TÜRKİYE'NİN SİBER GÜVENLİK POLİTİKALARI[1]

Prof. Dr. Ozan ÖRMECİ[2]

Öz: Bu çalışma, Türkiye'nin siber güvenlik politikalarının 2013-2028 döneminde geçirdiği kurumsal ve hukuki dönüşümü, ulusal güvenlik ve siber dayanıklılık perspektifinden incelemektedir. Araştırmanın temel sorusu, Türkiye'nin siber güvenlik alanında geliştirdiği strateji, kurum ve mevzuatın kritik altyapıların korunması, kurumsal koordinasyon, caydırıcılık ve uluslararası iş birliği bakımından nasıl bir politika modeli ortaya koyduğudur. Çalışmada nitel doküman analizi yöntemi kullanılmış; ulusal strateji belgeleri, mevzuat, kurumların görev tanımları ve konuya ilişkin akademik çalışmalar amaçlı örnekleme yoluyla değerlendirilmiştir. Analiz, Türkiye'nin 2025 yılında Siber Güvenlik Başkanlığı'nın kurulması ve 7545 sayılı Siber Güvenlik Kanunu'nun kabulüyle merkezi koordinasyonu güçlendiren yeni bir kurumsal aşamaya geçtiğini göstermektedir. Bununla birlikte, kurumlar arası görev paylaşımı, uygulama kapasitesi, kritik altyapılarda ölçülebilir dayanıklılık, nitelikli insan kaynağı ve yerli teknolojilerin sürdürülebilirliği bakımından politika hedefleri ile uygulama sonuçları arasında değerlendirilmesi gereken alanlar bulunmaktadır. Çalışmanın özgün katkısı, Türkiye'nin siber güvenlik mimarisini yalnızca kurum ve mevzuat envanteri olarak sunmak yerine, güvenliğin genişlemesi ve siber caydırıcılık yaklaşımları çerçevesinde koordinasyon, kapasite ve dış iş birliği eksenlerinde değerlendirmesidir.

Anahtar Kelimeler: *Siber Güvenlik, Türkiye, Siber Caydırıcılık, Kritik Altyapılar, Siber Güvenlik Başkanlığı*.

Makale Geliş Tarihi: 28.10.2026

Makale Kabul Tarihi: 11.11.2026

DOI: 10.5281/zenodo.24254394

[1] Bu çalışmanın bazı bölümleri şu önceki çalışmadan özetlenmiştir; Ozan Örmeci & Eren Alper Yılmaz & Ahmet Emre Köker (2022), "Turkey's Cyber Security Policies", içinde *Cyber Environment and International Politics* (editörler: Hasret Çomak & Burak Şakir Şeker & Yaprak Civelek & Çağla Arslan Bozkuş), Londra: TPLondon, ss. 67-91.

[2] Siyaset Bilimi Profesörü, Uluslararası Politika Akademisi (UPA) Genel Koordinatörü, ESUPA (Elektronik Sanat ve Uluslararası Politika Enstitüsü) Başkanı.
Email: ozanormeci@gmail.com.
ORCID: 0000-0001-8850-6089.

TÜRKİYE'S CYBERSECURITY POLICIES

Abstract: This study examines the institutional and legal transformation of Türkiye's cybersecurity policies during 2013–2028 from the perspectives of national security and cyber resilience. It asks how Türkiye's strategies, institutions and legislation constitute a policy model in terms of critical infrastructure protection, institutional coordination, deterrence and international cooperation. The study employs qualitative document analysis, examining national strategy documents, legislation, institutional mandates and relevant academic studies selected through purposive sampling. The analysis indicates that the establishment of the Cybersecurity Presidency in 2025 and the adoption of Cybersecurity Law No. 7545 marked a new phase aimed at strengthening central coordination. Nevertheless, the relationship between policy objectives and implementation outcomes requires further assessment in areas such as inter-agency responsibilities, implementation capacity, measurable resilience of critical infrastructure, skilled human resources and the sustainability of domestic technologies. The study's contribution is to assess Türkiye's cybersecurity architecture not merely as an inventory of institutions and legislation, but through the analytical dimensions of coordination, capacity and external cooperation, informed by the expansion of security and cyber deterrence approaches.

Keywords: *Cybersecurity, Türkiye, Cyber Deterrence, Critical Infrastructure, Cybersecurity Presidency*.

Giriş

İnternet teknolojilerinin ve sosyal medyanın gelişmesiyle birlikte, son 30 yılda tüm sektörlerin ve yaşamın çeşitli alanlarının daha çok internet tabanlı veya çevrimiçi hale geldiği yadsınamaz bir gerçektir. Son Covid-19 (koronavirüs) pandemisi sırasında, çevrimiçi eğitim sistemlerinin hızla yayılması ve e-ticaretin patlamasıyla birlikte, internetin yoğun etkileri daha da belirgin hale geldi. İnternetin hayatı kolaylaştırdığı ve daha konforlu hale getirdiği şüphesizdir. Bu teknoloji, kişisel özgürlükleri önemli ölçüde arttırmıştır. Ancak, kötü niyetli, suçlu kişiler, terör örgütleri ve düşman devletler de internet özgürlüklerinden faydalanmaktadır. Bu nedenle, siber güvenlik son 20 yılda tüm devletler için büyük bir mesele haline gelmiştir. Gelişmekte olan bir ülke olarak, Türkiye de bu konuda istisna değildir ve bu nedenle internetin doğasında var olan koşullara uyum sağlamaya çalışmaktadır.

1990'ların başlarından itibaren, küreselleşme sürecinde bilgi kavramı büyük bir rol oynamıştır. Gelişmiş ülkelerde bilgi ve iletişim teknolojilerinin hızla yayılması ve devletlere yönelik tehditlere ilişkin yeni algılar nedeniyle "*güvenlik*" kavramı yeniden tanımlanmıştır. Organize suç, insan kaçakçılığı, yasadışı göç, kara para aklama vb. suç eylemleri uluslararası sistemin dengesini bozmuş ve devletler için yeni düşmanlar ortaya çıkmıştır. Özellikle 11 Eylül 2001 (9/11) felaketinden sonra artan gerilim, "*Dijital Felaket*" senaryolarına yol açmış ve Batı'ya karşı siber terörizm (siber terör) eylemleri korkusunu yaratmıştır. Son yıllarda, IŞİD/DEAŞ benzeri köktendinci terör örgütlerinin ortaya çıkışı da siber terörizm olgusuyla aynı zamana denk gelmiş ve bu tarz radikal örgütlerin faaliyetlerinde interneti özgürce kullanabilmeleri eleştirilere neden olmuştur.

Bu çalışma, Türkiye'nin siber güvenlik politikalarını ulusal güvenlik ve siber dayanıklılık bağlamında incelemektedir. Araştırmanın temel sorusu şudur: Türkiye'nin strateji belgeleri, kurumsal yapılanması ve mevzuatı; kritik altyapıların korunması, kurumlar arası koordinasyon, siber caydırıcılık ve uluslararası iş birliği bakımından ne ölçüde tutarlı ve işlevsel bir politika çerçevesi oluşturmaktadır? Bu soruya bağlı olarak, çalışma, Türkiye'de siber güvenlik yönetişiminin 2013-2028 dönemindeki gelişimini ve özellikle 2025 yılında ortaya çıkan kurumsal-hukuki dönüşümü değerlendirmeyi amaçlamaktadır. Araştırmanın kapsamı ulusal strateji belgeleri, ilgili mevzuat, Siber Güvenlik Başkanlığı ve diğer kamu kurumlarının görevleri ile NATO ve uluslararası iş birliği boyutlarıyla sınırlıdır. Yöntem olarak nitel doküman analizi

benimsenmiştir. Belgeler; (i) kurumsal yetki ve koordinasyon, (ii) kritik altyapıların korunması ve olaylara müdahale, (iii) caydırıcılık ve savunma kapasitesi, (iv) insan kaynağı ve yerli teknoloji, (v) uluslararası iş birliği ölçütleri üzerinden tematik olarak değerlendirilmiştir. Resmî belgeler politika hedeflerini ve hukuki yetki dağılımını; akademik çalışmalar ise bu hedeflerin kavramsal ve analitik bağlamını anlamak amacıyla kullanılmıştır. Kamuya açık performans verilerinin sınırlılığı nedeniyle, çalışma, kurumların operasyonel başarısına ilişkin ölçülmemiş nicel sonuçlar ileri sürmemekte; politika tasarımı ve kurumsal kapasite üzerinden nitel bir değerlendirme sunmaktadır.

Bu yaklaşımın literatüre katkısı, Türkiye örneğini yalnızca tarihsel gelişmelerin ve kurumların sıralandığı betimleyici bir anlatı olarak değil, güvenlik politikalarının genişlemesiyle ortaya çıkan yeni tehditlere verilen kurumsal yanıtın tutarlılığı üzerinden ele almasıdır. Güvenliğin genişlemesi yaklaşımı, siber alanın yalnızca teknik bir mesele olmadığını; ekonomik düzen, kamu hizmetleri, askerî kapasite, bireysel haklar ve siyasal istikrarla doğrudan ilişkili olduğunu göstermektedir. Siber caydırıcılık literatürü ise, saldırganın kimliğinin tespiti, misillemenin inandırıcılığı, savunma kapasitesi ve orantılılık gibi sorunların siber alanda caydırıcılığı güçleştirdiğine işaret etmektedir. Bu iki yaklaşım, aşağıdaki Türkiye incelemesinde analitik ölçütler olarak kullanılacaktır.

1. 'Siber' Kavramları

"*Siber*" (*Cyber*) terimi, genel olarak internet ve sanal ortamı olarak tanımlanan bilgisayarları, bilgisayar ağlarını ve bunlarla ilgili şeyleri ifade eder.[3] Ancak bu terim, literatürde sıklıkla "*siber uzay"* (*cyber space*) terimiyle eşanlamlı olarak kullanılmaktadır.Birleşmiş Milletler (BM), siber alanı "*genel olarak ağ olarak bilinen, internete bağlı bilgisayarların, iletişim altyapılarının, çevrimiçi konferans kuruluşlarının, veri tabanlarının ve bilgi hizmetlerinin küresel sistemler sistemi*" olarak tanımlar.[4] Bu, çoğunlukla internet anlamına gelir, ancak terim aynı zamanda bir ordunun, bir şirketin ve/veya bir hükümetin belirli ve sınırlı elektronik bilgi ortamını belirtmek için de kullanılabilir.[5]

Singer ve Friedman, siber uzay için temel bir tanım olarak, "*bilgisayarlardan füzelere ve güneşten*

[3] Merriam-Webster, "Cyber", Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.merriam-webster.com/dictionary/cyber.
[4] UNTerm, "Cyber space", Erişim Tarihi: 04.10.2026, Erişim Adresi: https://unterm.un.org/unterm2/en/.
[5] Jason Andress & Steve Winterfield (2014), *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Waltham, MA: Elsevier Inc., s. 4.

gelen ışınlara kadar elektronik ve elektromanyetik spektrumun kullanımının karakterize ettiği alan" ifadesini kullanmışlardır.[6] Başka bir tanıma göre ise, siber uzay, "*dünyanın ve uzayın tamamına yayılmış bilgi sistemlerinden, bu sistemleri birbirine bağlayan ağlardan veya bağımsız bilgi sistemlerinden oluşan sayısal ortamdır*."[7] Öte yandan, ABD Ordusu'nun Siber Uzay Operasyonlarına İlişkin Ulusal Askeri Stratejisi, siber uzayı "*elektronik ve elektromanyetik spektrumun ağ üzerinden veri depolamak, değiştirmek ve alışverişi yapmak için kullanıldığı alan*" olarak tanımlar.[8]

Siber uzay, fiziksel ve sanal olmak üzere iki bileşik yapıdan oluşur. Fiziksel yapı, her türlü bilgi ve iletişim sistemini içerir. Bunlar arasında dijital elektronik cihazlar, bilgisayarlar, akıllı telefonlar, akıllı nesneler, sensörler/dedektörler, uydu sistemleri ve tüm bilgisayar ağları yer almaktadır. Sanal yapı ise, özellikle fiziksel ortamdaki işletim sistemleri olmak üzere, yazılım ve kodlarla üretilen, depolanan, iletilen ve çeşitli amaçlar için kullanılan her türlü veri ve bilgiyi içerir.[9]

Siber uzayın karmaşıklığını anlayabilmek için, öncelikle, iki ayrı uygulama alanını birbirinden ayırarak başlayalım. İlk olarak, halkın günlük faaliyetlerine hizmet eden ve genellikle devlet dışı aktörlerin hedefi olan ticari interneti ele alalım. Bu alanın kırılganlığı, sırasıyla Nisan-Mayıs 2007 ve Ağustos 2008'de Estonya ve Gürcistan'da gerçekleşen siber saldırılarla ortaya çıktı. İkincisi, askeri ağlar ve diğer devletlerin güvenliğini tehdit edebilecek şekilde önem kazandı. Son 20 yılda, çeşitli devletlerin orduları, ağ merkezli savaş yoluyla savaş yeteneklerini geliştirmeye çalıştı. Örneğin, Carafano ve Sayers'a göre, Amerika Birleşik Devletleri'ne askeri olarak daha zayıf olan Çin Halk Cumhuriyeti (Çin) ve Rusya Federasyonu (Rusya) gibi devletler, ABD siber alanının kırılganlığını tespit etmiş ve casusluk yoluyla elde edilen askeri bilgilerden yararlanmak için ayrıntılı çalışmalar yürütmüştür.[10]

---

[6] P. W. Singer & Allan Friedman (2014), *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford: Oxford University Press, s. 13.
[7] Republic of Turkey Ministry of Transport Maritime Affairs, and Communications, *2016-2019 National Cyber Security Strategy,* Erişim Tarihi: 04.10.2026, Erişim Adresi: https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusalsibereng.pdf, s. 7.
[8] Jason Andress & Steve Winterfield (2014), *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, s. 3.
[9] Mustafa Şenol (2020), "Türkiye'nin Ulusal Siber Güvenlik Strateji ve Politikalarının Olusturulması Çerçevesinde Caydırıcılık", Doktora Tezi, İstanbul Teknik Üniversitesi, İstanbul, Türkiye, s. 9.
[10] James Carafano & Eric Sayers (2008), "Building Cyber Security Leadership for the 21st Century", The Heritage Foundation, 16.12.2008, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.heritage.org/defense/report/building-cyber-security-leadership-the-21st-century.

1.1. Siber Güvenlik

Siber güvenlik (*cyber security*), kurumların, kuruluşların ve kullanıcıların siber ortamdaki güvenlik risklerine karşı koyabilecek şekilde güvenlik özelliklerini oluşturmayı ve sürdürmeyi amaçlar. Bu tanım, personelini, altyapılarını, uygulamalarını, hizmetlerini, elektronik iletişim sistemlerini ve kurumların, kuruluşların ve kullanıcıların siber ortamında iletilen ve depolanan tüm bilgileri içerir.[11] Türkiye'nin 2016-2019 Ulusal Siber Güvenlik Stratejisi'ne göre, siber güvenlik, "*siber uzayı oluşturan bilgi sistemlerinin saldırılardan korunması, bu ortamda işlenen bilgi/verilerin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması, saldırıların ve siber güvenlik olaylarının tespit edilmesi, karşı önlem mekanizmalarının devreye sokulması ve sistemlerin siber güvenlik olayından önceki duruma geri döndürülmesi*" anlamına gelmektedir.[12]

Siber güvenliğin temel ilkeleri, ülkeleri siber risklere ve tehditlere karşı korumak için bilgi güvenliğinin özünü oluşturur. "*CIA üçgeni*" olarak bilinen gizlilik, bütünlük ve erişilebilirlik ilkelerinin herhangi birine zarar verilirse, güvenlik tehlikeye girer. Veriye ilişkin bu üç temel ilkeye zarar verildiğinde, bilgi sistemlerini içeren altyapılar can kaybına, büyük ölçekli ekonomik kayıplara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına neden olabilir.[13]

1.2. Siber Caydırıcılık

Genel olarak, caydırıcılığı (*deterrence*), "*diğerlerini düşmanca eylemlerde bulunmaktan caydırmak*" olarak açıklayan Libicki, siber caydırıcılığı (*cyber deterrence*) ise "*siber ortamda saldırganın eylemini cezalandırarak ve bir tür tehdit oluşturarak saldırganı siber saldırıdan caydırmak*" olarak tanımlar.[14]

Cezalandırıcı önlemler, düşmanın siber saldırganlığın maliyetlerinin faydalarından daha ağır basıp basmadığına dair hesaplamalarına katkıda bulunur. Iasiello'nun görüşüne göre, "*siber caydırıcılık, savunma yapan bir devletin, düşmanın karar alma mekanizmasını hedef alarak ve etkileyerek, ilk saldırganın daha büyük bir misillemeden korkması nedeniyle yıkıcı siber faaliyetlerde bulunmaktan kaçınmasını sağlayarak, düşmanca siber faaliyetleri caydırma niyetini işaret ederek*

[11] M. Emin Ulaşanoğlu & Ramazan Yılmaz & M. Alper Tekin (2010), *Bilgi Güvenliği: Riskler ve Öneriler*, Ankara: Bilgi Teknolojileri ve İletişim Kurumu (BTK), s. 8.
[12] Republic of Turkey Ministry of Transport Maritime Affairs, and Communications, *2016-2019 National Cyber Security Strategy,* Erişim Tarihi: 04.10.2026, Erişim Adresi: https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusalsibereng.pdf, s. 10.
[13] *A.g.e.*, s. 9.
[14] Martin C. Libicki (2009), *Cyber Deterrence and Cyberwar*, California: RAND Corporation, s. 28.

statükoyu korumaya çalıştığı bir stratejidir."[15]

Siber caydırıcılık, başarılı caydırıcılık sonuçlarına ulaşmak için uygulanması gereken birçok tekniği içerdiğinden, uygulanması oldukça zordur. Bir siber caydırıcılık stratejisinin, işleyişini sağlayan bazı temel parametrelere sahip olması gerekir.Bu parametreler olmadan, saldırgan savunmacının niyetini alıp işleyemez; bu nedenle devletler yanlış anlama veya yanlış yorumlama riskleriyle karşı karşıya kalabilir. Bu parametreler; iletişim, sinyal verme, atıf ve orantılılıktır.[16]

1.3. Siber Suç

Uluslararası bir sorun gibi görünen siber suç, genel olarak şu şekilde anlaşılmaktadır: "*Bilgilerin otomatik olarak işlenmesini içeren ve bilgisayarlar aracılığıyla veri aktarımı hakkındaki kanuna aykırılık teşkil eden eylemler*."[17] 2002 yılında, Suçun Önlenmesi ve Suçluların Islahı konulu Onuncu Birleşmiş Milletler Kongresi'nde, bu durum, "*bilgi sistemi güvenliğini/veri işlemlerini hedef alan ve bilgi sistemi/ağı aracılığıyla gerçekleştirilen yasadışı eylemler*" olarak tanımlanmıştır.[18]

Siber suç, suçluların hırsızlık yapmak veya başka türlü yasa dışı faaliyetlerde bulunmak için dijital araçları kullanması olarak da tanımlanır. En yaygın siber suç türü, kimlik bilgilerinin çalınması veya hesap bilgilerinin finansal ve ödeme sistemlerini dolandırmak için kötüye kullanılmasıdır. Bu sistemler arasında kredi kartları, ATM hesapları ve çevrimiçi bankacılık hesapları yer almaktadır.[19] Avrupa Konseyi Siber Suçlar Sözleşmesi (2004), yetkisiz erişim, sistemik müdahale ve dolandırıcılık suçlarına ek olarak, yaygın bilgi ve internet sistemlerini kullanan çocuk pornografisi ve telif hakkı ihlalleri gibi niceliksel olarak artan eylemlerin de siber suç kapsamına dahil olduğunu belirlemiştir.[20]

1.4. Siber Terörizm/Siber Terör

Günümüzün modern terör örgütleri, örgütlerini yapılandırmak, personel temin etmek ve eylemlerini

[15] Emilio Iasiello (2014), "Is Cyber Deterrence an Illusory Course of Action?", *Journal of Strategic Security*, 7(1), Bahar 2014, s. 55.
[16] *A.g.e.*, ss. 56-59.
[17] Hüseyin Çakır & M. Serkan Kılıç (2014), *Güncel Tehdit Siber Suçlar*, Ankara: Seçkin Yayınları, s. 50.
[18] Oğuzhan Turhan (2006), "Bilgisayar Ağları İle İlgili Suçlar", Planlama Uzmanlığı Tezi, DPT Müsteşarlığı, Ankara, Türkiye, s. 30.
[19] P. W. Singer & Allan Friedman (2014), *Cybersecurity and Cyberwar: What Everyone Needs to Know*, s. 85.
[20] Mehmet Yayla (2014), "Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı", *Hacettepe Hukuk Fakültesi Dergisi*, 4(2), s. 190.

organize etmek için bilgi teknolojilerini yaygın olarak kullanmaktadır. Bu tarz yapılar, kirli amaçlarına ulaşmak için, kamu ve özel kurumların bilgi sistemlerine karşı siber saldırılar düzenlemektedir. Özellikle 2000'li yıllarda yoğunlaşan siber terörizm (*cyber terrorism*) eylemleri, kilit kurumları hedef alarak gizli bilgi ve para akışını sağlamayı amaçlamaktadır. Yayla, siber terörizmi genel olarak şu şekilde tanımlar: "*Siyasi veya sosyal hedefleri gerçekleştirmek, devletleri ve vatandaşlarını tehdit etmek, devletleri politikalarını değiştirmeye zorlamak amacıyla bilgi teknolojisi olanaklarını kullanarak bilgisayarlara, ağ sistemlerine ve veri tabanlarına yönelik yasadışı tehditler ve zarar verici saldırılar*."[21] Amerikan Federal Soruşturma Bürosu (FBI) ise, siber terörizmi "*ulusal altı gruplar veya gizli ajanlar tarafından, savaşçı olmayan hedeflere karşı şiddete yol açan, bilgiye, bilgisayar sistemlerine, bilgisayar programlarına ve verilere yönelik önceden planlanmış, siyasi amaçlı bir saldırı*" olarak tanımlar.[22] Bu değerlendirme, yasadışı ve zarar verici saldırıları da içermektedir.

Jalil, siber terörizmi aşağıdaki kategoriler altında analiz etmektedir:[23]

Saldırı: Siber teröristlerin bu tarz eylemlerdeki temel amacı, bir ağa erişerek bilgi edinmek veya sistemdeki bilgileri değiştirerek karşı tarafa karşı avantaj sağlamaktır. Bu yöntem, çok yaygın ve yüksek başarı oranıyla geniş çapta kullanılmaktadır.

Yıkım: Buradaki asıl amaç, bilgisayar sistemlerini yok etmek veya zarar vermektir. Bu tür bir saldırının sonuçları korkunç olabilir; kuruluşlar büyük zarar görebilir. Saldırıların şiddeti nedeniyle belirsiz bir süre boyunca operasyonlardan uzak kalmak zorunda bile kalınabilir.

Dezenformasyon: Buradaki amaç, söylentiler yayarak ve bilgileri kirleterek devlet içinde korku ve kaos ortamı yaratmaktır. Bu tür saldırıları kontrol etmek çok zordur; çünkü hedefteki bilgisayar ve ağ sistemlerine erişime gerek kalmadan neredeyse anında gerçekleştirilebilir.

1.5. Siber Savaş

Siber savaş (*cyberwarfare*), temel olarak "*bir devletin başka bir devletin bilgisayar sistemlerine ve ağlarına sızarak zarar verme veya aksamaya neden olma eylemi*" anlamına gelir.[24] Bu tanıma

[21] *A.g.e.*, s. 195.
[22] P. W. Singer & Allan Friedman (2014), *Cybersecurity and Cyberwar: What Everyone Needs to Know*, s. 96.
[23] Shamsuddin Abdul Jalil (2003), "Countering Cyber Terrorism Effectively: Are We Ready to Rumble?", GIAC, Haziran 2003, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154, s. 8.
[24] Richard A. Clark & Robert K. Knake (2011), *Siber Savaş*, Çeviri: Murat Erduran, İstanbul: İstanbul Kültür

göre, siber savaş, devletler arasında siber uzayda gerçekleşir. Buna göre, Steven A. Hildreth tarafından 2001 yılında hazırlanan bir kongre raporuna göre, siber savaş, "*bilgisayar ağlarını siber uzaydaki saldırılardan korumak ve düşmanın gelecekte aynı saldırıyı başlatma yeteneğini engellemek için çok çeşitli unsurları*" içerir.[25]

Siber savaş, devletler veya devlet destekli gruplar tarafından yürütülen simetrik veya asimetrik, saldırgan veya savunma amaçlı dijital ağ faaliyetleridir. Bu faaliyetler, siber ağlarda aksamalara yol açar. Hedef, ülkedeki kritik ulusal altyapıları, askeri sistemleri ve/veya ciddi endüstriyel yapıları tehdit etmektir. Siber savaş olgusu, son yıllarda Rusya ve Çin tarafından desteklenen bilgisayar korsanlarının Ukrayna da dahil olmak üzere diğer bazı Batılı ülkelere saldırılar düzenlediğine dair raporlarla birlikte gündeme gelmiştir. Hatta Birleşik Krallık'ta bile, İngiliz Ordusu'nun kötü amaçlı yazılımları askeri bir araç olarak kullanmanın yollarını araştırdığı bildirilmiştir.[26]

2. Soğuk Savaş Sonrası Güvenlik Algısı/Perspektifinde Değişim: Soğuk Savaş Sonrası Dönemde Güvenlik Perspektifindeki Değişim

Soğuk Savaş döneminde silah temelli güvenlik stratejileri ve "*dehşet dengesi*" gibi kavramlar ön planda yer aldı. İki büyük blok (Batı bloku: ABD; Doğu bloku: Sovyetler Birliği) tarafından şekillendirilen uluslararası sistem, büyük güç rekabeti ve nükleer karşılıklı bağımlılık tarafından belirleniyordu. Karşılıklı güvence altına alınmış yıkım (*mutually assured destruction*) düşüncesi, doğrudan büyük ölçekli bir ABD-Sovyet savaşı riskini sınırlarken, vekâlet savaşlarını ise ortadan kaldırmadı. Nitekim bu yıllarda, "*nükleer denge*"nin yarattığı büyük varoluşsal risk, iç ve dış politikalarda durgun bir istikrarı koruyordu.[27] Burada, karşılıklı olarak güvence altına alınmış yıkımı sağlamak amacıyla "*terör/dehşet dengesi*" stratejisi izlenmiştir. Neticede, Soğuk Savaş, büyük ölçekli dünya savaşlarının ortaya çıkmasını engellemede başarılı oldu, ancak ABD ile diğer ülkeler arasında vekalet savaşları yoluyla küçük ölçekli başka savaşlar yaşandı. Sonunda, Sovyetler Birliği'nin dağılması ve Soğuk Savaş'ın sona ermesiyle, 1990'ların başındaki birleşmeyle dünya bambaşka bir yer haline geldi.

1989'da Berlin Duvarı'nın yıkılması, 3 Ekim 1990'da Almanya'nın yeniden birleşmesi ve Aralık

Üniversitesi Yayınları, s. 8.

[25] Steven A. Hildreth (2001), "Cyberwarfare", CRS Report for Congress, 19.06.2001, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-014.pdf.

[26] Jane McCallion (2022), "What is cyber warfare?", ITPro, 20.05.2022, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.itpro.com/security/28170/what-is-cyber-warfare.

[27] Ali Karaosmanoğlu (2015), "Savunma Planlaması ve Stratejik Belirsizlik", *Bilge Strateji,* 7(12), ss. 23-45.

1991'de Sovyetler Birliği'nin dağılması, birbirleriyle bağlantılı ancak farklı tarihsel süreçlerdi. Soğuk Savaş'ın sona ermesiyle uluslararası sistemin güç dengeleri ve güvenlik gündemi dönüşmüş; devlet dışı aktörler, ekonomik karşılıklı bağımlılık ve bilgi-iletişim teknolojileri güvenlik analizlerinde daha görünür hale gelmiştir.

Yeni paradigma, başlangıçta tek kutuplu dünya sistemi gibi görünse de, ABD'nin bile dünyayı kontrol edemeyeceği kısa sürede anlaşıldı. Dolayısıyla, 21. yüzyılın ayırt edici özelliği, giderek artan çok kutupluluk eğilimleri oldu. 21. yüzyılın yeni dünya düzeni, ABD ve Rusya'nın giderek güç kaybetmesiyle birlikte, Çin'in hızlı yükselişi ve 27 Avrupa ülkesi arasında güçlü bir birliğin oluşması gibi yeni parametrelerle şekillendi. Ancak daha da önemlisi, teknolojik dönüşüm sayesinde, dünyamız, 1990'lardan bu yana çok değişti. Bilgisayarlar, internet teknolojileri, cep telefonları, uzaktan sistemler, dronlar ve sosyal medya, 21. yüzyılın başlarında sıradan özellikler haline geldi. 21. yüzyılın teknolojik ilerlemesi sayesinde, bu teknolojiler ve platformlar insanlar için daha rahat bir yaşam yaratırken, aynı zamanda bireyler, şirketler ve devletler için yeni riskler de doğurdu.

Bu dönüşüm, güvenliğin yalnızca askerî tehditlere indirgenemeyeceğini ortaya koymuştur. Kopenhag Okulu'nun güvenlikleştirme yaklaşımı bakımından siber tehditler; devletin egemenliği, ekonomik süreklilik, toplumsal düzen ve bireysel mahremiyet gibi farklı referans nesnelerini etkileyebilmektedir. Bununla birlikte, her teknik arıza veya suç faaliyeti doğrudan ulusal güvenlik tehdidi olarak nitelendirilmemelidir. Tehdidin ölçeği, etkisi, faili, hedef aldığı altyapının kritik niteliği ve kamu düzeni üzerindeki sonuçları birlikte değerlendirilmelidir. Bu ayrım, siber suç, siber casusluk, siber saldırı ve silahlı çatışma bağlamındaki siber operasyonların birbirine karıştırılmasını önlemek açısından önemlidir. Türkiye'nin politikaları da bu nedenle yalnızca savunma tedbirleriyle değil, tehdit sınıflandırması, kurumsal görev paylaşımı ve demokratik-hukuki denetim boyutlarıyla ele alınmalıdır.

1990'ların başından beri, bilgi, siyasi araçlar açısından önemi nedeniyle Uluslararası İlişkiler disiplininde de kilit bir rol oynamaktadır. Bilgi ve iletişim teknolojileri, günümüzde sanayileşmiş devletlerin birçok alanında baskın konumdadır.[28] Güvenliğin derinleşmesi ve genişlemesi, temelde güvenlik tehditlerinin çoğalmasıyla ilgilidir. Bu bağlamda, güvenlik, küreselleşme ve teknoloji

[28] Myriam Dunn Cavelty (2010), "Cyber Security", içinde (editör: J. Peter Burgess) *The Routledge Handbook of New Security Studies*, New York: Taylor & Francis Group, s. 159.

arasındaki ilişkiyi incelemek gereklidir. Küreselleşme ve teknolojinin yarattığı sınırların geçirgenliği ve akışkanlık, bireylere ve devlete yönelik tehditlerin sayısını da arttırmıştır.[29] 1990'lardan bu yana, küreselleşme olgusunun hızlanmasıyla birlikte, çok hızlı ve kaçınılmaz bir değişim süreci başlamıştır. Küreselleşme, güvenlik tehditlerinin farklılaşmasını o kadar kapsamlı bir şekilde çoğaltmıştır ki, güvenlik kavramının kendisinin yeniden değerlendirilmesi gerekmektedir. Organize suç, yasadışı göç, insan kaçakçılığı, uyuşturucu/silah kaçakçılığı ve kara para aklama gibi yeni tehditler, büyük uluslararası istikrarsızlaştırıcılar olarak ortaya çıkmıştır. Bu nedenle, geleneksel tehdit algıları ve bu unsurlarla mücadele yöntemleri, bu yeni tehlikelerle mücadelede yetersiz kalmıştır. Bu yetersizlik, yeni bir güvenlik tanımının yanı sıra, yeterli bir yanıt uygulamak için yeni araçlar gerektirmiştir.[30] Siber saldırıların artan oranı, ulus devletleri veya uluslararası aktörleri bu alanda hızla çalışmaya yöneltmiştir. Temel kritik altyapıların ve siber güvenliğin geliştirilmesi, ulusal çıkarlar için hayati önem taşımaktadır. Bu nedenle, her aktör, siber savaşa sadece savunma için değil, aynı zamanda saldırı yetenekleri oluşturmak için de önem vermeye başlamıştır. Son gelişmeler, siber savaşların 21. yüzyılda da bir gerçeklik olarak kalacağını göstermektedir.[31]

3. 11 Eylül Sonrası Siber Saldırılar ve Siber Güvenlik Girişimleri

Soğuk Savaş'tan sonra, küresel güvenlik ortamını derinden etkileyen ve şekillendiren en önemli olay, 11 Eylül 2001'deki ABD'ye yönelik terör saldırılarıydı. 11 Eylül'den önce, siber uzayın riskleri ve güvenlik sorunları yalnızca küçük bir uzman grubu tarafından tartışılan konular arasındaydı. O günden beri ise, siber dünya, birbirine giderek daha fazla bağımlı hale gelen toplumlar için ciddi riskler yaratmıştır. 11 Eylül'de El Kaide saldırılarıyla İkiz Kuleler'e giren uçaklar, Washington DC ve uluslararası sistemdeki güvenlik, tehditler ve gündem tanımlarını tamamen değiştirdi. Bu saldırılar sonucunda, Soğuk Savaş'tan sonra nispeten belirsizleşen ulusal güvenlik kavramı, birçok ülkenin öncelik listesinde yeniden en üst sıraya yerleşti. Terörle mücadele veya Başkan Bush'un ifadesiyle "*teröre karşı savaş*", yalnızca saldırılara maruz kalan ülkelerin hükümetlerinin değil, sistemdeki neredeyse tüm aktörlerin gündemine girdi ve ABD'nin

[29] Muharrem Aksu & Faruk Turhan (2012), "Yeni Tehditler, Güvenliğin Genişleme Boyutları ve İnsani Güvenlik", *Uluslararası Alanya İşletme Fakültesi Dergisi*, 4(2), s. 71.
[30] Bilal Karabulut (2015), *Güvenlik: Küreselleşme Sürecinde Güvenliği Yeniden Düşünmek*, Ankara: Barış Kitabevi, s. 119.
[31] Ayhan Gücüyener (2016), "21. Yüzyılda 'Siber' Rekabet: Yeni Hedef Kritik Altyapılar mı?", Linkedin, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.linkedin.com/pulse/21-y%C3%BCzy%C4%B1lda-siber-rekabet-yeni-hedef-kritik-m%C4%B1-ayhan-gucuyener/.

liderliğinde hızla ivme kazandı.

Enkazın üzerindeki tozlar yatıştıktan hemen sonra, saldırıları gerçekleştiren teröristlerin internet üzerinden kendi aralarında iletişim kurdukları ve daha önce bu uçaklarla simülasyon çalışmaları yaptıkları anlaşıldı. Bu açıklama, internetin terörizm için kullanılabileceği fikrini güçlendirdi.[32] Örneğin, 11 Eylül (9/11) saldırganlarının hepsinin Hotmail hesapları vardı ve bu hesapları haberleşmek için kullandıkları düşünülüyordu. Ayrıca araştırmalar sonucu anlaşıldı ki, teröristler, El Kaide lideri Usame bin Ladin'in yardımcılarından birinin kayınbiraderi tarafından yönetilen bir internet sitesinin ziyaretçi defteri bölümüne bırakılan notlar aracılığıyla koordinasyon sağlamıştı.[33]

11 Eylül (9/11) sonrası yüksek gerilim döneminde, uluslararası arenada en çok tartışılan konulardan biri, varsayımsal olarak NATO üyesi ülkelerden birini felç edecek olan "*Dijital Felaket*" senaryosuydu. Terörist grupların siber saldırı olasılığı, olası bir "*Dijital Pearl Harbor*" beklentisini arttırdı. Ulus devletlerin ekonomik ve diğer kritik altyapılarının, siber sistemlerine yönelik saldırılar sonucunda yok edilebileceği düşünülüyordu.[34] Bu tür endişeler ulusal güvenlikle yakından ilişkili olduğundan, birçok ülke siber güvenlik stratejilerini ulusal güvenlik belgelerine eklemiş ve bunları düzenli olarak güncellemiştir. Örneğin, Siber Güvenlik Yasası, ABD'de 13 Kasım 2001'de kabul edildi. Bu durum, polisin mahkeme kararı olmaksızın telefon dinlemesi yapmasına veya elektronik gözetim kullanmasına olanak sağladı. Bu bağlamda, Savunma Bakanlığı tarafından terörizmle mücadele için geliştirilen "*Toplam Bilgi Farkındalığı*" (*Total Information Awareness*) planı, ülke genelinde uygulamaya konuldu.[35]

2007 yılında Estonya'ya yönelik siber saldırılar, Soğuk Savaş sonrası artan siber tehdidin açık bir örneğiydi. Sovyetler Birliği'nin çöküşünün ardından Rusya ve Estonya arasında sürekli bir gerginlik yaşandı. Estonya yetkililerinin 26 Nisan 2007'de Tallinn'deki bir meydandan Bronz Asker adlı Sovyet savaş anıtını kaldırmasıyla, bu iki ülke arasındaki ilişkiler iyice gerildi. Bu süreçte, büyük bir Rus azınlığı barındıran Estonya, üç hafta boyunca yoğun siber saldırılara maruz kaldı. Saldırılar, Estonya Cumhurbaşkanlığı ve parlamentosunu, siyasi partileri, devletin tüm

[32] Timothy L. Thomas (2003), "Al Qaeda and the Internet: The Danger of 'Cyberplanning'", *Parameters*, 33(1), s. 120.
[33] P. W. Singer & Allan Friedman (2014), *Cybersecurity and Cyberwar: What Everyone Needs to Know*, s. 101.
[34] Lene Hansen & Helen Nissenbaum (2009), "Digital Disaster, Cyber Security and the Copenhagen School", *International Studies Quarterly,* 53(4), s. 1160.
[35] TUİÇ (2017), "Gözetim Politikaları ve Terörizm: 11 Eylül 2001", 04.01.2017, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.tuicakademi.org/gozetim-politikalari-terorizm-11-eylul-2001/.

Bakanlıklarını, ülkenin en ünlü üç medya kuruluşunu, en büyük bankasını ve iletişim şirketlerini hedef aldı. Siber saldırılar, Avrupa'nın en güçlü kablolu yayın ağına ve en üst düzey e-devlet uygulamasına sahip olan Estonya'da hayatı durma noktasına getirdi. Olay, NATO veya Avrupa Birliği (AB) tarafından "*siber savaş*" olarak nitelendirilmemiş; bunun yerine "*siber saldırı*" eylemleri olarak sınıflandırılmıştır. Önemli maddi hasar veya insanlara zarar verilmemesi nedeniyle, bu olay doğrudan bir savaş eylemi olarak kabul edilmemiştir. Bu bağlamda, yapanları belirlemenin zor olduğu siber saldırıları açık bir askeri eylem olarak tanımlamanın zor olduğu da açıkça belirtilmiştir.[36] Bu saldırının ardından, NATO ve Estonya arasında NATO İşbirliğine Dayalı Siber Savunma Mükemmeliyet Merkezi kurulmuştur.

Dahası, 2008 yılında Rusya ve Gürcistan arasındaki karşılıklı siyasi krizin bir sonucu olarak, Rusya, bu yıl içerisinde Gürcistan'a karşı bir siber saldırı başlattı. Rus siber savaşı, Gürcistan'ın hükümet web sitelerine ve ülkenin birçok ticari web sitesine karşı da kullanıldı. Bu sabotaj, interneti birkaç gün boyunca devre dışı bıraktı ve hatta elektrik kesintilerine yol açtı. Ancak Gürcistan'ın internet ağları çok gelişmiş olmadığı için siber saldırılar Estonya'da yaşanan kadar büyük hasara yol açmadı.

Yakın tarihte, muazzam bir etki yaratan bir başka büyük siber saldırı daha yaşandı. Stuxnet saldırısı adı verilen sabotaj eylemini, ABD, 2009 yılında İran'ın nükleer santrallerine yönelik olarak gerçekleştirdi. ABD yetkilileri saldırıların sorumluluğunu üstlenmese de, siyasi ve istihbari analizler ABD'nin bu olayda mutlak bir rolü olduğunu ortaya koydu.[37] Saldırı, 2010 yılında tespit edildi. İran'ın zenginleştirilmiş uranyum tesislerinde bir yıl içinde değiştirilen santrifüjlerin yüzde 10'unun doluluk oranına ulaşması, sistemde bir sorun olduğunu ortaya koydu. Bir yıllık bir çalışma, santrifüjlerdeki değişikliklerin aslında bir bilgisayar arızasından kaynaklandığını kanıtladı. Program o kadar güçlüydü ki, 100.000'den fazla bilgisayara bağlantı sağlıyordu.[38]

Son yıllarda, köktendinci terör örgütleri de sıklıkla siber yöntemler kullanmaktadır. Örneğin, IŞİD/DEAŞ terör örgütü, 2015 yılında ABD Merkez Komutanlığı'nın (CENTCOM) resmi Twitter

[36] James P. Farwell & Rafal Rohozinski (2011), "Stuxnet and the Future of Cyber War", *Survival,* 53(1), s. 32.
[37] Şener Çelik (2014), "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi*, 15(1), s. 144.
[38] Kim Zetter (2011), "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History", *Wired*, 11.07.2011, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.

ve YouTube hesaplarına siber saldırı düzenledi. Korsanlar, ele geçirdikleri hesaplardan şu mesajı paylaştılar: "*Amerikan askerleri, geliyoruz, arkanızı kollayın. Kişisel telefonlarınızı ve ailelerinizi biliyoruz*."[39] İddialara göre, bu saldırıları, kendilerine Siber Halifelik adını veren IŞİD bağlantılı bir grup organize etti. ABD medyasına göre, saldırı, IŞİD'in en başarılı bilgisayar sihirbazı olarak tanımlanan İngiliz bilgisayar korsanı Junaid Hussein (Abu Hussein El Britani) tarafından organize edildi.[40] Dahası, 2015 yılında, Fransa'da, IŞİD/DEAŞ, programları dünya çapında 200'den fazla ülkede yayınlanan küresel yayın kuruluşu *TV5 Monde*'a bir siber saldırı düzenledi. Kanalın internet sitelerini ele geçiren bilgisayar korsanları, Facebook ve Twitter hesapları, "*Siber cihatçılar*" adı altında "*Ben IŞİD'im*" mesajını yayınladı. Mesajlarında, teröristler, ayrıca, Fransa Cumhurbaşkanı François Hollande ve Fransız Ordusu'nu da tehdit ettiler.[41]

2019'da Sri Lanka'da IŞİD/DEAŞ tarafından gerçekleştirilen bombalı saldırının Bitcoin ile finanse edilmesi ve teröristler ile sempatizanlarının örgüte Bitcoin aracılığıyla para transferi yapması, siber terörizmin internetteki tehlikeli boyutunu ortaya koymaktadır. IŞİD/DEAŞ, fiziksel dünyada büyük bir darbe almış olsa da, son birkaç yıldır siber alanda giderek daha aktif hale gelmiştir.[42]

4. Türkiye'de Siber Güvenlik

Türkiye'de 86 milyonluk toplam nüfusun yüzde 92-93'lük çok büyük bir kısmı internet kullanmaktadır.[43] İnternet ve bilgisayar kullanımının artması, diğer devletler gibi Türkiye'de de birçok siber güvenlik riskini de beraberinde getirmektedir. Bu güvenlik riskleri arasında kritik altyapıların güvenliği, gizliliğin ihlali, bilgi bütünlüğünün veya erişilebilirliğinin bozulması, büyük ölçekli ekonomik zararlar, ulusal güvenlik açıkları veya kamu düzeninin bozulması yer

[39] *Reuters* (2015), "Apparent Islamic State backers hack U.S. military Twitter feed", 13.01.2015, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.reuters.com/article/us-cybersecurity-centcom-hack-idUSKBN0KL1UZ20150112/.

[40] *The Guardian* (2015), "Briton lead suspect after US Central Command's Twitter account is hacked", 14.01.2015, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.theguardian.com/us-news/2015/jan/14/briton-suspect-us-central-command-twitter-hack-junaid-hussain-tony-blair.

[4141] Ozan Örmeci & Eren Alper Yılmaz & Ahmet Emre Köker (2022), "Turkey's Cyber Security Policies", içinde (editörler: Hasret Çomak & Burak Şakir Şeker & Yaprak Civelek & Çağla Arslan Bozkuş) *Cyber Environment and International Politics*, Londra: TPLondon, s. 76.

[42] Emine Çelik (2019), "Siber Terörizm ve IŞİD-Bitcoin İlişkisi", *Ortadoğu Analiz*, 10(89), ss. 90-91.

[43] *Anadolu Ajansı* (2026), "Türkiye'de internet kullananların oranı bu yıl yüzde 92,3'e yükseldi", 05.09.2026, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.aa.com.tr/tr/bilim-teknoloji/turkiyede-internet-kullananlarin-orani-bu-yil-yuzde-92-3e-yukseldi/4018733.

almaktadır. Öte yandan, Türkiye'de mobil cihazların artması ve "*nesnelerin interneti*"nin gelişmesiyle birlikte tüm süreçlerin işleyişi siber alana girmiştir. Bu nedenle, siber alanın bu beklenmedik genişlemesi, onu her türlü saldırıya karşı savunmasız hale getirmiştir.

4.1. Türkiye'deki Siber Güvenlik Kurumları

Türkiye'de siber alanın kontrolü ve yönetimiyle ilgili temel kurum T.C. Cumhurbaşkanlığı'na bağlı olarak 2025 yılında kurulan Siber Güvenlik Başkanlığı'dır.[44] Siber Güvenlik Başkanlığı, Türkiye'nin siber uzaydaki millî güvenliğini ve dijital egemenliğini sağlamak amacıyla Cumhurbaşkanlığı'na bağlı olarak kurulan en üst düzey yetkili merciidir. 8 Ocak 2025 tarihinde 177 sayılı Cumhurbaşkanlığı kararnamesi ile kurulan kurum, halen Ümit Önal başkanlığında faaliyetlerine devam etmektedir.

4.1.1. Siber Güvenlik Başkanlığı

Resim 1. Siber Güvenlik Başkanlığı logosu

Kurum web sitesinden özetlemek gerekirse, T.C. Cumhurbaşkanlığı'na bağlı Siber Güvenlik Başkanlığı'nın temel görevleri şunlardır:

A-) Siber Güvenlik ve Tehdit Yönetimi

- ✓ **Politika ve Strateji Belirleme:** Siber Güvenlik Başkanlığı, ulusal siber güvenlik politika, strateji ve hedeflerini belirler, eylem planları hazırlar ve mevzuat çalışmalarını yürütür.
- ✓ **Kritik Altyapıların Korunması:** Siber Güvenlik Başkanlığı, kamu kurumlarının ve kritik

[44] T.C. Siber Güvenlik Başkanlığı, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://siberguvenlik.gov.tr/.

altyapıların siber tehditlere karşı korunması amacıyla izleme, analiz ve önleyici tedbir faaliyetlerini koordine eder.

- ✓ **Siber Tehdit İstihbaratı:** Siber Güvenlik Başkanlığı, siber tehdit aktörlerini ve küresel zafiyetleri takip ederek elde ettiği bulguları ilgili paydaşlarla paylaşır.
- ✓ **Olay Müdahale ve Koordinasyon:** Siber Güvenlik Başkanlığı, siber olayların tespiti, analizi ve müdahale kapasitesinin artırılması için ulusal düzeyde hazırlık seviyesini yükseltir. Siber Olaylara Müdahale Ekiplerinin (SOME) koordinasyonunu sağlar.
- ✓ **Denetim ve Gözetim:** Siber Güvenlik Başkanlığı, belirlenen standartların ve siber güvenlik düzenlemelerinin uygulanmasını denetler.

B-) Dijital Devlet ve Altyapı Güvenliği

- ✓ **E-Devlet Kapısı Yönetimi:** Siber Güvenlik Başkanlığı, E-Devlet altyapısının güvenli bir şekilde işletilmesini ve kamu hizmetlerinin kesintisiz sürdürülmesini sağlar.
- ✓ **Veri Güvenliği ve Bulut Stratejileri:** Siber Güvenlik Başkanlığı, Kamu Bulut Bilişim Stratejisi, Açık Devlet Verisi uygulamaları ve kamuda açık kaynak kodlu yazılım kullanımına yönelik standartları oluşturur.

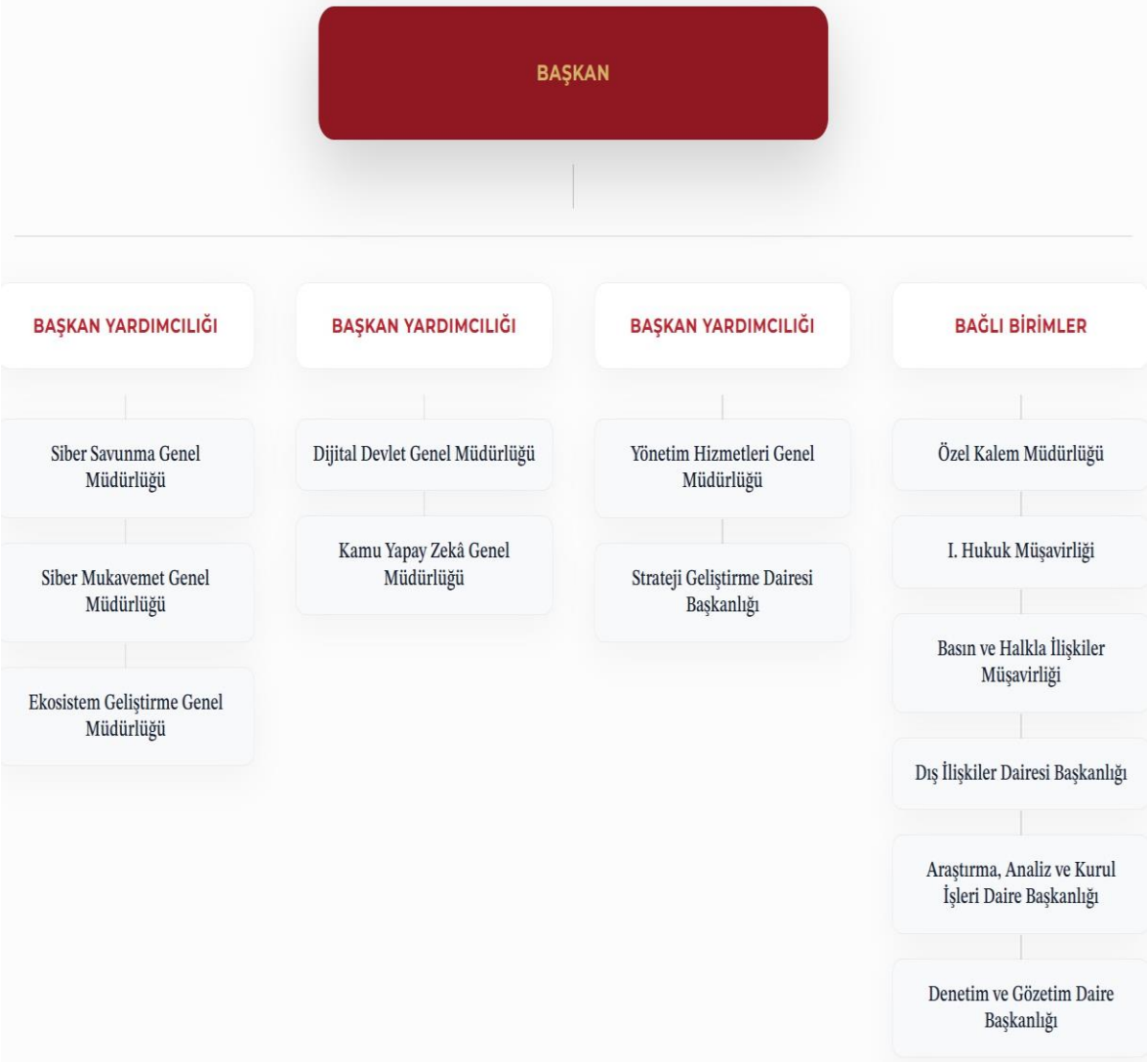
C-) Kamu Yapay Zekâsı ve Teknoloji Yönetimi

- ✓ **Güvenli Yapay Zekâ Kullanımı:** Siber Güvenlik Başkanlığı, kamuda yapay zekâ ve veri analitiği teknolojilerinin güvenli, sorumlu ve etik kurallara uygun olarak kullanılmasına yönelik düzenlemeler ve uygulamalar geliştirir.

Ç-) Ekosistem Geliştirme ve İş Birlikleri

- ✓ **Kapasite ve İnsan Kaynağı Geliştirme:** Siber Güvenlik Başkanlığı, Türkiye'nin ulusal siber güvenlik uzmanı ihtiyacını karşılamak üzere kapasite geliştirme süreçlerini ve personel istihdamını yönetir.
- ✓ **Ulusal ve Uluslararası İş Birliği:** Siber Güvenlik Başkanlığı, kamu, özel sektör, akademi ve uluslararası paydaşlar arasında bilgi paylaşım ağları kurarak siber güvenlik ekosistemini büyütür.

Resim 2. Siber Güvenlik Başkanlığı'nın kurumsal şeması



4.1.2. Diğer Kurumlar

Ancak yeni kurulan Siber Güvenlik Başkanlığı dışında da bu alanda faaliyet gösteren bazı önemli resmi kuruluşlar bulunmaktadır.

Resim 3. BTK logosu

Bilgi Teknolojileri ve İletişim Kurumu (BTK): BTK, Türkiye'de elektronik haberleşme, bilgi teknolojileri ve posta sektörlerini düzenleyen ve denetleyen bağımsız bir kamu otoritesidir. 2025 yılının başında T.C. Cumhurbaşkanlığı'na bağlı Siber Güvenlik Başkanlığı (SGB) kurulmadan önce, Türkiye'deki ulusal siber güvenlik süreçlerinin koordinasyonu ve operasyonel yönetimi ağırlıklı olarak Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yapılıyordu. SGB'nin kurulmasının ardından bu alandaki yetkilerini devreden BTK'nın şu andaki temel görev ve yetkileri şunlardır:

- ✓ **Sektörel Düzenleme ve Yetkilendirme:** Telekomünikasyon ve internet alanında faaliyet gösteren operatörlere ve işletmecilere lisans/yetki verir, pazar kurallarını belirler ve adil rekabeti korur.
- ✓ **Tüketici Hakları:** Abonelik sözleşmelerini, faturalandırma süreçlerini ve hizmet kalitesini denetler; tüketicilerden gelen şikâyetleri değerlendirir.
- ✓ **Frekans ve Altyapı Yönetimi:** Radyo frekanslarının tahsisini yapar, spektrum izleme ve yönetim faaliyetlerini yürütür.
- ✓ **IMEI Kayıt İşlemleri:** Cep telefonlarının kayıt altına alınması, IMEI sorgulama ve eşleştirme işlemlerini yönetir.
- ✓ **Alan Adı Yönetimi:** .tr uzantılı alan adlarının TRABİS sistemi üzerinden tahsis ve yönetim süreçlerini düzenler.

- ✓ **BTK Akademi:** 16 yaş ve üzeri herkese yazılım, siber güvenlik ve yapay zekâ gibi alanlarda ücretsiz çevrim içi eğitimler sunar.
- ✓ **Erişim Engelleme ve Güvenlik:** Güvenli internet hizmetlerini düzenler ve yasal mevzuat çerçevesinde internet sitelerine erişimin engellenmesi kararlarını uygular.

BTK USOM (Ulusal Siber Olaylara Müdahale Merkezi): Bilgi Teknolojileri ve İletişim Kurumu bünyesinde ülkenin siber güvenlik olaylarına müdahale ana merkezidir ve ulusal koordinasyonu yürütür. Temel görev ve faaliyetleri şöyledir:

- ✓ **Siber Tehdit İstihbaratı:** Ülke genelindeki siber saldırıları ve riskleri izler, zararlı bağlantıları (Zararlı Bağlantılar) raporlar.
- ✓ **Zafiyet Yönetimi:** Kritik altyapılardaki güvenlik açıklarını tespit ederek ilgili kurum ve kuruluşları uyarır.
- ✓ **SOME Koordinasyonu:** Kurumlar arası Siber Olaylara Müdahale Ekiplerinin (SOME) eş güdümünü sağlar ve SİP (SOME İletişim Platformu) üzerinden güvenli bilgi paylaşımı yürütür.
- ✓ **İhbar Süreçleri:** Vatandaşlardan ve kurumlardan gelen siber güvenlik ihbarlarını değerlendirir.

TÜBİTAK BİLGEM (Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi): Siber güvenlik ve kriptoloji alanında yerli Ar-Ge çözümleri ve ürünler (ör. Siper, Ulak) geliştiren temel araştırma merkezidir. BİLGEM, çatısı altında farklı uzmanlık alanlarına odaklanmış 6 stratejik enstitü barındırır:

1. **UEKAE:** Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü,
2. **BTE:** Bilişim Teknolojileri Enstitüsü,
3. **SGE:** Siber Güvenlik Enstitüsü,
4. **YTE:** Yazılım Teknolojileri Araştırma Enstitüsü,
5. **İLTAREN:** İleri Teknolojiler Araştırma Enstitüsü,
6. **YZE:** Yapay Zekâ Enstitüsü.

TSK Siber Savunma Komutanlığı: Türk Silahlı Kuvvetleri (TSK) bünyesindeki Siber Savunma Komutanlığı, TSK'nın dijital hudutlarını korumak ve askeri bilgi sistemlerinin güvenliğini sağlamakla görevlidir. Komutanlık, TSK Siber Savunma Merkezi (SİSAMER) aracılığıyla ülkede meydana gelen siber olaylara anında tepki vererek olası zararları ve kriz durumlarını en aza indirir. Ayrıca dışa bağımlılığı azaltmak amacıyla yerli ve milli siber güvenlik yazılımları geliştirir, entegre eder ve güncel tutar. Ek olarak, ulusal güvenliği hedef alan siber tehditleri önceden belirlemek için istihbarat ve güvenlik analizleri gerçekleştirir. Bunların yanı sıra, TSK'nın kritik iletişim altyapısını korumak ve savunma reflekslerini tek bir merkezden koordine etmekle yükümlüdür. Son olarak, yine SİSAMER'e bağlı Siber Savunma Harekât Merkezi aracılığıyla TSK ağlarına ve sistemlerine yönelik her türlü siber saldırıyı veya yetkisiz erişim girişimini kesintisiz takip eder.

Emniyet ve Jandarma Siber Suçlarla Mücadele Daire Başkanlıkları: Türkiye'deki temel yetkili kurum olan EGM Siber Suçlarla Mücadele Daire Başkanlığı'nın (ve Jandarma bünyesindeki muadilinin) ulusal çatı kuruluş olan T.C. Siber Güvenlik Başkanlığı'nın çalışmaları doğrultusunda belirlenen görev ve yetkileri şu şekildedir:

- Adli kolluk olarak doğrudan siber suçların tespiti, soruşturulması ve suçluların yakalanmasıyla görevlidirler.
- Bilişim sistemlerine hukuka aykırı girme (*hacking*), sistemleri engelleme/bozma, veri hırsızlığı, nitelikli internet dolandırıcılığı, yasadışı bahis ve siber zorbalık gibi suçları araştırırlar.
- Suç mahalli ya da şüphelilerden elde edilen bilgisayar, telefon, hard disk gibi bilişim sistemlerinde mahkeme kararıyla arama yapar, adli kopyalarını (imaj) alır, silinen verileri kurtarır ve raporlayarak adli makamlara sunarlar.
- İnternet ortamında açık kaynaklar üzerinden 7/24 önleyici izleme yapar; suç unsuru barındıran paylaşımları, siber tehditleri ve terör faaliyetlerini tespit ederler.
- Teknoloji bağımlılığı, güvenli internet kullanımı ve siber zorbalığa karşı toplumda farkındalık yaratmak amacıyla Siberay gibi projeler üzerinden eğitim ve bilgilendirme faaliyetleri yürütürler.
- Son olarak, sınır aşan siber suçlarla (uluslararası siber nitelikli dolandırıcılık gibi)

mücadele etmek için Europol, Interpol ve diğer ülkelerin siber polis birimleriyle ortak operasyonlar ve bilgi paylaşımı gerçekleştirirler.

Türkiye Siber Güvenlik Kümelenmesi: T.C. Cumhurbaşkanlığı Savunma Sanayii Başkanlığı öncülüğünde; kamu, özel sektör ve akademiyi bir araya getiren ekosistem platformudur.

Savunma ve Kamu Kaynaklı Şirketler: HAVELSAN, STM ve ASELSAN gibi kurumlar da ulusal siber savunma sistemleri ve operasyonel merkezler (SOC) kurmaktadır.

Kurumsal yapı bakımından temel mesele, kurumların sayısından çok görev ve sorumlulukların açık biçimde tanımlanması ve ortak bir müdahale zinciri içinde çalışabilmesidir. Siber Güvenlik Başkanlığı'nın strateji ve koordinasyon rolü ile BTK/USOM'un teknik izleme ve olay müdahalesi, kolluk birimlerinin adli soruşturma yetkileri, TÜBİTAK BİLGEM'in araştırma-geliştirme kapasitesi ve TSK'nın askerî ağlara ilişkin sorumlulukları birbirini tamamlayabilecek niteliktedir. Ancak bu çok aktörlü yapı, bilgi paylaşımında gecikme, mükerrer görevler veya kriz anında yetki belirsizliği risklerini de beraberinde getirebilir. Dolayısıyla, kurumsal etkinliğin değerlendirilmesinde ortak olay müdahale tatbikatları, bildirim süreleri, kritik altyapı sektörleriyle bilgi paylaşımı, personel yeterliliği ve olay sonrası öğrenme mekanizmaları gibi göstergeler önem taşımaktadır. Bu göstergelere ilişkin karşılaştırılabilir ve kamuya açık veriler bulunmadığı ölçüde, kurumsal kapasite ile fiilî performans arasında ayrım yapılmalıdır.

4.2. Ulusal Siber Güvenlik Stratejisi

Türkiye'nin ulusal siber güvenlik politikaları, en güncel olarak Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028) çerçevesinde siber dayanıklılığı artırmayı ve yerli teknolojileri geliştirmeyi amaçlamaktadfir.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028), Türkiye'nin siber uzaydaki güvenliğini arttırmak, riskleri azaltmak ve yerli teknolojileri geliştirmek amacıyla 7 Eylül 2024 tarihli *Resmi Gazete* süreçleri sonrasında yürürlüğe girmiştir.

Temel Amaç ve Kapsam:

- Vizyon: Türkiye'nin siber dayanıklılığını en üst seviyeye çıkarmak ve uluslararası alanda güvenilir bir siber güvenlik ekosistemi oluşturmak.
- Koordinasyon: Çalışmalar Ulaştırma ve Altyapı Bakanlığı koordinasyonunda yürütülmektedir.

- Temel Yapı: Plan, 4 temel kavram (İnsan, Savunma, Caydırıcılık, İş Birliği) üzerine kurulmuştur.

Stratejik Bileşenler:

Belge, genel hatlarıyla şu ana unsurları içerir:

- 6 Stratejik Amaç: Siber dayanıklılık, proaktif siber savunma, insan odaklı yaklaşım, güvenli teknoloji kullanımı, yerli ve millî çözümler ile uluslararası iş birliği.
- 18 Hedef ve 61 Eylem Maddesi: Kritik altyapıların korunmasından siber farkındalığın artırılmasına kadar somut adımlar.
- İzleme ve Değerlendirme: Hedeflerin gerçekleşme oranları periyodik olarak raporlanmakta ve ilgili kamu kurum ile kuruluşlarının sorumlulukları takip edilmektedir.

4.3. Mevzuat

Türkiye'nin siber güvenlik alanındaki ana omurgasını, 19 Mart 2025 tarihinde yürürlüğe giren 7545 sayılı Siber Güvenlik Kanunu ve Cumhurbaşkanlığı bünyesinde kurulan T.C. Siber Güvenlik Başkanlığı Mevzuat rehberliği oluşturur.

Türkiye'deki siber güvenlik mevzuatı, başlıca şu temel kanun, kararname ve düzenlemelerden meydana gelir:

1. Ana Kanun ve Kurumsal Yapı:

- 7545 sayılı Siber Güvenlik Kanunu: Türkiye'nin siber uzaydaki milli gücünü korumak, siber güvenliği güçlendirmek ve Siber Güvenlik Başkanlığı ile Siber Güvenlik Kurulu'nu tesis eden temel ve bağlayıcı kanundur. Kamu kurumlarını, meslek örgütlerini, gerçek ve tüzel kişileri kapsar.
- Cumhurbaşkanlığı Kararnameleri: Siber Güvenlik Başkanlığı'nın teşkilat yapısını, görev, yetki ve sorumluluk alanlarını belirleyen ikincil üst düzey idari düzenlemeler.

2. Türk Ceza Kanunu (TCK) - Siber Suçlar:

- Madde 243 (Bilişim Sistemine Girme): Bir sisteme izinsiz girme veya kalma.
- Madde 244 (Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme): Bilişim sistemlerinin çalışmasını engelleme veya verileri bozma/silme.

- Madde 245 (Banka veya Kredi Kartlarının Kötüye Kullanılması): Kartların izinsiz kullanılması veya sahte üretilmesi.
- Madde 245/A (Yasak Cihaz veya Programlar): Siber saldırı araçlarının imal, ithal veya sevk edilmesi.

3. Bilgi ve İletişim Güvenliği Düzenlemeleri:

- Bilgi ve İletişim Güvenliği Rehberi: Kamu kurumları ve kritik altyapı işleten kritik sektörlerdeki firmalar için uyulması zorunlu teknik ve idari güvenlik standartlarını belirler.
- SOME (Siber Olaylara Müdahale Ekibi) Yönetmelikleri: Ulusal ve kurumsal düzeyde siber olay müdahale süreçlerini, koordinasyon esaslarını ve raporlama yükümlülüklerini düzenler.

4. Kişisel Verilerin Korunması ve Sektörel Mevzuat:

- 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK): Kişisel verilerin hukuka aykırı işlenmesini önlemek ve veri güvenliğini sağlamak amacıyla veri sorumlularına teknik/idari tedbir alma zorunluluğu getirir.
- Sektörel Düzenlemeler: Bankacılık (BDDK düzenlemeleri), elektronik haberleşme (BTK yönetmelikleri) ve enerji piyasası gibi kritik altyapı sektörlerine özel siber güvenlik ve loglama standartları.

4.4. Türkiye'nin Siber Güvenlik Politikalarının Analitik Değerlendirmesi

Türkiye'nin siber güvenlik mimarisi, son 10 yılda strateji belgeleri, teknik müdahale birimleri ve mevzuat aracılığıyla aşamalı biçimde gelişmiş; 2025 yılında Siber Güvenlik Başkanlığı'nın kurulması ve 7545 sayılı Kanun'un kabul edilmesiyle daha merkezi bir yönetişim modeline yönelmiştir. Bu gelişme, siber güvenliğin yalnızca haberleşme ve bilişim sektörüne ait teknik bir konu olmaktan çıkarak ulusal güvenlik, kamu yönetimi ve dijital egemenlik başlıklarıyla birlikte ele alındığını göstermektedir. Bununla birlikte, merkezî koordinasyonun güçlendirilmesi tek başına etkili uygulamayı garanti etmez. Kurumların görev sınırlarının ikincil düzenlemelerle açıklığa kavuşturulması, bütçe ve uzman personel kapasitesinin sürdürülebilirliği ve kamu-özel sektör arasında güvenilir bilgi paylaşımının sağlanması gerekmektedir.

Kritik altyapıların korunması, politikanın başarısını sınayacak temel alanlardan biridir. Enerji,

finans, ulaştırma, sağlık, elektronik haberleşme ve kamu hizmetleri gibi sektörlerde dijital sistemlerin birbirine bağımlılığı, tek bir kurumda ortaya çıkan güvenlik açığının sektörler arası sonuçlar doğurabilmesine yol açmaktadır. Bu nedenle, yalnızca saldırıların önlenmesi değil, hizmetlerin kesinti sırasında sürdürülebilmesi, yedekleme ve kurtarma kapasitesi, tedarik zinciri güvenliği ve düzenli tatbikatlar da siber dayanıklılığın parçası olarak görülmelidir. Mevcut metinde sıralanan kurum ve mevzuat, bu hedefler için bir yönetişim zemini sunmaktadır; ancak etkinliğin kanıtlanması için sektör bazlı risk değerlendirmeleri ve ölçülebilir performans göstergelerinin düzenli yayımlanması gereklidir.

Siber caydırıcılık açısından Türkiye'nin karşı karşıya olduğu temel güçlükler, siber saldırıların kaynağını yüksek kesinlikle tespit etmenin (atıf) zorluğu, saldırıların farklı aktörler üzerinden yürütülebilmesi ve verilecek karşılığın hukuki-siyasi sınırlarıdır. Bu nedenle, caydırıcılık, yalnızca misilleme kapasitesine indirgenmemelidir. Güçlü savunma, hızlı toparlanma, saldırıların maliyetini artıran ulusal ve uluslararası koordinasyon, kamuoyuna doğru ve zamanında bilgilendirme ve hukuka uygun karşılık seçenekleri birlikte düşünülmelidir. Bu yaklaşım, siber saldırıların her durumda silahlı saldırı veya savaş eylemi sayılmaması gerektiği yönündeki uluslararası hukuk tartışmalarıyla da uyumludur.

Uluslararası iş birliği, Türkiye'nin NATO üyeliği ve sınır aşan siber tehditlerin niteliği nedeniyle ayrıca önem taşımaktadır. Siber olayların ulusal sınırları aşması, tehdit istihbaratının paylaşılmasını, ortak tatbikatları, teknik standartların uyumlaştırılmasını ve adli makamlar arasında iş birliğini gerekli kılmaktadır. NATO'nun siber savunmayı kolektif savunma ve dayanıklılık gündeminin parçası olarak ele alması, Türkiye açısından askerî ağların korunmasının yanı sıra sivil kritik altyapıların dayanıklılığı ve müttefiklerle birlikte çalışabilirlik bakımından da önemlidir. Bununla birlikte, uluslararası iş birliği ulusal kapasitenin ikamesi değildir; yerli araştırma-geliştirme, nitelikli insan kaynağı ve güvenilir tedarik zinciriyle desteklenmelidir.

Yerli siber güvenlik teknolojilerinin geliştirilmesi, dışa bağımlılığı azaltma ve stratejik özerklik açısından önemlidir. Ancak yerlilik tek başına güvenlik veya kalite göstergesi değildir. Ürünlerin bağımsız güvenlik testlerinden geçirilmesi, güncel tutulması, uluslararası standartlarla uyumlu olması ve yaşam döngüsü boyunca desteklenmesi gerekir. Benzer biçimde, uzman personel yetiştirme politikaları yalnızca kısa süreli eğitim programlarıyla sınırlı kalmamalı; üniversiteler, kamu kurumları ve özel sektör arasında sürdürülebilir araştırma ve istihdam kanalları

oluşturulmalıdır.

Son olarak, siber güvenlik politikalarının uygulanması temel haklar ve hukukun üstünlüğü ilkeleriyle birlikte değerlendirilmelidir. Güvenlik amacıyla alınan tedbirlerin kişisel verilerin korunması, ifade özgürlüğü, haberleşmenin gizliliği ve etkili başvuru yolları üzerindeki etkileri açık ve ölçülü olmalıdır. Bu çerçevede 7545 sayılı Kanun'un uygulaması, yetki ve denetim mekanizmalarının açıklığı ile idari işlemlere karşı hukuki güvenceler bakımından da izlenmelidir. Böylece siber güvenlik, yalnızca teknik kapasite veya devletin müdahale gücü olarak değil, demokratik meşruiyet ve toplumsal güven üreten bir kamu politikası olarak ele alınabilir.

Sonuç

2000'li yıllarda dijitalleşmenin hızlanmasıyla birlikte Türkiye'ye yönelik siber saldırılarda da artış yaşandı. Bu artış, yasal ve kurumsal önlemlerin alınmasını zorunlu kıldı. Bu bağlamda, daha önce yayımlanan Ulusal Siber Güvenlik Stratejisi, 2013-2014 Eylem Planı ve 2016-2019 Ulusal Siber Güvenlik Stratejileri, Türkiye'nin siber alanda nasıl hareket ettiğine katkıda bulunmuştur. Türkiye, 29 Aralık 2020 tarihinde 2020-2023 dönemini kapsayan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nı belirlemiştir. Yakın zamanda ise, Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028) kabul edilmiştir. Daha da önemlisi, önceden BTK'nın ilgilendiği siber güvenlik konusunu tek öncelikli işi yapan Siber Güvenlik Başkanlığı, 2025 yılı başlarında faaliyetlerine başlamıştır. Böylece, Türkiye, siber güvenliğini sağlamak için proaktif bir rol üstlenmeye ve gerekli mevzuat ve kurumları oluşturmaya başlamıştır.

Kilit kurumlar arasında koordineli politikalara rağmen, Türkiye, halen zaman zaman siber güvenlik alanında etkili bir oyuncu olarak ortaya çıkmakta zorlanmaktadır. Bu tarz siber saldırıları azaltabilmek için, Türkiye'nin, komşuları ve diğer devletlerle siyasi sorunlarını çözerek daha barışçıl ilişkiler kurmaya ve yine kendi içerisinde toplumsallaşan siyasi sorunları çözmek için yeni stratejiler uygulayarak militan grupların tehdidini etkisiz hale getirmeye çalışması akılcı olacaktır. Zira günümüzde hiçbir devlet kendi başına yüzde yüz korunaklı değildir; bu konuda uluslararası iş birliği ve uluslararası hukukun geliştirilmesi şarttır. Bu konuda da Birleşmiş Milletler'in ve üye devletlerin öncü rol üstlenmesi gerekmektedir.

KAYNAKÇA

- Aksu, Muharrem & Turhan, Faruk (2012), "Yeni Tehditler, Güvenliğin Genişleme Boyutları ve İnsani Güvenlik", *Uluslararası Alanya İşletme Fakültesi Dergisi*, 4(2), ss. 69-80.
- *Anadolu Ajansı* (2026), "Türkiye'de internet kullananların oranı bu yıl yüzde 92,3'e yükseldi", 05.09.2026, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.aa.com.tr/tr/bilim-teknoloji/turkiyede-internet-kullananlarin-orani-bu-yil-yuzde-92-3e-yukseldi/4018733.
- Andress, Jason & Winterfield, Steve (2014), *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners,* Waltham, MA: Elsevier Inc.
- Carafano, James & Sayers, Eric (2008), "Building Cyber Security Leadership for the 21st Century", The Heritage Foundation, 16.12.2008, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.heritage.org/defense/report/building-cyber-security-leadership-the-21st-century.
- Cavelty, Myriam Dunn (2010), "Cyber Security", içinde (editör: J. Peter Burgess) *The Routledge Handbook of New Security Studies,* New York: Taylor & Francis Group, ss. 154-162.
- Clark, Richard A. & Knake, Robert K. (2011), *Siber Savaş*, Çeviri: Murat Erduran, İstanbul: İstanbul Kültür Üniversitesi Yayınları.
- Çakır, Hüseyin & Kılıç, M. Serkan (2014), *Güncel Tehdit Siber Suçlar,* Ankara: Seçkin Yayınları.
- Çelik, Emine (2019), "Siber Terörizm ve IŞİD-Bitcoin İlişkisi", *Ortadoğu Analiz*, 10(89), ss. 86-89.
- Çelik, Şener (2014), "Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme", *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi,* 15(1), ss. 137-175.
- Farwell, James P. & Rohozinski, Rafal (2011), "Stuxnet and the Future of Cyber War", *Survival,* 53(1), ss. 23-40.
- Gücüyener, Ayhan (2016), "21. Yüzyılda 'Siber' Rekabet: Yeni Hedef Kritik Altyapılar mı?", Linkedin, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.linkedin.com/pulse/21-y%C3%BCzy%C4%B1lda-siber-rekabet-yeni-hedef-kritik-m%C4%B1-ayhan-gucuyener/.
- Hansen, Lene & Nissenbaum, Helen (2009), "Digital Disaster, Cyber Security and the Copenhagen School", *International Studies Quarterly,* 53(4), ss. 1155-1175.
- Hildreth, Steven A. (2001), "Cyberwarfare", CRS Report for Congress, 19.06.2001, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://nsarchive2.gwu.edu//NSAEBB/NSAEBB424/docs/Cyber-014.pdf.
- Iasiello, Emilio (2014), "Is Cyber Deterrence an Illusory Course of Action?", *Journal of Strategic Security,* 7(1), Bahar 2014, ss. 54-67.
- Jalil, Shamsuddin Abdul (2003), "Countering Cyber Terrorism Effectively: Are We Ready to Rumble?", GIAC, Haziran 2003, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.giac.org/paper/gsec/3108/countering-cyber-terrorism-effectively-ready-rumble/105154.
- Karabulut, Bilal (2015), *Güvenlik: Küreselleşme Sürecinde Güvenliği Yeniden*

Düşünmek, Ankara: Barış Kitabevi.

- Karaosmanoğlu, Ali (2015), "Savunma Planlaması ve Stratejik Belirsizlik", *Bilge Strateji,* 7(12), ss. 23-45.

- Libicki, Martin C. (2009), *Cyber Deterrence and Cyberwar*, California: RAND Corporation.

- McCallion, Jane (2022), "What is cyber warfare?", ITPro, 20.05.2022, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.itpro.com/security/28170/what-is-cyber-warfare.

- Merriam-Webster, "Cyber", Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.merriam-webster.com/dictionary/cyber.

- Örmeci, Ozan & Yılmaz, Eren Alper & Köker, Ahmet Emre (2022), "Turkey's Cyber Security Policies", içinde (editörler: Hasret Çomak & Burak Şakir Şeker & Yaprak Civelek & Çağla Arslan Bozkuş) *Cyber Environment and International Politics,* Londra: TPLondon, ss. 67-91.

- Republic of Turkey Ministry of Transport Maritime Affairs, and Communications, *2016-2019 National Cyber Security Strategy,* Erişim Tarihi: 04.10.2026, Erişim Adresi: https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusalsibereng.pdf.

- *Reuters* (2015), "Apparent Islamic State backers hack U.S. military Twitter feed", 13.01.2015, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.reuters.com/article/us-cybersecurity-centcom-hack-idUSKBN0KL1UZ20150112/.

- Singer, P. W. & Friedman, Allan (2014), *Cybersecurity and Cyberwar: What Everyone Needs to Know,* Oxford: Oxford University Press.

- Şenol, Mustafa (2020), "Türkiye'nin Ulusal Siber Güvenlik Strateji ve Politikalarının Olusturulması Çerçevesinde Caydırıcılık", Doktora Tezi, İstanbul Teknik Üniversitesi, İstanbul, Türkiye.

- T.C. Siber Güvenlik Başkanlığı, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://siberguvenlik.gov.tr/.

- *The Guardian* (2015), "Briton lead suspect after US Central Command's Twitter account is hacked", 14.01.2015, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.theguardian.com/us-news/2015/jan/14/briton-suspect-us-central-command-twitter-hack-junaid-hussain-tony-blair.

- Thomas, Timothy L. (2003), "Al Qaeda and the Internet: The Danger of 'Cyberplanning'", *Parameters,* 33(1), ss. 114-122.

- TUİÇ (2017), "Gözetim Politikaları ve Terörizm: 11 Eylül 2001", 04.01.2017, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.tuicakademi.org/gozetim-politikalari-terorizm-11-eylul-2001/.

- Turhan, Oğuzhan (2006), "Bilgisayar Ağları İle İlgili Suçlar", Planlama Uzmanlığı Tezi, DPT Müsteşarlığı, Ankara, Türkiye.

- Ulaşanoğlu, M. Emin & Yılmaz, Ramazan & Tekin, M. Alper (2010), *Bilgi Güvenliği: Riskler ve Öneriler*, Ankara: Bilgi Teknolojileri ve İletişim Kurumu (BTK).

- UNTerm, "Cyber space", Erişim Tarihi: 04.10.2026, Erişim Adresi: https://unterm.un.org/unterm2/en/.
- Yayla, Mehmet (2014), "Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı", *Hacettepe Hukuk Fakültesi Dergisi*, 4(2), ss. 181-200.
- Zetter, Kim (2011), "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History", *Wired*, 11.07.2011, Erişim Tarihi: 04.10.2026, Erişim Adresi: https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/.