğinin sağlanması ve siber güvenlik alanında yürütme ve denetim işlevlerini yerine getirecek bir mekanizma olarak Siber Güvenlik Kurulunun kurulması olduğu görülmektedir.[50] Kapsamı "*Siber uzayda varlık gösteren, faaliyet yürüten, hizmet sunan kamu kurum ve kuruluşları, kamu kurumu niteliğinde meslek kuruluşları, gerçek ve tüzel kişiler ile tüzel kişiliği bulunmayan kuruluşlar"* şeklinde düzenlenen [51]Kanunda, bazı faaliyetler kapsam dışında bırakılmıştır.[52]

C) Kanunda Yer Alan Temel İlkeler

1.Siber Güvenliğin Milli Güvenliğin Ayrılmaz Bir Parçası Olması

Kanunda siber güvenliğin milli güvenliğin temel unsurlarından biri olduğu açıkça belirtilmektedir.[53]Ülkelerin siber güvenliğe yaklaşımlarını milli güvenlik ile bağdaştırmasının nedeni, siber saldırılar ile zarar verilen kritik altyapı tesisleri, finans kurumları gibi alanlarda yaşanacak bozulmaların kamu düzenini bozacağı düşüncesidir.[54] Devletler, kamu düzenin koruma amacıyla ulusal savunma planlarına siber güvenlik stratejileri eklemekte ve siber caydırıcılığı sağlamaya çalışmaktadır.

---

[49] T.C. Resmî Gazete, "7545 Sayılı Siber Güvenlik Kanunu", 19 Mart 2025, Sayı: 32846. Erişim tarihi: 12.05.2025.

[50] 7545 sayılı Kanun, m. 1

[51] 7545 sayılı Kanun, m. 2/1

[52] 4/7/1934 tarihli ve 2559 sayılı Polis Vazife ve Salâhiyet Kanunu, 9/7/1982 tarihli ve 2692 sayılı Sahil Güvenlik Komutanlığı Kanunu ve 10/3/1983 tarihli ve 2803 sayılı Jandarma Teşkilat, Görev ve Yetkileri Kanunu uyarınca yürütülen istihbarı faaliyetler ile 1/11/1983 tarihli ve 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilâtı Kanunu ile 4/1/1961 tarihli ve 211 sayılı Türk Silahlı Kuvvetleri İç Hizmet Kanunu uyarınca yürütülen faaliyetler bu Kanun kapsamı dışındadır.

[53] 7545 sayılı Kanun, m. 4/1-a

[54] **ÇAKIR** Hüseyin & **TAŞER** Murat. (2023). "Türkiye'de Yapılan Siber Güvenlik Faaliyetlerinin ve Eğitim Çalışmalarının Değerlendirilmesi", *Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji, (11*)2, s. 348. https://doi.org/10.29109/gujsc.1165131 Erişim tarihi: 13.05.2025.

2.Güvenli Siber Uzayın Oluşturulması

Kanun metninde, *"kritik altyapı ve bilişim sistemlerinin korunması ile güvenli bir siber uzay oluşturulması"* hedefi yer almaktadır. Kritik altyapı ve bilişim sistemlerinin korunması hususu USOM koordinasyonunda SOME'lere verilen görevler ile sağlanmaya çalışılmaktadır.[55] 2016-2019 yıllarını kapsayan Ulusal Siber Güvenlik Stratejisi belgesi ve devamındaki düzenlemelerde de yer alan güvenli bir siber uzay oluşturulması hedefi son olarak Siber Güvenlik Kanunu ile hüküm altına alınmıştır.[56]

3.Kurumsallık, Süreklilik ve Sürdürülebilirlik Temelli Çalışma

Siber güvenlikle ilgili çalışmaların kurumsal düzeyde yürütülmesi amacıyla 7545 sayılı Kanun ile Siber Güvenlik Kurulu ve 177 sayılı Cumhurbaşkanlığı Kararnamesi ile Cumhurbaşkanlığına bağlı Siber Güvenlik Teşkilatı kurulmuştur. [57]Kurumsal yapıların oluşturularak bu yapıların siber güvenlik kapasitelerinin sürekli artırılması ve sürdürüle-bilir stratejilerin belirlenmesiyle birlikte siber dayanıklılığın sağlanacağı yönünde görüşler bulunmaktadır.[58]

4. Tedbirlerin Tüm Yaşam Döngüsü Boyunca Uygulanması

Anderson'a göre, Siber güvenlik devam eden bir süreçtir ve bu süreç alınan tedbirlerle birlikte tüm yaşan döngüsü boyunca devam ettirilmelidir. [59]Bu yaklaşım Siber Güvenlik Kanununda tedbirlerin tüm yaşam döngüsü boyunca uygulanması olarak yerini almaktadır.[60]

---

55 **BARUN** Başak. (2024). "The Impact of Cybersecurity Threats on National Security: Strategies", *International Journal of Humanities Social Science and Management*,s. 1361.

56 7545 sayılı Kanun, m.4/1-b

57 T.C. Resmi Gazete, "Siber Güvenlik Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi (Kararname No: 177)", Resmî Gazete, 08 Ocak 2025, Sayı: 32776.

58 **HOHMANN** Mirko, **PIRANG** Alexander & **BENNER** Thorsten, Advancing Cybersecurity Capacity Building: Implementing a Principle-Based Approach, Global Public Policy Institute (GPPi), Berlin, 2017.

59 **ANDERSON** Ross, Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley, Indianapolis, 2020, s. 283.

60 7545 sayılı Kanun, m.4/1-ç

5. Siber Güvenliğin Sağlanmasında Yerli ve Milli Ürünlerin Tercih Edilmesi

Siber güvenlik alanında markalaşmak isteyen Türkiye, bu alanda yerli ve milli ürünlerin tercih edilmesiyle siber uzayda egemenliğinin sağlanacağını düşünmektedir.[61]

6. Siber Güvenliğin Sağlanması Yolunda Çok Paydaşlık İlkesi

Siber güvenlik alanında çok paydaşlık yaklaşımı, kamu kurumları, özel sektör, akademi ve sivil toplum kuruluşlarının iş birliğini esas alarak tehditlere karşı daha kapsamlı ve etkili bir savunma hattı oluşturmayı amaçlamaktadır. [62]Türkiye'de siber güvenlik alanında çok paydaşlık anlayışının kurumsallaşması, Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı ile resmiyet kazanmıştır.[63]

7.Siber Güvenlik ve Hesap Verilebilirlik İlkesi

Kanunda yer alan tanıma göre siber güvenlik*" Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber olayların tespit edilmesini, bu tespitlere karşı tepki ve alarm mekanizmalarının devreye alınmasını ve sonrasında yaşanan siber olay öncesi duruma geri döndürülmesini kapsayan faaliyetler bütününü*" ifade etmektedir. Süreçlerin yürütülmesinde ise hesap verilebilirlik ilkesinin esas olduğu ifade edilmiştir.[64]

Hesap verilebilirlik ilkesinin hangi şart ve durumlarda uygulanacağı ise Kanunda yer almamaktadır.

---

61 **ELDEM** Tuba, *Between Multi-stakeholderism and Cyber Sovereignty: Understanding Turkey's Cybersecurity Strategy*, EDAM Cyber Policy Paper Series, No. 2021/1, İstanbul, 2021.

62 **TAGAREV** Todor & **SHARKOV** George. (2016). "Multi-Stakeholder Approach to Cybersecurity and Resilience", Information & Security: *An International Journal, (34*)1, s. 60

63 Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm (Eri-şim tarihi: 13.05.2025).

64 7545 Sayılı Kanun, m.4/1-f

8.İnsan Odaklı Yaklaşım ve Temel İnsan Hak ve Hürriyetlerinin Korunması

Türkiye, Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı'nda nitelikli insan kaynağını artırarak siber güvenlik alanında ilerle-me sağlama hedefi taşımaktadır. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planından günümüze gelen süreçte ise siber güvenliğin sağlanması esnasında "*temel insan hak ve hürriyetlerinin korunması"* ilkesi metinlerde varlığını devam ettirmektedir.

D. Siber Güvenlik Başkanlığı

177 sayılı Cumhurbaşkanlığı Kararnamesi ile kurulan Siber Güvenlik Başkanlığı, Cumhurbaşkanlığına bağlı, kamu tüzel kişiliği haiz, merkezi Ankara'da olacak şekilde kurulmuştur. Başkanlığın görev ve yetkileri Kararnamede düzenlenmekte, Başkanlığın görev ve yetkilerine 7545 sayılı Kanunda da yer verilmektedir.

Siber Güvenlik Başkanlığı'nın "*Kritik altyapılar ve bilişim sistemlerinin siber dayanıklılığının artırılması ile siber dayanıklılığın sağlanması yönünde faaliyet gösteren, siber güvenlik alanında faaliyet gösterenlerin uyması gereken usul ve esasları düzenlemek, siber güvenlik alanına ilişkin standartları hazırlamak, siber güvenlik denetimini gerçekleştirmek ve sonucuna göre yaptırım uygulamak"* görevleri bulunmaktadır.[65]*"Başkanlık, "Kanun kapsamındakilerin siber saldırılara karşı korunması ve bu saldırıların kaynağına karşı caydırıcılık sağlanması için gerekli tedbiri alır veya aldırır. Bu kapsamda bilişim sistemlerine uygun bulunan yazılım ve donanım ürünlerinin kurulum ve entegrasyonunu sağlayabilir, bu ürünler tarafından üretilen veya toplanan veri ve log kayıtlarını Başkanlık yönetiminde bulunan bilişim sistemlerine aktarabilir, siber olayların tespitine yönelik gerekli yöntemi ve aracı kullanabilir."*[66] 7545 sayılı Kanuna göre, Kanun kapsamında faaliyet gösterenlerin "*Başkanlığın görev ve faaliyetleri kapsamında talep ettiği her türlü veri, bilgi, belge, donanım, yazılım ve diğer her türlü katkıyı öncelikle ve zamanında Başkanlığa iletmek"* ve *"Siber güvenliğe yönelik olarak milli güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla mevzuatın öngördüğü tedbirleri almak, hizmet sundukları alanda tespit ettikleri zafiyet veya siber olayları gecikmeksizin Başkanlığa bildirmek"* sorumlukları bulunmaktadır.[67]

---

[65] 7545 sayılı Kanun, m. 5

[66] 7545 sayılı Kanun, m. 6

[67] 7545 Sayılı Kanun m.7/1-a, b

1. Siber Güvenlik Kurulu

2012/3842 Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar ile kurulan Siber Güvenlik Kurulu, 7545 sayılı Kanun ile de düzenlenmiştir. "*Kurul, Cumhurbaşkanı, Cumhurbaşkanı Yardımcısı, Adalet Bakanı, Dışişleri Bakanı, İçişleri Bakanı, Milli Savunma Bakanı, Sanayi ve Teknoloji Bakanı, Ulaştırma ve Altyapı Bakanı, Milli Güvenlik Kurulu Genel Sekreteri, Millî İstihbarat Teşkilâtı Başkanı, Savunma Sanayii Başkanı ve Siber Güvenlik Başkanından oluşur*."[68]
Kurulun görevleri arasında:
"a) Siber güvenlikle ilgili politika, strateji, eylem planı ve diğer düzenleyici işlemlere yönelik kararları almak, alınan kararların tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek.
b) Başkanlık tarafından hazırlanan siber güvenlik alanına ilişkin teknoloji yol haritasının ülke çapında uygulanmasına yönelik kararlar almak.
c) Siber güvenlik alanında teşvik verilecek öncelikli alanları belirlemek, siber güvenlik alanındaki insan kaynağının geliştirilmesine yönelik karar almak.
ç) Kritik altyapı sektörlerini belirlemek.
d) Başkanlık ile kamu kurum ve kuruluşları arasında meydana gelebilecek ihtilaflar hakkında karar almak" bulunmaktadır. [69]

IV. Avrupa Birliği ve Türkiye'nin Siber Güvenlik Yaklaşımlarının Karşılaştırılması

A. NIS2 Direktifi ve AI Act

Avrupa Birliği (AB), dijital altyapıların güvenliğini artırmak amacıyla 2016 yılında ilk siber güvenlik hukuk metni olan Ağ ve Bilgi Sistemlerinin Güvenliği Direktifini (NIS) kabul ederek, üye ülkelerin kritik altyapılarını siber tehditlere karşı daha dirençli hale getirmeyi hedeflemiştir. [70]Direktifin temel amacının dijital ekonomiyi desteklemek ve üye devletler arasında siber güvenlik kapasiteleri arasında uyum sağlamak olduğu

---

68 7545 Sayılı Kanun, m. 9

69 7545 Sayılı Kanun, m. 9/4

70 European Parliament and of the Council, "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)", Official Journal of the European Union, L 194, 19 July 2016, s. 1–30.

ifade edilmektedir.[71]Direktif üzerinde 2020 yılında revize çalışmaları başlatılmış ve 2023 itibarıyla yürürlüğe giren NIS2 Direktifi ile Avrupa Birliğinin siber güvenlik alanında stratejik çerçevesi genişletilmiş ve tüm üye devletlerin enerji, sağlık, ulaşım ve finans gibi alanlarda asgari siber güvenlik normlarına uymalarını zorunlu kılmıştır[72]. NIS2, ulusal bilgisayar güvenlik ekiplerinin (CSIRT) oluşturulmasını, olay bildirimini ve denetim mekanizmalarını içermektedir.[73]

1. Risk Temelli Yaklaşımın Değerlendirilmesi

Direktifte risk sınıflandırması *"kritik kuruluşlar (essential entities)"* ve "*önemli kuruluşlar (important entities)"* şeklinde yapılmaktadır. Avrupa Birliği Yapay Zekâ Tüzüğü (EU AI Act)'nde ise risk temelli yaklaşım, daha detaylı şekilde ele alınmıştır. Düzenlemede sistemler; risk olmayan, düşük riskli, sınırlı riskli, yüksek riskli ve kullanımı yasak uygulamalar şeklinde ele alınmıştır. [74] Henüz yürürlüğe girmeyen Yapay Zekâ Kanun Teklifinde risk temelli yaklaşım "diğer sistemlerden daha fazla risk taşıyan yüksek riskli sistemler" olarak ele alınmış ve bu yapay zekâ sistemlerine karşı özel önlemler alınması gerektiği ifade edilmiştir.[75]

7545 sayılı Kanunda ise kritik altyapı tesislerine yönelik siber güvenlik önlemlerinde risk analizlerinin yapılması gerektiği ifade edilmekte, sistemlere yönelik herhangi bir risk sınıflandırması yer almamaktadır. [76]

---

71 **MARKOPOULOU** Dimitra, **PAPAKONSTANTINOU** Vagelis & **HERT** Paul De. (2019). "The NIS Directive, ENISA's Role and the General Data Protection Regulation", Computer Law & Security Review, (35), s. 2.

72 European Parliament and of The Council, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union", Official Journal of the European Union, L 333, 27 december 2022.

73 European Parliament and of The Council, Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2), Official Journal of the European Union, L 333, 27 december 2022, m. 9.

74 European Parliament and of The Council, "Artificial Intelligence Act", Official Journal of the European Union, L 1689, 2024, m European Parliament and of The Council, European Parliament and of The Council,d. 5, 6.

75 Türkiye Büyük Millet Meclisi, Yapay Zekâ Kanunu Teklifi, https://www.tbmm.gov.tr/Yasama/KanunTeklifi/e21539a0-888a-4500-81be-01904a918c53 Erişim Tarihi: 13.05.2025.

76 7545 sayılı Kanun m.5

2. Bildirim Yükümlülüğü

Direktife göre, kritik veya önemli kuruluşlar siber güvenliğe ilişkin önemli bir olayı tespit ettiklerinde gecikme olmaksızın ve her halükârda 24 saat içinde bir erken uyarı bildirimi vermek zorundadırlar.[77] Yapılan erken uyarının ardından ise gecikmeksizin ve her halükârda 72 saat içinde olay bildirimi ve olaya ilişkin değerlendirme yapılması yükümlülüğü de bulunmaktadır.[78]Nihai rapor ise, olay bildiriminin yapılmasından itibaren 1 ay içinde sunulmalıdır. Direktifte yer alan bildirim hükümleri incelendiğinde erken uyarı ve olay bildirimi mekanizmalarının işletildiği ve böylece siber güvenliğin sağlanmasına ilişkin proaktif ve reaktif yaklaşımların bulunduğu görülmektedir.

Yapay zekâ sistemlerinin kullanılmasından kaynaklı meydana gelen ihlallere ilişkin bildirim yükümlüğüne ilişkin süreler Avrupa Birliği Yapay zekâ Kanunu (AI Act)'nda da yer almaktadır. Düzenlemeye göre, genel bildirim süresi yapay zekâ sistemi ile meydana gelen olay arasında nedensellik bağı kurulmasından itibaren 15 gündür. [79]Düzenlemeye göre, yaygın ihlal ya da ciddi bir durumun gerçekleşmesinde derhal veya olayın öğrenilmesinden itibaren en geç iki gün içinde bildirim yükümlülüğü getirilmiştir. [80]Yüksek riskli yapay zekâ sistemlerinin kullanılmasından kaynaklanan ölüm olaylarında, nedensellik bağı kurulmasında derhal ve her hâlükârda olayın öğrenilmesinden itibaren on gün içinde rapor sunulmalıdır.[81]Düzenlemede zamanında bildirim yapılamayacak olması halinde, belirtilen süreler içinde eksik bir raporun sunulabileceğini ve ardından bu eksiğin tamamlanarak giderilebileceği ifade edilmektedir.[82]

Bildirim yükümlülüğü, 7545 sayılı Siber Güvenlik Kanununda siber güvenliğe ilişkin bir zafiyetin tespit edilmesi ve siber olaylara ilişkin bir olayın meydana gelmesi halinde durumun "*gecikmeksizin"* Siber Güvenlik Başkanlığına bildirilmesi şeklinde düzenlenmiştir. [83]

Yapay Zekâ Kanun Teklifinde ise bildirim yükümlülüğüne ilişkin ayrıntılı bir düzenleme bulunmamakta, yapay zekâ operatörlerinin de-

---

77 European Parliament and of The Council Directive (EU), 2022/2555, m 23/4(a).

78 Parliament and of The Council Directive (EU), 2022/2555, m 23/4(b).

79 European Parliament and of The Council, "Artificial Intelligence Act , Art. 73(2).

80 Art. 73(3).

81 Art. 73(4).

82 Art. 73(5).

83 7545 sayılı Kanun, m. 7/1-b.

netim makamlarını yanlış bilgilendirmesi halinde haklarında para cezası kararı verileceği ifade edilmiştir.[84]

3. Denetim Mekanizması

Direktife göre her üye devlet, NIS2 hükümlerinin uygulanmasının kontrolü için bir veya birden fazla yetkili makam atamalıdır. [85]NIS2 Direktifine göre siber olayların tespiti ve siber sorunların çözümü amacıyla ulusal bilgisayar güvenlik ekipleri (CSIRT) kurulmuş, siber olayların bu ekiplere bildirilerek ekiplerin bildirim içeriğine derhal ulaşması ve ilgili bilgi trafiğini yönetebilmesi yetkisi verilmiştir. [86]Ayrıca her ülke, NIS2 kapsamında ulusal düzeyde bir irtibat noktası (SPoC) oluşturmakla yükümlüdür. Bu irtibat noktaları sayesinde Ulusal Bilgisayar Güvenlik Ekipleri (CSIRT) ile yetkili makamlar arasında veri ve bilgi akışı sağlanmaktadır.[87]

Avrupa Birliği Siber Güvenlik Ajansı (ENISA) ise Avrupa Birliğinin siber güvenlik politikalarını belirlemekte ve bu alanda devletler arası iş birliği sürecini yürütmektedir. Ajans, NIS2'nin uygulanması sürecinde üye devletlere teknik rehberlik yapma görevini yürütmektedir[88].

AI Act'e göre denetim mekanizmaları ulusal düzeyde, Birlik düzeyinde ve bağımsız uygunluk değerlendirme kuruluşu düzeyinde olmak üzere ayrılmaktadır.

Ulusal Pazar Gözetim Otoriteleri, her üye devlet tarafından kendi ulusal sınırlarında denetim yapılması amacıyla belirlenmekte ve yapay zekâ sistemlerinin uygunluk durumlarının denetleyen, uyumsuz sistemlerin piyasadan çekilmesi veya faaliyetlerinin durdurulmasını sağlayan, gerektiğinde idari yaptırım uygulayan mekanizmalar olarak karşımıza çıkmaktadır. [89]

Yapay zekâ sistemleri AB genelinde bilgi ve birikimi geliştirmek, ülkelerin bu alanda yetkinliğini artırmak amacıyla Avrupa Yapay Zekâ

---

84 Türkiye Büyük Millet Meclisi, Yapay Zekâ Kanunu Teklifi, m. 6.

85 European Parliament and of The Council, "Directive (EU) 2022/2555 Art. 8(1).

86 Art. 9.

87 Art. 11(2).

88 Art. 7(4)

89 Artificial Intelligence Act, m. 74.

Ofisi (AI Office)kurulmuştur.[90]Ofis, risk analizi ve risk yönetimi [91]ile genel amaçlı sistemlerde denetim ve uyum izleme yetkisine sahiptir. [92]Ofisin ayrıca Avrupa Yapay Zekâ Kurulu toplantılarının gündemini hazırlama görevi bulunmaktadır. [93]

Bir başka denetim mekanizması olan Uygunluk Denetim Kuruluşları AB veya ulusal akreditasyon kurumları tarafından yetkilendirilmiş kuruluşlardır. Bu kuruluşlar, yüksek riskli yapay zekâ sistemlerinin mevzuata uygunluğunu denetleyerek uygunluk değerlendirmesi sonucunda CE belgesi [94]vermekte veya ret yönünde karar verilmektedir.[95]

Türkiye'deki denetim mekanizmaları incelendiğinde, Yapay Zekâ Kanun Teklifi metninde denetim mekanizmaları ibaresinin geçtiği fakat "*denetim mekanizmalarının*" hangi kurum veya kuruluşlar olduğunun belirtilmediği görülmektedir. 7545 sayılı Siber Güvenlik Kanunu'nda denetim yetkisinin verildiği kuruluşun Siber Güvenlik Başkanlığı olduğu belirtilmiştir. Kanuna göre Başkanlığın, "*Siber güvenlik denetimini gerçekleştirmek ve sonucuna göre yaptırım uygulamak ,kamu kurum ve kuruluşları ile kritik altyapılarda kullanılacak siber güvenlik ürün ve hizmetleri ile bunları sağlayacak işletmelerin taşıması gereken niteliklere yönelik teknik kriterler belirlemek ve mevzuat düzenlemeleri yapmak, bunların denetimini yapmak ya da yaptırmak, denetimleri yapacak kuruluşların taşımaları gereken nitelikleri belirlemek, bu kuruluşları görevlendirmek, gerektiğinde görevlendirmeyi geçici olarak durdurmak ya da iptal etmek*" görevleri bulunmaktadır.[96]

"Başkanlık, denetim yetkisi kapsamında bağımsız denetçiler ve bağımsız denetim kuruluşlarını yetkilendirebilir."[97] *"Mülki amirler, kolluk kuvvetleri ve diğer kamu kurumlarının amir ve memurları inceleme veya denetimle görevlendirilenlere her türlü kolaylığı göstermek ve yardımda bulunmakla yükümlüdürler."*[98]

Avrupa Birliği ile Türkiye'nin siber güvenliğe ilişkin oluşturduğu sistemler karşılaştırıldığında, siber olaylara yönelik müdahale sürecinde AB bünyesindeki CSIRT ve Türkiye bünyesinde USOM'ların işlevsel olarak benzerlik gösterdiği ; siber güvenliğin sağlanmasında teknik rehberlik

---

90 Art. 64.
91 Art.56.
92 Art. 75.
93 Art. 65.
94 Art. 129.
95 Art. 43.
96 7545 sayılı Kanun, m. 5/1-h, ı.
97 m. 6/1-ğ.
98 m. 8/3.

görevini üstlenen kuruluşlar incelendiğinde AB düzeyinde stratejik rehberlik sağlayan ENISA ve Türkiye'de politika ve strateji geliştirme konusunda yetkili olan Siber Güvenlik Kurulu arasında görev tanımları açısından benzerlik bulunduğu görülmektedir. ENISA, siber güvenlik alanına ilişkin standartların belirlenmesi yetkisi açısından Siber Güvenlik Başkanlığı ile de benzerlik göstermektedir. Ulusal Pazar Gözetim Otoriteleri ile Siber Güvenlik Başkanlığı, uygulayıcı denetim otoriteleri olmaları açısından önem taşımaktadır. Kurumlar, uyumsuzluk tespiti ve yaptırım uygulama yetkisine sahip olmaları açısından benzerlik taşımaktadır. Başkanlık, sistemlerin siber güvenlik standartlarına uyumunu denetleyebilmekte veya bunun yerine getirilmesi için bağımsız denetçi veya denetim kuruluşlarını yetkilendirebilmektedir. Başkanlık bu yönden, AI Act'te yer alan uygunluk denetim kuruluşları ile benzer nitelik göstermektedir.

SONUÇ

Türkiye'nin siber güvenlik politikalarının evrimi, dijital dönüşümün getirdiği zorluklara karşı gösterdiği tepkinin bir yansıması olarak değerlendirilebilir. 1990'lı yılların başında internetin toplumsal hayata girmesiyle birlikte bilişim suçları ekseninde şekillenen hukuki yaklaşımlar, zamanla daha kurumsal, stratejik ve kapsamlı bir siber güvenlik mimarisine dönüşmüştür. Bu dönüşümde en kritik eşik, 2025 yılında yürürlüğe giren 7545 sayılı Siber Güvenlik Kanunu olmuştur. Kanun, Türkiye'nin dağınık, yönetmeliklere dayalı ve büyük ölçüde sektörel strateji belgeleri ile sınırlı olan siber güvenlik yaklaşımını bir bütünlük içerisine taşımıştır. Bu bağlamda, Siber Güvenlik Kurulu, USOM, SOME'ler ve nihayetinde Siber Güvenlik Başkanlığı, siber güvenlikte koordinasyon, denetim ve stratejik yönlendirme fonksiyonlarını üstlenmiştir. Türkiye, bu kurumsal yapılar aracılığıyla Avrupa Birliği (AB) ile fonksiyonel düzeyde paralellik gösteren bir yapıya ulaşmayı başarmıştır.

Türkiye'nin siber güvenlik stratejisi, AB'nin NIS/NIS2 Direktifleri, AI Act gibi güncel düzenlemeleri ile karşılaştırıldığında önemli benzerlikler içerdiği kadar, dikkat çeken farklılıklar da barındırmaktadır. AB'nin detaylı risk sınıflandırmaları, bildirim yükümlülükleri ve çok katmanlı denetim sistemleri Türkiye'deki daha genel ve esnek çerçeveyle tezat oluşturmaktadır. Özellikle NIS2 Direktifinde yer alan "*kritik*" ve "*önemli*" kuruluşların ayrımı, 24 saat içinde yapılması gereken erken uyarı bildirimi, ardından 72 saat içinde olay bildirimi gibi süreçlerin belirgin şekilde düzenlenmiş olması, Türkiye'deki mevzuatın geliştirilmesi gerektiğini

ortaya koymaktadır. Türkiye'nin "*gecikmeksizin*" bildirim yapılmasını öngören genel ifadeleri, uygulamada zaman ve sorumluluk belirsizliklerine yol açabilir. Ayrıca, AI Act kapsamında yüksek riskli yapay zekâ uygulamalarına getirilen yükümlülükler, Türkiye'nin henüz başlangıç aşamasında olan Yapay Zekâ Kanun Teklifinde oldukça yüzeysel yer almaktadır. Bu durum, Türkiye'nin yapay zekâ kaynaklı siber tehditlere karşı hazırlık düzeyinin düşük olduğu izlenimini vermektedir.

7545 sayılı Kanun'un getirdiği kurumsal yapı ve yetki dağılımı, siber güvenlikte merkezi bir otorite olarak yer alacak Siber Güvenlik Başkanlığı tesis edilmesini sağlamış, bu başkanlık birçok açıdan Avrupa'daki ENISA ile benzerlik göstermeye başlamıştır. Ancak Türkiye'de siber güvenlik uygulamalarının düzenleyici netlik, denetim mekanizmalarının bağımsızlığı ve hesap verilebilirlik açısından geliştirilmesi gerekmektedir.

Kanunda yer alan *"hesap verilebilirlik"* ilkesi, soyut düzeyde tanımlanmış; hangi koşullarda, ne tür bir şeffaflık ve sorumluluk mekanizmasının işleyeceği ise açık bırakılmıştır. Aynı şekilde, bildirilen olaylara dair geri bildirim süreci, kamuya açık raporlama yükümlülüğü gibi demokratik hesap verebilirlik araçları eksiktir. Bu araçların siber güvenlik alanında varlığı hem kamuoyunun bilinçlendirilmesi hem de kurumsal güvenin sağlanması açısından kritik önem taşımaktadır.

Siber güvenlik politika ve stratejilerinin yürütülmesinden tüm kamu kurum ve kuruluşları ile gerçek ve tüzel kişilerin sorumlu olması Kanunun getirdiği önemli ilkeler arasında yer almaktadır. Ancak bu ilkede belirtilen kamu-özel sektör iş birliğinin uygulamada ne düzeyde işleyeceği henüz öngörülememektedir. Özellikle yerli ve milli yazılımlar geliştiren firmalara yönelik teşviklerin artırılması, bu ürünlerin bağımsız denetim mekanizmalarından geçirilerek kamu sistemlerine entegre edilmesi gerekmektedir. Akademi, sivil toplum ve özel sektör arasındaki bilgi ve veri paylaşım protokolleri de açık biçimde tanımlanmalı, güven esaslı bir iş birliği çerçevesi oluşturulmalıdır.

Türkiye'nin siber güvenlik alanında yapısal ihtiyaçları arasında yetişmiş insan kaynağı oluşturmak bulunmaktadır. Nitelikli uzman eksikliği hem denetim mekanizmalarının işletilmesini zorlaştırabilmekte hem de SOME ve USOM gibi yapıların etkinliğini sınırlayabilmektedir.

Türkiye kendi siber güvenlik politikasını oluştururken, ilköğretimden itibaren dijital vatandaşlık ve siber farkındalık eğitimlerinin zorunlu ders olarak müfredata entegre edilmesi, üniversitelerde yer alan siber güvenlik ve yapay zekâ hukuku bölümlerinin hızla artırılması, Kadınların ve dezavantajlı grupların siber güvenlik sektörüne entegrasyonunu artıracak sosyal programlar tasarlanması yolunda adımlar atılması toplumsal bilinci güçlendirerek siber vatandaşlık anlayışının hayata geçmesine katkı sağlayacaktır.

Siber güvenlik, sadece bir teknik savunma hattı değil; ulusal egemenliğin, ekonomik istikrarın ve birey haklarının korunması açısından da stratejik bir alandır. Bu nedenle Türkiye'nin Avrupa Birliğinin risk temelli yaklaşımını dikkate alması ve oluşturduğu mevzuatta bu yaklaşıma ayrıntılı olarak yer vermesi gerekliliği bulunmaktadır.

Kanunda yer alan Kanun kapsamında yer alan mercilere yönelik "*tespit ettikleri zafiyet veya siber olayları gecikmeksizin Başkanlığa bildirmek*" ifadesi açıklığa kavuşturulmalı, belirsizliklerin önüne geçmek için net süreler mevzuata eklenmelidir.

ENISA ve benzeri kuruluşlarla sürekli bilgi ve uzman değişimi sağlanmalı; Türkiye'nin NATO, OECD ve G20 platformlarında siber güvenlik konularında daha aktif rol alması teşvik edilmelidir. Türkiye'nin bu alanda etkin olması, uluslararası iş birliğinin sağlanması açısından oldukça önem taşımaktadır.

Kritik altyapılar için belirli periyotlarla ulusal düzeyde siber tatbikat yapılması ve bu tatbikatlar sonucunda yayımlanan raporların kamuoyuyla paylaşılmasının ise siber güvenlik alanında Türkiye'nin siber dayanıklılığını artırması öngörülmektedir.

Sonuç olarak,7545 sayılı Kanun Türkiye'nin dijital egemenlik iddiasını destekleyen stratejik bir dönüm noktası olarak karşımıza çıkmaktadır. Ancak bu düzenlemenin tam anlamıyla işlevsellik kazanması, sadece yasal metinle değil; kurumsal yapıların etkinliği, insan kaynağının niteliği, toplumsal farkındalık düzeyi ve uluslararası iş birliği kapasitesi ile mümkündür. AB'nin NIS2 ve AI Act gibi çok katmanlı ve yönetişime dayalı modelleriyle bütünleşmek, bu bütünleşme sürecinde siber güvenlik alanında kendi yapısına uygun gerçekleştireceği özgün dokunuşlar ile

bir siber güvenlik politikası oluşturmak Türkiye'yi siber güvenlikte sadece savunmacı değil; aynı zamanda yönlendirici ve standart belirleyici bir ülke konumuna getirebilecektir.

KAYNAKÇA

AKINTOLA, Adeyemi Samuel (2024). Integrating research testbeds, attack mechanisms, and defence strategies into a holistic framework for cybersecurity. Journal of Computer Science Review and Engineering, 8(2), 1–12. https://doi.org/10.5281/zenodo.14543273

ANDERSON Ross, Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley, Indianapolis, 2020, s. 283.

ARQUILLA, John., & **RONFELDT**, David. (Eds.). (2001). Networks and netwars: The future of terror, crime, and militancy. RAND Corporation. https://www.rand.org/pubs/monograph_reports/MR1382.html

AYTEKİN, Akın. (2015). Türkiye'nin siber güvenlik stratejisi ve eylem planının değerlendirilmesi (Yüksek lisans tezi, Gazi Üniversitesi, Bilişim Enstitüsü). Yükseköğretim Kurulu Ulusal Tez Merkezi. https://tez.yok.gov.tr/

BALDWIN, David. A. (1997). The concept of security. Review of International Studies, 23(1), 5–26. https://dbaldwin.scholar.princeton.edu/sites/g/files/toruqf4596/files/dbaldwin/files/baldwin_1997_the_concept_of_security.pdf

BARRINHA André & **RENARD**, Thomas. (2017). "Cyber-diplomacy: the making of an international society in the digital age", Global Affairs, (3)4–5, s. 353–364. https://doi.org/10.1080/23340460.2017.1414924 Erişim tarihi: 12.05.2025.

BARUN Başak. (2024). "The Impact of Cybersecurity Threats on National Security: Strategies", International Journal of Humanities Social Science and Management,s. 1361.

BAYUK, Jennifer **L./HEALEY,** Jason**/ROHMEYER,** Paul**/SACHS,** Marcus **H./SCHMIDT,** Jeffrey**/WEISS,** Joseph**:** Cyber Security Policy Guidebook, John Wiley & Sons, Hoboken 2012.LEWIS,

BIÇAKCI Salih, **ERGUN** Doruk & **ÇELİKPALA** Mitat, "Türkiye'de Siber Güvenlik", EDAM Siber Politika Kağıtları Serisi, EDAM Yayınları, 2015, s. 30. https://edam.org.tr/wp-content/uploads/2015/12/EDAM_TR_Siber_Guv_1.pdf. Erişim tarihi: 08.05.2025.

BOZKURTLAR Burak, Ulus Devletlerin Siber Güvenlik Stratejileri ve Siber Vatan, Siber Vatan, 2021, s. 1–22. https://www.academia.edu/

BTK AKADEMİ: BTK Akademi Eğitim Portalı, https://www.btkakademi.gov.tr/portal (Erişim Tarihi: 08.05.2025).

CRAIGEN, Dan**/DIAKUN-THIBAULT,** Nadia**/PURSE,** Randy. (2014). Defining Cybersecurity. *Technology Innovation Management Review, (4)*10, s. 15.

ÇAKIR Hüseyin & **TAŞER** Murat. (2023). "Türkiye'de Yapılan Siber Güvenlik Faaliyetlerinin ve Eğitim Çalışmalarının Değerlendirilmesi", Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji, (11)2, s. 348. https://doi.org/10.29109/gujsc.1165131 Erişim tarihi: 13.05.2025.

ELDEM Tuba, Between Multi-stakeholderism and Cyber Sovereignty: Understanding Turkey's Cybersecurity Strategy, EDAM Cyber Policy Paper Series, No. 2021/1, İstanbul, 2021.

EL-ZUGHAID, Aya Issa, **FUNOUSH**, Zuhayr A., **YOUNIS** A. & **ALGHAMDİ** Mohammed Yahya, (2024). "A Zero Trust Framework to Secure IoT Devices", University of Ha'il – Journal of Science, 5(2), s. 51.

EUROPEAN PARLIAMENT AND OF THE COUNCIL "Artificial Intelligence Act", Official Journal of the European Union, L 1689, 2024, m European Parliament and of The Council, European Parliament and of The Council,d. 5, 6.

EUROPEAN PARLIAMENT AND OF THE COUNCIL, "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS

Directive)", Official Journal of the European Union, L 194, 19 July 2016, s. 1–30.

EUROPEAN PARLIAMENT AND OF THE COUNCIL, "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union", Official Journal of the European Union, L 333, 27 december 2022.

HEKİM, Hakan., & **BAŞIBÜYÜK,** Oğuzhan. (2013). Siber suçlar ve Türkiye'nin siber güvenlik politikaları. Uluslararası Güvenlik ve Terörizm Dergisi, 4(2), 135–158. https://search.trdizin.gov.tr/tr/yayin/detay/150969/

HOHMANN Mirko, **PIRANG** Alexander & **BENNER** Thorsten, Advancing Cybersecurity Capacity Building: Implementing a Principle-Based Approach, Global Public Policy Institute (GPPi), Berlin, 2017.

I**NTERNATİONAL TELECOMMUNICATION UNION DEVELOPMENT SECTO**R, Global Cybersecurity Index 2024 – 5th Edition, Eylül 2024. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx Erişim tarihi: 12.05.2025.

KOÇAK, Hüseyin. (2020). Dijital çağda iletişim güvenliği ve toplum. Journal of Social, Humanities and Administrative Sciences, 6(34), 2302.

KUEHL Daniel T, "From Cyberspace to Cyberpower: Defining the Problem", **KRAMER** Franklin D., **STARR** Stuart H. & **WENTZ** Larry K. (Ed.), Cyberpower and National Security, Washington DC, 2009, s. 24–42.

KUNER, Christopher, "Data Nationalism and Its Discontents", Emory Law Journal Online, 64, 2015, s. 2089. https://scholarlycommons.law.emory.edu/elj-online/25. Erişim tarihi: 08.05.2025.

KUZEY ATLANTİK ANTLAŞMASI ÖRGÜTÜ (NATO). Warsaw Summit Communiqué, 9 Temmuz 2016. https://www.nato.int/cps/en/natohq/official_texts_133169.htm. Erişim tarihi: 08.05.2025.

LEWIS, James Andrew. (2011). Cybersecurity: Assessing the immediate threat to the united states. *Testimony Before the US House Oversight and Government Reform Committee, 3*(4), 14. https://www.csis.org/analysis/cybersecurity-assessing-immediate-threat-united-states

MARKOPOULOU Dimitra, **PAPAKONSTANTINOU** Vagelis & **HERT** Paul De. (2019). "The NIS Directive, ENISA's Role and the General Data Protection Regulation", Computer Law & Security Review, (35), s. 2.

NOGHONDAR,Elham Rajabian "Importance of Human Factors on Cybersecurity within Organizations", 2023. https://personales.upv.es/thinkmind/dl/conferences/securware/securware_2022/securware_2022_1_10_30004.pdfErişim tarihi: 09.05.2025.

QUDUS, Lawal (2025). Resilient Systems: Building Secure Cyber-Physical Infrastructure for Critical Industries Against Emerging Threats. International Journal of Research Publication and Reviews (6)1, s. 3330.

RIBBLE, Mike S., **BAILEY**, Gerald, D., & **ROSS**, Tweed, W. (2004, September). Digital citizenship: Addressing appropriate technology behavior. Learning & Leading with Technology, 32(1), 6–9, 11. https://files.eric.ed.gov/fulltext/EJ695788.pdf

ROSHANAEI, Maryam. (2021). Resilience at the core: Critical infrastructure protection challen-ges, priorities and cybersecurity assessment strategies. Journal of Computer and Communications, 9(8), 80–102. https://doi.org/10.4236/jcc.2021.98006

SHARMA, Anuj (2022). "Cyber Terrorism: A Growing Threat to India's Cyber Security". Indian Journal of Cyber Law (5)2, s. 61.

STEINER, Hrafn. (2016). Cyber-attacks as coercive instruments. Analys & Perspektiv, (3), 148. https://kkrva.se/artiklar/cyber-attacks-as-coercive-instruments/

T.C. CUMHURBAŞKANLIĞI DİJİTAL DÖNÜŞÜM OFİSİ, Bilgi ve İletişim Güvenliği Rehberi, Ankara, 2020. https://assets.kpmg.com/content/dam/kpmg/tr/pdf/2020/08/bilgi-iletisim-guvenligi-rehberi.pdf (Erişim tarihi: 08.05.2025).

T.C. CUMHURBAŞKANLIĞI DİJİTAL DÖNÜŞÜM OFİSİ, Strateji ve Eylem Planı (2024–2028), Ankara, 2024, s. 26. Erişim tarihi: 09.05.2025.

T.C. RESMİ GAZETE, "Siber Güvenlik Başkanlığı Hakkında Cumhurbaşkanlığı Kararnamesi (Kararname No: 177)", Resmî Gazete, 08 Ocak 2025, Sayı: 32776.

T.C. RESMÎ GAZETE,1 Sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi", 10 Temmuz 2018, Sayı: 30474. https://www.resmigazete.gov.tr/eskiler/2018/07/20180710-1.pdf. Erişim tarihi: 08.05.2025.

T.C. RESMÎ GAZETE. (2012, 20 Ekim). 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının yürütülmesi, yönetilmesi ve koordinasyonuna ilişkin karar. https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18.htm (Erişim tarihi: 08.05.2025).

T.C. RESMÎ GAZETE. (2013, 20 Haziran). 2013/4890 sayılı Ulusal Siber Güvenlik Stratejisi ve 2013–2014 Eylem Planı hakkında Bakanlar Kurulu kararı. https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm

T.C. RESMÎ GAZETE. (2025, 19 Mart). 7545 sayılı Siber Güvenlik Kanunu. Resmî Gazete (Sayı: 32846). https://www.resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm

T.C. ULAŞTIRMA VE ALTYAPI BAKANLIĞI. (2020). Ulusal Siber Güvenlik Stratejisi ve 2020–2023 Eylem Planı. Ankara.

TAGAREV Todor & **SHARKOV** George. (2016). "Multi-Stakeholder Approach to Cybersecurity and Resilience", Information & Security: An International Journal, (34)1, s. 60

TÜRKİYE BÜYÜK MİLLET MECLİSİ, 7545 Sayılı Siber Güvenlik Kanunu Teklifi, https://www.tbmm.gov.tr/Yasama/KanunTeklifi/af1dfbdb-e3e3-4820-a493-0194504c63b4 Erişim tarihi: 12.05.2025.

TÜRKİYE BÜYÜK MİLLET MECLİSİ, Yapay Zekâ Kanunu Teklifi, https://www.tbmm.gov.tr/Yasama/KanunTeklifi/e21539a0-888a-4500-81be-01904a918c53 Erişim Tarihi: 13.05.2025.

ULAŞTIRMA VE ALTYAPI BAKANLIĞI. Ulusal Siber Güvenlik Stratejisi ve 2024–2028 Eylem Planı. Ankara, 2024. https://www.uab.gov.tr/uploads/pages/ulusal-siber-guvenlik-stratejisi/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2024-2028.pdf. Erişim tarihi: 08.05.2025.

ULAŞTIRMA, DENİZCİLİK VE HABERLEŞME BAKANLIĞI. Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. https://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1.htm (Erişim tarihi: 08.05.2025).

ULAŞTIRMA, DENİZCİLİK VE HABERLEŞME BAKANLIĞI. Ulusal Siber Güvenlik Stratejisi ve 2016–2019 Eylem Planı. Ankara, 2016. https://www.resmigazete.gov.tr/eskiler/2016/10/20161020-1.htm. Erişim tarihi: 08.05.2025.

WIENER, Norbert. (1975). Emek, sibernetik ve toplum (İ. Keskin, Çev.). İstanbul: Özgün Yayınları. (Orijinal eser 1948'de yayımlanmıştır).