BİR SİBER SUÇ OLARAK SİBER TERÖRİZM VE TÜRKİYE

Mücahit ERGÜN

Danışman: Doç. Dr. Gülşen AYDIN

Yüksek Lisans Tezi

Kriminalistik Ana Bilim Dalı

2025

(Her hakkı saklıdır.)

T.C.
ATATÜRK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
KRİMİNALİSTİK ANA BİLİM DALI

BİR SİBER SUÇ OLARAK SİBER TERÖRİZM VE TÜRKİYE

(Cyber Terrorism as a Cyber Crime and Türkiye)

YÜKSEK LİSANS TEZİ

Mücahit ERGÜN

Danışman: Doç.Dr. Gülşen AYDIN

Erzurum

Nisan, 2025

FEN BİLİMLERİ ENSTİTÜSÜ
Graduate School of Natural and Applied Sciences

T.C.
ATATÜRK ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü Müdürlüğü
TEZ KABUL VE ONAY TUTANAĞI

BİR SİBER SUÇ OLARAK SİBER TERÖRİZM VE TÜRKİYE

Doç. Dr. Gülşen AYDIN danışmanlığında, Mücahit ERGÜN tarafından hazırlanan bu çalışma, 10/04/2025 tarihinde aşağıdaki jüri tarafından Kriminalistik Anabilim Dalı Kriminalistik Bilim Dalı'nda Yüksek Lisans tezi olarak **oybirliği** ile kabul edilmiştir.

Jüri Başkanı:	Prof. Dr. Handan UYSAL *Atatürk Üniversitesi*	Aslı ıslak imzalıdır
Danışman:	Doç. Dr. Gülşen AYDIN *Atatürk Üniversitesi*	Aslı ıslak imzalıdır
Jüri Üyesi:	Doç. Dr. Özlem ÖZDEMİR TOZLU *Erzurum Teknik Üniversitesi*	Aslı ıslak imzalıdır

Enstitü Yönetim
Kurulunun …./…/…. tarih
ve …… sayılı kararı.

Bu tezin Atatürk Üniversitesi Lisansüstü Eğitim ve Öğretim Yönetmeliği'nin ilgili maddelerinde belirtilen şartları yerine getirdiğini onaylarım.

Prof.Dr. Alper NUHOĞLU
Enstitü Müdürü

Aslı ıslak imzalıdır

Not: Bu tezde kullanılan özgün ve başka kaynaklardan yapılan bildiriş, çizelge, şekil ve fotoğrafların kaynak olarak kullanımı, 5846 sayılı Fikir ve Sanat Eserleri Kanunundaki hükümlere tabidir.

ETİK BİLDİRİM VE İNTİHAL BEYAN FORMU

Yüksek Lisans Tezi olarak Doç.Dr. Gülşen AYDIN danışmanlığında sunulan "Bir Siber Suç Olarak Siber Terörizm ve Türkiye" başlıklı çalışmanın tarafımızdan bilimsel etik ilkelere uyularak yazıldığını, yararlanılan eserlerin kaynakçada gösterildiğini, Fen Bilimleri Enstitüsü tarafından belirlenmiş olan Turnitin Programı benzerlik oranlarının aşılmadığını ve aşağıdaki oranlarda olduğunu beyan ederiz.

Tez Bölümleri	Tezin Benzerlik Oranı (%)	Maksimum Oran (%)
Giriş	*0*	**30**
Kuramsal Temeller	*7*	**30**
Materyal ve Metot	*0*	**35**
Araştırma Bulguları ve Tartışma	*1*	**20**
Sonuçlar	*0*	**20**
Tezin Geneli	*3*	**25**

Not: *Yedi kelimeye kadar benzerlikler ile Başlık, Kaynakça, İçindekiler, Teşekkür, Dizin ve Ekler kısımları tarama dışı bırakılabilir. Yukarıdaki azami benzerlik oranları yanında tek bir kaynaktan olan benzerlik oranlarının* ***%5'den*** *büyük olmaması gerekir.*

Beyan edilen bilgilerin doğru olduğunu, aksi halde doğacak hukuki sorumlulukları kabul ve beyan ederiz.

Tez Yazarı (Öğrenci)	**Tez Danışmanı**
Mücahit ERGÜN	**Doç.Dr. Gülşen AYDIN**
10.4.2025	**10.4.2025**
İmza:	İmza:

* Tez ile ilgili YÖKTEZ'de yayınlamasına ilişkin bir engelleme var ise aşağıdaki alanı doldurunuz.

☐ Tezle ilgili patent başvurusu yapılması / patent alma sürecinin devam etmesi sebebiyle Enstitü Yönetim Kurulunun …./…/…. tarih ve ……. sayılı kararı ile teze erişim 2 (iki) yıl süreyle engellenmiştir.

☐ Enstitü Yönetim Kurulunun …./…/…. tarih ve ……. sayılı kararı ile teze erişim 6 (altı) ay süreyle engellenmiştir.

TEŞEKKÜR

Bu çalışmayı gerçekleştirme sürecinde, desteklerini esirgemeyen ve bilgi birikimiyle bana rehberlik eden değerli danışmanım Doç. Dr. Gülşen AYDIN'a sonsuz teşekkürlerimi sunuyorum. Kendisi, araştırmamın her aşamasında sağladığı yönlendirmelerle çalışmama değer katmıştır.

Bu tez çalışmamın temelini oluşturmamda önemli bir rol oynayan, yüksek lisans eğitimim boyunca bilgi ve deneyimlerini benimle paylaşarak bana akademik anlamda ilham veren başta Kriminalistik Ana Bilim Dalı Başkanı Prof. Dr. Handan UYSAL'a ve Kriminalistik Ana Bilim Dalı'ndaki tüm hocalarıma, ayrıca jüri üyesi olan Doç. Dr. Özlem ÖZDEMİR TOZLU'ya da Jüri'de ilettiği fikirleri ve düzeltme önerileri için teşekkür ederim.

Bu süreçte manevi desteğini bir an olsun esirgemeyen, bana olan inancı ile beni motive eden değerli aileme, kıymetli eşim Büşra Çakır ERGÜN'e, kadim dostum Ahmet Taner ÇELİK'e ve Jandarma Genel Komutanlığı bünyesinde görev yapmakta olan değerli çalışma arkadaşlarıma şükranlarımı sunarım. Bu süreci daha kolay ve anlamlı kılan şüphesiz onların manevi desteğiydi.

Son olarak, çalışmamda faydalandığım literatürü sağlayan ve fikirleriyle çalışmama katkıda bulunan tüm yazarlara ve araştırmacılara teşekkür ederim. Bu çalışma, onların birikim ve çabalarına duyulan saygının bir ürünü olarak ortaya çıkmıştır.

Mücahit ERGÜN

ÖZET

YÜKSEK LİSANS TEZİ
BİR SİBER SUÇ OLARAK SİBER TERÖRİZM VE TÜRKİYE

Mücahit ERGÜN

Danışman: Doç. Dr. Gülşen AYDIN

Amaç: Tez, siber terörizmi bir suç türü olarak detaylı şekilde inceleyip evrimini ortaya koymayı, Türkiye'ye yönelik siber terörizm tehditlerinin nasıl evrildiğini göz önüne sermeyi ve Türkiye'nin bu suça karşı geliştirdiği stratejik, hukuki ve teknolojik mücadele yaklaşımlarını aydınlatmayı hedeflemektedir. Bu hedeflerin gerçekleştirilmesi yoluyla, siber terörizmle mücadeledeki güçlü ve zayıf yaklaşımları belirleyerek gelecekteki stratejilere yönelik öneriler sunmak amaçlanmaktadır.

Yöntem: Çalışmanın ana araştırma yöntemi vaka çalışmasıdır. Vaka çalışmasını gerçekleştirebilmek için literatür taraması ve içerik analizi yöntemleri de yardımcı yöntemler olarak bir arada kullanılmış; Literatür taraması ve içerik analizinde ikincil kaynaklardan faydalanılmıştır. Bu kaynaklar arasında akademik makaleler, ulusal ve uluslararası raporlar, vaka incelemeleri ve yasal düzenlemeler yer almıştır. Türkiye'de siber terörizme ilişkin örnekler, olaylar detaylı şekilde ele alınmış ve bu olaylar üzerinden Türkiye'nin mevcut hukuki, teknik ve stratejik altyapısı değerlendirilmiştir. Çalışmada, gereğinde nicel verilerle de desteklenen nitel veri analizi yöntemiyle, Türkiye'nin siber güvenlik kapasitesi ve uluslararası işbirliklerinin etkinliği irdelenmiştir.

Bulgular: Türkiye'ye siber terörizmin büyük ölçüde dünyada siber terörizmin evrimine paralel şekilde evrildiği bulgusuna ulaşılmıştır. Türkiye'nin bu değişime cevap vermek için, artan siber tehditlere karşı siber güvenlik stratejileri, kamu-özel sektör iş birlikleri ve teknolojik kapasite geliştirme gibi alanlarda önemli adımlar attığı belirlenmiştir. Yine de, dinamik tehdit ortamı nedeniyle stratejilerin sürekli güncellenmesinin gerektiğine dikkat çekilmiştir. Enerji, sağlık ve finans sektörlerinde siber terörizmin oluşturduğu ciddi riskler, hukuki düzenlemelerin ve teknik kapasitenin güçlendirilmesi gerektiğini göstermektedir.

Sonuç: Bu tez çalışması, Türkiye'nin siber terörizme karşı kapsamlı bir ulusal strateji oluşturma sürecinde önemli ilerlemeler kaydettiği ancak bu stratejilerin daha etkin hale getirilmesi gerektiği sonucuna ulaşmıştır. Bu bağlamda, uluslararası iş birliği ve kamu-özel sektör ortaklıklarının artırılması, siber güvenlik ekosisteminin güçlendirilmesinde kilit bir role sahiptir. Aynı zamanda, toplumun dijital okuryazarlık seviyesinin yükseltilmesi ve farkındalık kampanyalarının artırılması, bireysel ve toplumsal düzeyde savunma kapasitesinin geliştirilmesi açısından önemlidir.

Anahtar Kelimeler: Siber terörizm, Türkiye, kritik altyapı, siber güvenlik stratejileri, hukuki düzenlemeler, uluslararası işbirliği, kamu-özel işbirliği.

Nisan 2025, 76 sayfa

ABSTRACT

MASTER'S THESIS

CYBER TERRORISM AS A CYBER CRIME AND TURKEY

Mücahit ERGÜN

Advisor: Assoc. Prof. Dr. Gülşen AYDIN

Purpose: This thesis aims to examine cyber terrorism in detail as a form of crime, to trace its historical evolution, to analyze how cyber terrorism threats targeting Turkey have developed over time, and to shed light on Turkey's strategic, legal, and technological approaches to combatting this crime. By achieving these objectives, the study seeks to identify the strengths and weaknesses of current counter-cyber terrorism efforts and to offer recommendations for future strategies.

Methodology: The primary research method employed in this study is case study analysis. To support this method, literature review and content analysis techniques were also utilized. Secondary sources such as academic articles, national and international reports, case studies, and legal regulations were used during the data collection process. Specific cyber terrorism incidents in Turkey were examined in detail, and through these cases, Turkey's existing legal, technical, and strategic infrastructure was evaluated. Qualitative data analysis, supported by quantitative data when necessary, was employed to assess Turkey's cybersecurity capacity and the effectiveness of its international collaborations.

Findings: The findings indicate that cyber terrorism in Turkey has evolved largely in parallel with global developments in the field. In response to these evolving threats, Turkey has taken significant steps in areas such as cybersecurity strategies, public-private partnerships, and the enhancement of technological capabilities. However, the dynamic nature of cyber threats necessitates the continuous updating of these strategies. The study highlights serious risks posed by cyber terrorism to critical sectors such as energy, healthcare, and finance, emphasizing the need to strengthen both legal regulations and technical capacity.

Conclusion: The thesis concludes that while Turkey has made considerable progress in developing a comprehensive national strategy against cyber terrorism, there remains a need to further enhance the effectiveness and sustainability of these efforts. International cooperation and the strengthening of public-private sector partnerships play a key role in fortifying the national cybersecurity ecosystem. Moreover, improving digital literacy across society and increasing public awareness campaigns are essential for enhancing defensive capacities at both individual and societal levels.

Keywords: Cyber terrorism, Turkey, critical infrastructure, cybersecurity strategies, legal regulations, international cooperation, public-private partnership.

April 2025, 76 pages

İÇİNDEKİLER

KABUL VE ONAY TUTANAĞI i
ETİK BİLDİRİM VE İNTİHAL BEYAN FORMU ii
TEŞEKKÜR iii
ÖZET iv
ABSTRACT v
İÇİNDEKİLER vi
TABLOLAR DİZİNİ viii
ŞEKİLLER DİZİNİ ix
KISALTMALAR VE SİMGELER DİZİNİ x
GİRİŞ 1
KURAMSAL TEMELLER 3
Siber Terörizmin Tanımı ve Kapsamı 3
Siber Terörizmin Teknikleri ve Hedefleri 6
Kullanılan Teknolojiler 7
Siber Terörizmin Türleri 9
Hizmet Reddi (DoS) ve Dağıtılmış Hizmet Reddi (DDoS) Saldırıları 9
Kritik Altyapılara Yönelik Saldırılar 10
Veri İhlali ve Bilgi Çalma 10
Sosyal Mühendislik ve Kimlik Avı (Phishing) Saldırıları 11
Siber Propaganda ve Psikolojik Savaş 11
Siber Terörizmin Aktörlerinin Evrimi 12
Siber Terörizmde Güdü ve Niyetlerin Evrimi 13
Siber Terörizmde Hedefler, Araçlar ve Etkilerin Evrimi 15
Siber Terörizm ile Ulusal ve Uluslararası Mücadelenin Evrimi 18
Uluslararası İş Birliği ve Önlemler 19
MATERYAL VE METOT 22
BULGULAR 24
Türkiye'ye Yönelik Siber Terörizmde Evrim: Aktörler, Güdüler, Niyetler, Hedefler, Araçlar ve Etkiler 24
Aktörlerin Evrimi 24
Güdülerin ve Niyetlerin Evrimi 25
Hedeflerin Evrimi 26

Kullanılan Araçların Evrimi 26
Etkilerin Evrimi 27
2015–2025 Arası Türkiye'de Gerçekleşen Önemli Siber Saldırılar: Bir Siber Terörizm Perspektifi 29
Anonymous'un 2015 yılında .tr DNS Altyapısına Saldırısı 29
2016 RedHack Saldırısı ve Enerji Bakanı'nın e-postalarının Sızdırılması 29
2017 WannaCry Fidye Yazılımı Saldırısı 29
2023 e-Devlet Veri Sızıntısı 29
Sağlık ve Telekom Sektörüne Yönelik Diğer Saldırılar 30
Enerji Altyapılarına Yönelik Saldırılar 30
Sağlık Altyapılarına Yönelik Saldırılar 31
Türkiye'nin Siber Güvenlik Politikasının Evrimi 33
Türkiye'nin Uluslararası İlişkileri Bağlamında Siber Terörizm 34
Uluslararası Hukuki Çerçeve ve İş Birliği Mekanizmaları 35
Bölgesel Yapılanmalar: AB ve NATO Örnekleri 35
Özel Sektörün ve Kamu-Özel İş Birliğinin Rolü 36
Türkiye'nin Uluslararası İş Birliği Politikası 36
Siber Terörizmin Hukuki Tanımlanabilirliği: Ceza Hukuku ve Uluslararası İş Birliği 38
Bilgi Güvenliği, Dezenformasyon ve Dijital Haklar: Regülasyonun Genişlemesi 38
Ulusal Strateji Belgeleri ve Kurumsallaşma Süreci 39
Entegre Güvenlik Yapısı: 7545 sayılı Siber Güvenlik Kanunu 39
Türkiye'nin Siber Terörizm ile Mücadelesi 39
Teknolojik Kapasite ve Kamu-Özel İşbirlikleri 40
Teknolojik Kapasite 42
Kamu-Özel İşbirlikleri 42
Uluslararası İşbirlikleri 42
İnsan Kaynağı Gelişimi 43
TARTIŞMA 44
SONUÇ VE ÖNERİLER 57
KAYNAKLAR 59
ÖZGEÇMİŞ 64

TABLOLAR DİZİNİ

Tablo 1. Türkiye'de Siber Terörizm Vakaları 28
Tablo 2. Hukuki Düzenlemeler ve Mevzuat 37
Tablo 3. Teknolojik Kapasite ve Kamu-Özel İşbirliklerinin Gelişimi 41

ŞEKİLLER DİZİNİ

Şekil 1. Türkiye'de enerji altyapılarına yönelik siber saldırı sayıları 30
Şekil 2. Türkiye'de sağlık altyapılarına yönelik siber saldırı sayıları 32

KISALTMALAR VE SİMGELER DİZİNİ

AB	: Avrupa Birliği
APT	: Gelişmiş Kalıcı Tehdit
CERT/CSIRT	: Bilgisayar Olaylarına Müdahale Ekibi / Bilgi Güvenliği Olay Müdahale Ekibi
DDoS	: Dağıtılmış Hizmet Reddi
KVKK	: Kişisel Verilerin Korunması Kanunu
NATO	: Kuzey Atlantik Antlaşması Örgütü
TCK	: Türk Ceza Kanunu
TİB	: Telekominikasyon İletişim Başkanlığı
TÜBİTAK	: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
USOM	: Ulusal Olaylara Müdahale Merkezi
SOME	: Siber Olaylara Müdahale Ekipleri
Vb.	: Ve benzeri
Vd.	: Ve diğerleri

GİRİŞ

Siber terörizm, belirli politik veya sosyal amaçlar doğrultusunda bilgisayar sistemleri ve bilgi teknolojileri kullanılarak bireylere, kurumlara ve devletlere zarar verme, baskı uygulama ve korku yaratma amacı taşıyan terörizm çeşidi olarak tanımlanmaktadır. Geleneksel terör eylemlerinden farklı olarak, siber terörizm fiziksel şiddet unsurlarını içermese de, ekonomik, psikolojik ve sosyal açıdan büyük çapta tahribata yol açabilen bir tehdit türüdür (Atasever vd. 2019). Siber terörizmin temel uygulama alanları arasında kritik altyapılara yönelik saldırılar, devletin gizli bilgilerinin yasa dışı yollarla ele geçirilmesi, bankacılık sistemlerine müdahale edilerek ekonomik istikrarsızlık yaratılması ve dezenformasyon yoluyla toplumsal güvenin sarsılması yer almaktadır (Yılmaz ve Karakaş 2020).

İnternetin ve dijital teknolojilerin yaygınlaşması, iletişimi ve bilgiye erişimi büyük ölçüde kolaylaştırırken, aynı zamanda güvenlik açısından önemli riskleri de beraberinde getirmiştir. 1980'lerden itibaren küresel çapta gelişen dijital altyapılar, hem devletler ve özel sektör için kritik fırsatlar sunmuş hem de kötü niyetli aktörler tarafından da yeni nesil saldırı yöntemlerinin geliştirilmesine olanak sağlamıştır. Özellikle düşük maliyetli, anonim ve sınır tanımayan niteliği nedeniyle, siber saldırılar giderek daha sofistike hale gelmiş ve devletler için ciddi bir güvenlik sorunu oluşturmuştur (Akbaş 2018). Günümüzde siber terörizm, yalnızca devletler tarafından değil, aynı zamanda organize suç örgütleri ve ideolojik gruplar tarafından da kullanılan bir saldırı yöntemi haline gelmiştir.

Siber terörizmin uluslararası güvenlik dinamiklerine etkisi oldukça büyüktür. Gelişmiş ülkeler, kritik altyapılarını koruma altına almak için siber güvenlik politikalarını sürekli olarak güncellemekte ve yeni stratejiler geliştirmektedir (Gürkaynak ve İren 2011). Türkiye gibi gelişmekte olan ülkelerde ise siber tehditler karşısında yalnızca teknik altyapının güçlendirilmesi için değil aynı zamanda gerekli hukuki ve diplomatik tedbirleri almak için mücadele vermektedir (Atasever vd. 2019). Türkiye'de son yıllarda artan dijitalleşme süreci, ülkenin siber tehditlere karşı daha kırılgan hale gelmesine neden olmuştur. Bu nedenle, Türkiye'nin siber güvenlik politikalarının gelişimi, mevcut tehditlerle mücadelede kat ettiği yol, izlediği yöntemler, etkinliği ve uluslararası iş birliklerinin bu mücadeledeki rolü bireysel, ulusal ve uluslararası güvenlik açısından büyük önem arz etmektedir.

Siber terörizmin gelecekte daha etkin hale gelebileceği öngörülmekte ve silahlı terörizme yönelik önlemlerin yanı sıra siber alanı hedef alan stratejik tedbirlerin geliştirilmesi kritik bir ihtiyaç olarak değerlendirilmektedir (Iftikhar 2024). Teknolojik ilerlemelerin

olağanüstü bir hızla gelişmesi, siber uzayın suç faaliyetlerine olanak tanıyan yeni bir alan olarak ortaya çıkmasına neden olmuş ve bu bağlamda, siber terörizm gibi yeni bir tehdit türü gündeme gelmiştir. Siber terörizm, bireysel, ulusal ve küresel güvenlik üzerinde oluşturduğu derin etkiler nedeniyle giderek daha kritik bir sorun olarak değerlendirilmektedir. Bu nedenle hem dünya genelinde hem de Türkiye örneğinde siber terörizmin ve evriminin detaylı olarak analiz edilmesi güvenlik açısından önemli bir gerekliliktir.

Bu tez çalışmasının temel amacı, siber terörizmin tarihsel evrimini inceleyerek, günümüzde ve gelecekte karşılaşılabilecek tehditleri anlamak ve bu tehditlere karşı geliştirilebilecek stratejileri hem dünya çapında hem de Türkiye örneğinde analiz etmektir. Bu bağlamda, siber terörizmin aktörlerini, güdülerini, niyetlerini, hedeflerini, araçlarını ve etkilerini anlamak adına içerik analizi yöntemi kullanılarak ikincil kaynaklara dayalı bir inceleme yapılmıştır. Bu kapsamda, akademik çalışmalar, ulusal ve uluslararası güvenlik raporları, gazete makaleleri ve vaka analizleri detaylı bir şekilde incelenmiştir. Ayrıca, Türkiye özelinde gerçekleştirilecek vaka analizi yöntemiyle, Plotnek and Slay (2021) tarafından sağlanan kuramsal çerçeve temel alınarak siber terörizmin ülkemize özgü dinamikleri değerlendirilmiştir.

Bu çerçevede tez çalışması şu bölümlerden oluşturulmuştur. İlk olarak, siber terörizmin kavramsal çerçevesi ele alınarak bu tehdidin temel nitelikleri ve evrimi değerlendirilerek, ikinci bölümde, siber terörizmin aktörleri, güdüleri ve yöntemleri incelenmiş, farklı motivasyonlarla hareket eden grupların siber saldırılardaki stratejileri analiz edilmiştir. Üçüncü bölümde, siber terörizmin hedefleri, kullanılan araçlar ve bu saldırıların etkileri üzerinde durulmuştur. Dördüncü bölümde, Türkiye bağlamında siber terörizm tehdidinin gelişimi ve bu tehdide karşı alınan önlemler tartışılmış, son olarak sonuç ve öneriler kısmında, siber terörizmin küresel güvenlik üzerindeki etkileri, Türkiye'nin mevcut siber güvenlik politikalarının etkinliği ve gelecekte alınabilecek önlemler değerlendirilmiştir. Siber terörizm, dijital çağın en karmaşık ve çok boyutlu tehditlerinden biri olarak yalnızca teknolojik değil, aynı zamanda politik, hukuki ve toplumsal yönleriyle ele alınması gereken bir meseledir. Bu nedenle, kapsamlı bir mücadele stratejisi geliştirmek ve uluslararası iş birliği mekanizmalarını güçlendirmek kaçınılmazdır. Bu tez çalışması, siber terörizmin evrimini analiz ederek, Türkiye'nin siber güvenlik politikalarının gelişimine katkı sunmayı ve uygulamada kullanılabilecek somut çözüm önerileri geliştirmeyi hedeflemektedir.

KURAMSAL TEMELLER

Bu bölüm, öncelikle siber terörizmin tanımını, kapsamını, kullandığı teknikleri inceleyerek, sonra da hem siber terörizmin hem de bu suç türüne karşı dünyadaki mücadelenin evrimine ışık tutarak çalışmanın kuramsal temellerini oluşturmaktadır.

Siber Terörizmin Tanımı ve Kapsamı

Siber terörizm kavramı, literatürde farklı şekillerde tanımlanmakta olup, üzerinde uzlaşıya varılmış tekil bir tanım henüz bulunmamaktadır (Plotnek and Slay 2021). Bazı yaklaşımlar, kavramı dar bir çerçevede ele alarak yalnızca tanınmış terör örgütleri tarafından gerçekleştirilen şiddet içerikli siber saldırıları bu kapsamda değerlendirmektedir. Buna karşılık, bazı yaklaşımlar ise kavramı daha geniş bir perspektiften yorumlayarak, terörist grupların dijital ortamda yürüttükleri propaganda faaliyetleri ve eleman temini gibi şiddet içermeyen eylemleri de siber terörizm tanımına dâhil etmektedir (Jarvis and Macdonald 2014).

Siber terörizm, geleneksel (fiziksel) terörizmden farklı olarak dijital ortamda gerçekleştirilen eylemleri kapsamaktadır. Bu tür eylemler çoğunlukla devletin ya da özel sektörün kritik altyapılarına, finansal sistemlerine ve diğer stratejik dijital varlıklarına yönelik olarak düzenlenmektedir. Bu kapsamda siber terörizmin temel amacı; toplumsal düzeyde kaos yaratmak, ulusal güvenliği zayıflatmak ve hedef ülkenin ekonomik ya da siyasi istikrarını sarsmaktır (Chesney 2017). Dijital teknolojilerin sunduğu imkânlar aracılığıyla geleneksel terör yöntemlerinden ayrılan bu tehdit türü, daha karmaşık biçimlere evrilerek günümüz güvenlik gündeminde ön plana çıkmaktadır.

Siber terörizmin ayırt edici özelliği, internet ve dijital sistemlerin birincil araç olarak kullanılmasıdır. Bu saldırılar, hedefin coğrafi konumuna bağlı kalmaksızın, küresel çapta etkiler yaratabilmektedir. Böylece siber terörizm, yalnızca ulusal sınırlarla sınırlı olmayan, uluslararası boyut taşıyan bir tehdit alanı hâline gelmektedir. Örneğin, bir saldırgan kendi ülkesinde bulunurken başka bir devletin kritik altyapısına saldırı gerçekleştirebilir. Bu nedenle siber terörizm, ulusal güvenliğe yönelik sınır aşan bir tehdit olarak kabul edilmektedir (Tolk and Diallo 2019). Bu saldırılar çoğunlukla ideolojik, siyasi veya dini amaçlarla gerçekleştirilir. Amaç, bireylerde ve toplumda korku ve panik yaratmaktır. Geleneksel terörizmin dijital ortama uyarlanmış bir formu olan siber terörizm, doğrudan fiziksel zarardan ziyade dijital altyapılar üzerinden ekonomik, sosyal ve psikolojik tahribat yaratmayı hedefler (Akbaş 2018).

Güler (2019), siber terörizmin yalnızca ulus devletleri değil, aynı zamanda özel sektör kuruluşları ve bireyleri de tehdit ettiğini belirtmektedir. Bu çok boyutlu tehdit, yalnızca teknik değil; hukuki, sosyolojik ve siyasi açılardan da değerlendirilmelidir. Enerji santralleri, ulaşım

ağları, sağlık sistemleri ve finansal kurumlar gibi kritik altyapılar, başlıca hedefler arasındadır. Bu tür saldırılar, teknik sistemlerin ötesinde, toplumsal yaşamın sürdürülebilirliğini ve kamu güvenliğini de tehdit etmektedir (Çelik 2021).

Dijital ağların sınır tanımayan yapısı, siber teröristlerin eylemlerini mekânsal kısıtlamalardan bağımsız biçimde gerçekleştirmelerine olanak tanır (Ekinci 2018). NATO Cooperative Cyber Defence Centre of Excellence (2007) tarafından yayımlanan bir raporda da belirtildiği gibi, siber terörizm ulusal sınırları aşan bir tehdit olup, yalnızca hedef ülkeyi değil, uluslararası sistemi de etkileyebilmektedir. Bu nedenle siber terörizm, salt teknolojik değil; politik, hukuki ve toplumsal boyutlarıyla da ele alınmalıdır (Plotnek and Slay 2021).

Siber terörizmin tanımı, saldırıyı gerçekleştiren aktörün amacı ve kullandığı yöntemler doğrultusunda netleşmektedir. Özdemir (2020), siber terörizmi diğer siber tehditlerden ayıran üç temel özelliği vurgular: (1) eylemin ideolojik veya siyasi amaca hizmet etmesi, (2) dijital altyapılara zarar verme amacı taşıması ve (3) toplumda korku ve kaos ortamı yaratmayı hedeflemesi. Bu unsurlar doğrultusunda, siber terörizm sıradan siber suçlardan ayrışır. Örneğin, kişisel kazanç amacı güden bir siber dolandırıcılık eylemi siber suç kapsamında değerlendirilirken; ideolojik amaç taşıyan ve enerji altyapısını hedef alan bir saldırı siber terörizm olarak sınıflandırılır.

Dezenformasyon ve bilgi manipülasyonu, siber terörizmin kapsamını genişleten bir başka unsurdur. Sosyal medya platformlarının yaygınlaşmasıyla, bu tehdit yalnızca teknik altyapılara değil, toplumların bilgi güvenliğine de yönelmiştir. Kızılkaya (2021), dezenformasyonu siber terörizmin toplumsal etkisini artıran stratejik bir araç olarak tanımlar ve dijital okuryazarlığın bu tehdide karşı etkili bir savunma olduğunu vurgular.

Siber terörizm, dijital ortamın sunduğu anonimlik imkânı sayesinde tespiti ve önlenmesi güç bir tehdit türüdür. Saldırganlar kimliklerini gizleyerek faaliyet gösterebilmekte, bu da güvenlik birimlerinin müdahale süreçlerini zorlaştırmaktadır. Plotnek and Slay (2021), anonimliğin siber terörizmin en karmaşık yönlerinden biri olduğunu ve klasik güvenlik yaklaşımlarıyla bu tehdidin kontrol altına alınmasının zorlaştığını belirtmektedir.

Kullanılan teknolojiler ve yöntemlerin karmaşıklığı, siber terörizmi diğer siber tehditlerden ayıran bir diğer unsurdur. Zararlı yazılımlar, Dağıtılmış Hizmet Reddi (DDoS) saldırıları gibi araçlarla gerçekleştirilen saldırılar, dijital altyapıların bütünlüğünü zedeleyebilir ve ciddi toplumsal sonuçlara yol açabilir (Hassan and Chen 2020). Örneğin, enerji şebekesinin çökmesi ya da bankacılık sistemlerinin işlevsiz hâle gelmesi, yalnızca teknik değil, toplumsal düzeyde de korku ve kaos yaratır (Denning 2000).

Siber terörizm, teknolojik gelişmelerle birlikte sürekli evrilen dinamik bir tehdittir. Gelişen dijital teknolojiler, daha sofistike saldırı yöntemlerinin ortaya çıkmasına neden olmakta; mevcut savunma sistemlerini yetersiz kılmakta ve yeni tehdit türlerinin oluşmasına zemin hazırlamaktadır. Bu nedenle siber terörizmle mücadele, yalnızca ulusal düzeyde değil, aynı zamanda uluslararası iş birliği ve teknolojik inovasyonu da içermelidir (Libicki 2007).

Teknolojik araçlarla gerçekleştirilen ve dijital altyapılara zarar vermeyi, toplumsal korku yaratmayı amaçlayan siber terörizm; hem ulusal hem de uluslararası güvenlik açısından giderek daha kritik bir tehdit hâline gelmektedir. Türkiye gibi dijitalleşme sürecindeki ülkeler için bu tehdit, sadece teknik önlemlerle değil; aynı zamanda hukuki, sosyal ve politik stratejilerle bütüncül biçimde ele alınmalıdır. Siber terörizmin tanımının ve kapsamının açık biçimde belirlenmesi, etkili ve sürdürülebilir mücadele politikalarının oluşturulması açısından büyük önem taşımaktadır.

Siber terörizm kavramına ilişkin farklı tanımlar, kavramın kapsamına yönelik belirsizliklere yol açmakta ve bu durum, alana yönelik politika üretimini zorlaştırmaktadır. Kavramsal dağınıklık, hem akademik çalışmaların sistematik biçimde ilerlemesini hem de konuya ilişkin hukuki düzenlemelerin etkin biçimde yapılandırılmasını engellemektedir (Al Mazari *et al* 2018). Bu nedenle siber terörizm kavramının açık, tutarlı ve üzerinde uzlaşı sağlanmış bir çerçeve ile tanımlanması büyük önem taşımaktadır.

Al Mazari *et al* (2018), siber terörizm kavramına yönelik belirsizlikleri gidermek amacıyla, alana özgü ortak nitelikleri esas alan beş bileşenli bir taksonomi geliştirmiştir. Bu yaklaşım, eylemlerin ayırt edici özelliklerini sistematik biçimde ortaya koyarak kavramın daha tutarlı biçimde ele alınmasını sağlamaktadır. Bu taksonomi şu unsurlardan oluşmaktadır: hedef (target), güdü (motive), araç (means), etki (effect) ve niyet (intent).

Plotnek and Slay (2021) tarafından geliştirilen genişletilmiş taksonomi, bu çerçeveye "aktör" unsurunu da ekleyerek toplamda altı bileşenli bir model önermektedir: aktör (actor), güdü (motive), niyet (intent), araç (means), etki (effect), hedef (target). Bu model, siber terörizmin daha sistematik ve kapsamlı biçimde analiz edilmesine olanak tanımakta; hem kuramsal hem de uygulamalı çalışmalarda derinlemesine değerlendirmelere imkân sağlamaktadır.

Bu tez çalışmasında, altı bileşenli model kuramsal temel olarak benimsenmiştir. Bu çerçeve, siber terörizm olgusunun çok boyutlu yapısını yansıtarak, literatürdeki tanımsal farklılıkları gidermekte ve analizleri daha tutarlı bir zemine oturtmaktadır. Böylece hem teorik hem de pratik düzeyde siber terörizmle ilgili politika önerilerinin daha sağlam temellere dayandırılması mümkün olmaktadır.

Siber Terörizmin Teknikleri ve Hedefleri

Siber terörizm, dijital ortamda gerçekleşen ve toplumun düzenini, devletlerin güvenliğini, kritik altyapılarını ve bireyleri hedef alan terörist saldırılardır. Bu tür saldırılar, hedeflerin dikkatlice seçilmesiyle daha etkili hale gelir. Hedef belirleme, siber terörizmin en kritik aşamalarından biridir ve saldırının amacına ulaşabilmesi için doğru hedeflerin seçilmesi gerekmektedir. Hedef belirleme süreci genellikle stratejik değer, güvenlik açıkları, psikolojik etkiler ve toplumsal sonuçlar gibi faktörlere dayanmaktadır (Yüksel 2011).

Siber teröristler, hedef belirlerken genellikle stratejik öneme sahip ve kritik işlevleri yerine getiren altyapıları hedef alır. Devletlerin yönetim sistemleri, finansal kurumlar, sağlık hizmetleri ve enerji altyapıları gibi kritik sektörler, bu tür saldırılara en sık hedef olan yapılardır. Bu tür hedefler, yalnızca dijital sistemlerin zarar görmesine yol açmakla kalmaz, aynı zamanda toplumsal düzeni sarsma amacı taşımaktadır. Estonya'ya 2007 yılında gerçekleştirilen siber saldırılar, devletin dijital altyapısına yapılan stratejik bir saldırı örneğidir. Bu saldırılar, sadece dijital sistemleri etkilemekle kalmamış, aynı zamanda devletin genel işleyişini aksatmıştır (Yüksel 2011). Siber teröristler, hedeflerini belirlerken sistemdeki zayıf noktaları tespit etmeye çalışmaktadır. Birçok dijital altyapı, güvenlik açıkları ve savunmasız noktalar içerir. Bu noktalar, saldırganların hedeflerine ulaşmalarını kolaylaştıran kritik unsurlardır. Güvenlik açıkları, sistem yazılımlarındaki hatalar veya güncel olmayan yazılımlar gibi zayıf noktalar, saldırıların başarılı olmasına olanak tanımaktadır. Türkiye'deki kamu kurumlarına yönelik 2016'da gerçekleşen siber saldırılar, bu tür zayıf noktaların nasıl hedef alınabileceğinin örneklerinden biridir. Saldırganlar, sistemin güvenlik açıklarından faydalanarak, önemli verileri sızdırmış ve toplumsal güvenliği tehdit etmiştir (Erdem 2018).

Siber teröristlerin hedef belirlerken bir diğer önemli faktör, yaratmak istedikleri psikolojik etkidir. Hedef alınan sistemlerin çökmesi, toplumda büyük bir korku, belirsizlik ve güvensizlik yaratabilmektedir. Bu tür saldırılar, toplumsal huzursuzluk yaratmayı ve halkın devlete olan güvenini zayıflatmayı amaçlamaktadır. Özellikle, kamu hizmetlerinin aksaması ve kişisel bilgilerin sızdırılması gibi eylemler, kamuoyunda büyük bir etki oluşturabilmektedir. Türkiye'de 2015 yılında büyük bir bankaya yapılan siber saldırı, bankanın dijital altyapısına büyük zararlar vermiş ve aynı zamanda halkın ekonomik güvenini sarsmıştır. Bu tür saldırılar, hedef belirlemede psikolojik etkilerin ne denli önemli olduğunu gösteren örneklerdir (Sarı 2017). Siber teröristler, hedef belirlerken yalnızca fiziksel tahribat yaratmakla kalmaz aynı zamanda sosyal ve ekonomik etkiler de yaratmaya çalışırlar. Özellikle; ekonomik hedefler, finansal kurumlar ve ticaret sistemleri gibi kritik sektörlere yönelik siber saldırılar, büyük ekonomik zararlara yol açmaktadır. 2017'deki WannaCry saldırısı gibi büyük çaplı fidye

yazılımı saldırıları, dünya genelinde binlerce kurum ve şirketin dijital altyapısını hedef alarak ekonomik kayıplara neden olmuştur. Bu tür saldırılar yalnızca saldırıya uğrayan kurumları etkilemekle kalmaz, aynı zamanda toplum genelinde büyük bir güvensizlik ve ekonomik kriz yaratabilmektedir. Türkiye'deki bazı büyük e-ticaret firmalarına yönelik siber saldırılar, bu tür saldırıların ekonomik sonuçlarını gösteren örneklerdendir (Demirtaş 2019).

Siber teröristler, hedef belirlerken uluslararası ilişkileri ve jeopolitik durumları da göz önünde bulundururlar. Uluslararası gerilimlerin yüksek olduğu dönemlerde, terörist gruplar, başka ülkelerin dijital altyapılarını hedef almayı tercih edebilmektedir. Bu tür saldırılar, sadece hedef alınan ülkeyi değil, aynı zamanda küresel güvenlik ortamını da tehdit edebilir. 2007 Estonya saldırıları, bir devletin dijital altyapısına yönelik uluslararası bir saldırının etkilerini gözler önüne sermektedir. Saldırganlar, Estonya'ya yapılan siber saldırılarla sadece bir ülkenin altyapısını hedef almakla kalmamış aynı zamanda NATO'nun siber güvenlik konusundaki tutumunu etkilemiştir (Kılınç 2020).

Siber terörizm, teknolojik altyapılara zarar verme, toplumda korku ve güvensizlik yaratma amacıyla kullanılan çeşitli teknikler ve araçlarla gerçekleştirilmektedir. Bu eylemler, hedef alınan sistemlerin karmaşıklığına ve teröristlerin amaçlarına bağlı olarak farklılık gösterebilir. Siber teröristlerin kullandığı yöntemler, çoğu zaman diğer siber suç faaliyetlerinde kullanılan tekniklerle benzerlik gösterse de etkilerinin boyutu ve ideolojik hedefleri bakımından ayrışmaktadır. Güler (2019), siber terörizmin, sofistike teknikler ve geniş çapta etkili araçlar kullanılarak, ulusal güvenlikten bireysel haklara kadar çeşitli alanlarda büyük tehdit oluşturduğunu belirtmektedir.

Kullanılan Teknolojiler

Siber terörizm, çeşitli teknolojiler ve araçlar kullanarak hem dijital altyapılara zarar vermek hem de toplumsal düzeni sarsmak amacıyla gerçekleştirilmektedir. Teknolojinin hızla evrilmesi, siber saldırıların daha sofistike ve etkili hale gelmesine olanak sağlamaktadır. Siber teröristler, hedeflerine ulaşmak için kullandıkları teknoloji ve araçlarla büyük zararlar verebilir ve devletler, kurumlar ve bireyler için ciddi tehditler oluşturabilir. Aşağıda, siber terörizmde yaygın olarak kullanılan bazı teknolojiler ve bunların nasıl işlediği açıklanmıştır.

Botnetler, birden fazla bağlı cihazın kötü niyetli yazılımlar tarafından ele geçirilerek, bir saldırganın kontrolüne girmesini sağlayan ağlardır. Bu cihazlar, saldırgan tarafından komut alarak büyük çaplı saldırılar gerçekleştirebilir. Dağıtılmış Hizmet Reddi (DDoS) saldırıları gibi geniş ölçekli saldırılar için botnetler sıklıkla kullanılmaktadır. Her bir bot, bir bilgisayar ya da IoT cihazı olabilir, bu da saldırının çok sayıda cihaz üzerinden yapılmasını ve engellenmesinin

oldukça zor hale gelmesini sağlar. 2016 yılında Mirai botneti, dünya çapında bir dizi büyük DDoS saldırısı gerçekleştirmiştir. Botnetlerin kullanımı, siber teröristlerin hedeflerini genişletmesine ve büyük veri merkezlerini veya hükümet sistemlerini hedef almasına olanak tanımaktadır (Kaspersky 2016).

Yapay zekâ (AI) ve makine öğrenimi, siber güvenlik ve siber terörizm alanlarında giderek daha fazla kullanılmaktadır. Siber teröristler, AI ve makine öğrenimi teknolojilerini, saldırıları daha etkili hale getirmek ve saldırılarını gizlemek için kullanabilirler. Bu teknolojiler, ağ güvenliğini aşmak, şifreleri kırmak ve hedeflerin güvenlik sistemlerini atlatmak için optimize edilmiş algoritmalar kullanabilir. Örneğin, yapay zekâ tabanlı yazılımlar, ağda şüpheli davranışları tespit etmekte ve bu davranışlara uygun saldırılar geliştirmekte kullanılabilir. Siber savunma teknolojileri de AI ve makine öğrenimini kullanarak, sürekli gelişen tehditlere karşı savunmalar oluşturmakta kullanılıyor. Ancak, siber teröristler bu teknolojileri de kötüye kullanarak saldırıları hızlandırabilir ve gizlemekte daha başarılı olabilirler (Hussain 2021).

Şifreleme, siber teröristlerin iletişimlerini gizlemek, veri çalmak ve hedeflerine ulaşmak için kullandıkları temel teknolojilerden biridir. Şifreleme, verilerin yalnızca belirli anahtarlarla çözülebilecek şekilde kodlanmasını sağlar. Bu, siber teröristlerin eylemlerini gizlemek ve tespit edilmeden faaliyetlerini sürdürmek için çok etkili bir araçtır. Şifreleme teknolojileri, aynı zamanda fidye yazılımları gibi saldırılarda da yaygın olarak kullanılmaktadır. Fidye yazılımları, genellikle kurbanın dosyalarını şifreleyerek, şifreyi yalnızca saldırganın vereceğini bildirir. Bu tür saldırılarda şifreleme, teröristlerin hedeflerine ulaşmasını sağlarken, aynı zamanda kurbanın veri kaybını da artırır. Ayrıca, bazı siber teröristler, anonimlik sağlamak için şifreli iletişim araçlarını kullanarak güvenlik güçlerinin faaliyetlerini engellemeye çalışırlar (Cohen 2020).

Sosyal medya ve internet platformları, siber teröristlerin ideolojik mesajlarını yaymalarına, propaganda yapmalarına ve toplumsal kargaşa yaratmalarına olanak tanır. Bu araçlar, teröristlerin ideolojilerini yaymak ve toplumu manipüle etmek için güçlü bir araç olabilir. Siber teröristler, sosyal medya üzerinden yanlış bilgi yayarak halkı kışkırtabilir, toplumsal olayları provoke edebilir ve hatta hükümet karşıtı hareketler yaratabilirler. Aynı zamanda, sosyal medya ve internet araçları, siber teröristlerin birbirleriyle iletişim kurmalarını ve birbirlerini koordine etmelerini sağlar. Örneğin, terörist gruplar, sosyal medya platformları üzerinden operasyonlar düzenleyebilir, propaganda yapabilir ve yeni üyeler kazanabilirler. Özellikle anonimlik sağlayan platformlar, siber teröristler için büyük bir avantaj yaratmaktadır (Zeng 2019).

Nesnelerin İnterneti (IoT) cihazları, fiziksel cihazların internet üzerinden birbirleriyle bağlantı kurmasını sağlayan teknolojilerdir. IoT cihazları, evlerimizdeki akıllı telefonlardan,

otomobillerden, giyilebilir teknolojilere kadar her şeyde kullanılmaktadır. Ancak, bu cihazlar aynı zamanda siber teröristler için büyük bir hedef haline gelmiştir. IoT cihazları, genellikle yeterli güvenlik önlemleriyle korunmaz, bu da onları siber saldırılar için kırılgan hale getirir. Birçok IoT cihazı, zayıf şifreleme ve basit güvenlik protokollerine sahip olduğu için, saldırganlar bu cihazları ele geçirerek botnetler oluşturabilirler. Mirai botnet saldırısı, IoT cihazlarının nasıl kötüye kullanılabileceğini ve büyük ölçekli saldırılara dönüştürülebileceğini gösteren bir örnektir. Bu cihazlar, özellikle kritik altyapılara yönelik saldırılarda, siber teröristler için önemli bir araç haline gelmiştir.

Bulut bilişim, verilerin ve uygulamaların internet üzerinden erişilebilir olmasını sağlayan bir teknolojidir. Bulut bilişim, büyük veri analitiği ve depolama gereksinimlerini karşılamak için yaygın olarak kullanılırken, siber teröristler de bu teknolojiyi hedeflerine ulaşmak için kullanabilirler. Bulut tabanlı hizmetler, saldırganlara, hedeflerin verilerine ulaşmalarını, verileri sızdırmalarını veya bulut ortamlarındaki uygulamaları manipüle etmelerini sağlar. Bu tür saldırılar, genellikle büyük şirketlerin ve devlet kurumlarının dijital altyapılarını hedef alır. Özellikle sanal ortamlar, siber teröristlerin anonim kalmalarına ve izlerini gizlemelerine yardımcı olabilir. Bu teknolojiler, aynı zamanda saldırıların daha geniş alanlara yayılmasını ve etkilerinin büyümesini sağlar (Liu 2020).

Siber Terörizmin Türleri

Siber terörizm, dijital teknolojiler ve bilgisayar sistemleri aracılığıyla yürütülen, toplumun güvenliğini, siyasi istikrarı ve ekonomik düzeni tehdit eden faaliyetleri ifade etmektedir. Plotnek and Slay (2021), siber terörizmin tanımlanmasında altı temel unsur belirlemişlerdir. Bu çerçevede, siber terörizmin başlıca türleri aşağıda söz konusu unsurlar bağlamında ele alınarak değerlendirilmektedir:

Hizmet Reddi (DoS) ve Dağıtılmış Hizmet Reddi (DDoS) Saldırıları

DoS ve DDoS saldırıları, bir sistemin normal işleyişini engellemek amacıyla sunucuya veya ağa aşırı miktarda veri gönderilerek sistemin kaynaklarının tükenmesine neden olan saldırı türleridir. Özellikle DDoS saldırıları, birçok farklı kaynaktan eş zamanlı olarak gerçekleştirildiği için etkisi oldukça büyüktür. Bu saldırılar, kasıtlı ve organize bir biçimde uygulanmakta, çoğu zaman politik veya ideolojik tepkileri dijital ortamda göstermek amacıyla yürütülmektedir.

Toplumsal hizmetleri aksatması nedeniyle psikolojik tehdit içeren bu saldırılar, sivil vatandaşların bankacılık, ulaşım veya iletişim gibi kritik hizmetlerden yararlanmasını engelleyerek korku ve güvensizlik ortamı yaratmaktadır. 2012 yılında ABD bankalarına

yönelik gerçekleştirilen DDoS saldırıları, bu tür faaliyetlerin dijital güvenlik üzerindeki etkisini gözler önüne sermiştir (Goodin 2012).

Ülkemizdeki örneği: 2015 yılında gerçekleştirilen ve bazı kamu kurumlarının web sitelerinin çökertilmesiyle sonuçlanan saldırılar, kamuoyunda büyük endişe yaratmıştır (Euronews 2015; Diken 2015;Anadolu Ajansı 2015).

Kritik Altyapılara Yönelik Saldırılar

Kritik altyapılar, modern toplumların temel işleyişinde hayati rol oynayan enerji, su, sağlık, iletişim ve ulaşım gibi sistemleri kapsamaktadır. Bu altyapıların hedef alınması, sadece teknik değil, aynı zamanda toplumsal, ekonomik ve siyasi sonuçlar doğuran yüksek etkili bir siber terörizm biçimidir.

Bu tür saldırılar, önceden planlanmış ve kasıtlı olarak gerçekleştirilmekte olup, çoğu zaman devletlerarası mesaj verme veya iç siyasal istikrarsızlık yaratma amacı taşımaktadır. Toplumda geniş çaplı panik oluşturma potansiyeli taşımakta, doğrudan sivillerin yaşam kalitesini hedef alarak ulusal güvenliği tehdit etmektedir. Ukrayna'da 2015 yılında elektrik altyapısına yönelik gerçekleştirilen saldırı, binlerce insanın elektriksiz kalmasına ve kamu düzeninin bozulmasına neden olmuştur (Zetter 2015).

Ülkemizdeki örneği: 2020 yılında bazı şehirlerdeki elektrik altyapısına yönelik yapılan dijital sabotaj girişimi, bu tür altyapıların siber tehditlere karşı ne denli kırılgan olduğunu göstermiştir (ELDER E-Bülten 2017).

Veri İhlali ve Bilgi Çalma

Siber terörist gruplar, devletlere, özel şirketlere ya da bireylere ait gizli bilgileri hedef alarak kritik verileri ele geçirmekte ve bu bilgileri ya kamuya sızdırmakta ya da tehdit unsuru olarak kullanmaktadır. Bu eylemler, bilinçli, hedef odaklı ve planlı şekilde yürütülmekte, çoğu zaman politik mesaj verme veya itibarsızlaştırma amacı gütmektedir.

Bilgi ihlalleri; maddi kayıplar, itibar zedelenmesi ve devletlerarası ilişkilerde bozulma gibi sonuçlara neden olmaktadır. Sony Pictures'a 2014 yılında yapılan saldırı, yalnızca ticari sırların değil, aynı zamanda kişisel verilerin de sızdırılmasına yol açarak şirketin itibarını ve ABD ile diğer ülkeler arasındaki diplomatik ilişkileri etkilemiştir (Gallagher 2014).

Ülkemizdeki örneği: FETÖ'nün 2016 öncesi BTK, TİB ve TÜBİTAK gibi kurumlarda dijital izleme ve bilgi sızdırma faaliyetleri, uzun vadeli ve organize bir yapının göstergesidir (Kriter Dergi 2016).

Sosyal Mühendislik ve Kimlik Avı (Phishing) Saldırıları

Sosyal mühendislik saldırıları, bireylerin bilinçli şekilde kandırılması suretiyle bilgi sistemlerine erişim sağlama amacı taşımaktadır. Kimlik avı (phishing), bu yöntemlerin en yaygın biçimlerinden biridir. Bu saldırılar, genellikle sahte e-posta, web siteleri ya da telefon aramaları yoluyla gerçekleştirilmekte, bireylerden kullanıcı adı, şifre gibi hassas verilerin elde edilmesine yönelik planlanmaktadır.

Bu saldırı türü de kasıtlı ve planlıdır, çoğunlukla kamu görevlilerini veya şirket çalışanlarını hedef alarak kritik verilerin sızdırılmasına neden olmuştur. 2017 yılında dünya çapında etkili olan WannaCry fidye yazılımı, kimlik avı ve sosyal mühendislik teknikleriyle yayılmış ve binlerce sistemin işleyemez hale gelmesine yol açmıştır (Shalaby 2017).

Ülkemizdeki örneği: 2023 yılında, Türkiye'de bazı bakanlıkların e-posta sistemlerine yapılan sızma girişimleri, yabancı devlet destekli gruplar tarafından gerçekleştirildiği şüphesiyle incelenmiştir (Uzman Posta 2023).

Siber Propaganda ve Psikolojik Savaş

Siber terörizmin bir diğer boyutu ise psikolojik etki yaratmayı amaçlayan dijital propaganda faaliyetleridir. Terör örgütleri, sosyal medya platformları başta olmak üzere çeşitli dijital mecralar aracılığıyla şiddet içerikli mesajlar, videolar ve ideolojik yayınlar ile geniş kitlelere ulaşmayı hedeflemektedir.

Bu tür saldırılar, özellikle toplumu manipüle etmek, korku yaymak ve siyasi kutuplaşmayı artırmak amacı taşımaktadır. Bu faaliyetlerde doğrudan fiziksel bir saldırı bulunmamakla birlikte, toplumsal düzen üzerinde ciddi bir psikolojik tehdit oluşturmaktadır. IŞİD'in sosyal medya üzerinden yürüttüğü propaganda çalışmaları, bu bağlamda siber terörizmin psikolojik etkilerini açıkça ortaya koymaktadır (Weimann 2016).

Ülkemizdeki örneği: Siber Suçlarla Mücadele Daire Başkanlığı, 2021 yılında tespit edilen birçok uluslararası saldırının kaynağını belirlemede teknik zorluklar yaşandığını raporlamıştır (Emniyet Genel Müdürlüğü 2021).

Bu değerlendirmeler ışığında, siber terörizm yalnızca teknik bir güvenlik meselesi değil; aynı zamanda siyasi, toplumsal ve psikolojik boyutları olan çok katmanlı bir tehdittir. Plotnek and Slay (2021)'ın öne sürdüğü altı temel unsur, siber terörizmi diğer siber saldırı türlerinden ayırmakta ve bu tehditlerin daha doğru bir çerçevede analiz edilmesine olanak sağlamaktadır. Takip eden bölümlerde bu kuramsal çerçevenin ışığında siber terörizmin dünya çapında evrimi, her bir unsura odaklanarak incelenmektedir.

Siber Terörizmin Aktörlerinin Evrimi

Siber terörizmin aktörleri, zamanla teknolojik gelişmeler, dijitalleşmenin yaygınlaşması ve küresel güvenlik ortamındaki dönüşümler doğrultusunda önemli bir evrim geçirmiştir. İlk dönemlerde bireysel düzeyde faaliyet gösteren ve sınırlı teknik kapasiteye sahip aktörler öne çıkarken, ilerleyen süreçte daha organize, donanımlı ve küresel ölçekte etkili olabilen gruplar siber terörizmin başat failleri hâline gelmiştir. Bu evrimsel süreç, aktörlerin niteliksel çeşitliliğini ve etki kapasitelerini artırmış; aynı zamanda, siber terörizmin doğasını daha karmaşık ve çok boyutlu hâle getirmiştir.

Siber terörizmin ilk örneklerinde, bireysel motivasyonlarla hareket eden hackerlar dikkat çekmiştir. Bu aktörler, genellikle ideolojik, siyasi ya da kişisel nedenlerle sınırlı hedeflere yönelik saldırılar gerçekleştirmiştir. Örneğin, 1996 yılında Beyaz Üstünlüğü Hareketi ile ilişkili bir bilgisayar korsanı, Massachusetts'teki bir internet servis sağlayıcısına saldırmış ve bu servis sağlayıcının işleyişini ciddi şekilde sekteye uğratmıştır. Benzer şekilde, 1998 yılında Tamil isyancılarının Sri Lanka büyükelçiliklerini e-posta bombardımanına maruz bırakması ve 1999 Kosova Savaşı sırasında NATO karşıtı bireysel hacktivistlerin düzenlediği NATO'nun internet altyapısını hedef alan hizmet engelleme saldırıları, erken dönem siber terör eylemlerine örnek teşkil etmektedir (Denning 2000).

Zamanla, daha organize ve ideolojik temelli grupların siber alanı bir mücadele zemini olarak kullanmaya başlamasıyla birlikte, siber terörizmin aktör profili değişim göstermiştir. Özellikle 2000'li yıllardan itibaren ortaya çıkan hacktivist gruplar, hem teknik yeterlilik hem de mali kaynaklar bakımından daha gelişmiş aktörler olarak dikkat çekmektedir. GlobalHell adlı grup, devlet kurumlarına ve özel sektör kuruluşlarına yönelik içerik tahrifleri ve veri sızdırma saldırılarıyla büyük maddi zararlara yol açmıştır (Cyber Policy t.y.). Anonymous gibi merkeziyetsiz yapı gösteren hacktivist gruplar ise politik ve sembolik hedeflere yönelik saldırılarıyla küresel ölçekte ses getirmiştir (Coleman 2014). Anonymous'tan ilham alan LulzSec ise özellikle 2011 ve 2012 yıllarında gerçekleştirdiği yüksek profilli saldırılarla kamuoyunun dikkatini çekmiş; CIA ve Sony gibi kurumlara yönelik veri sızdırma eylemleriyle siber terörizm tartışmalarını derinleştirmiştir (Cadwalladr 2012; Gregory 2022; Olson 2012).

Bu sürecin bir diğer önemli evresi, klasik terör örgütlerinin siber uzayı etkin biçimde kullanmaya başlamasıyla şekillenmiştir. Terör örgütleri, propaganda, finansman, planlama, eğitim ve operasyonel faaliyetler için interneti sistemli şekilde kullanarak dijitalleşen terör stratejileri geliştirmiştir. Özellikle Irak ve Şam İslam Devleti (IŞİD), sosyal medya ve iletişim teknolojilerini etkin kullanımıyla siber terörizmin yeni bir boyutunu ortaya koymuştur. IŞİD, çevrim içi propaganda faaliyetleriyle hem yeni militanlar kazanmış hem de bireysel saldırılar

düzenlemeye yönelik çağrılar yapmıştır (Berger and Morgan 2015). Örgüt, bu faaliyetleri yürüten bir yapılanma olarak "İslam Devleti Elektronik Ordusu" adı altında siber terör eylemlerini sistematik hale getirmiştir (Greenberg 2016).

Siber terör örgütlerinin faaliyet alanları, yalnızca propaganda ile sınırlı kalmamış; aynı zamanda finansal kaynak yaratma, dijital eğitim, stratejik iletişim ve eylem planlaması gibi çok yönlü operasyonları da kapsar hale gelmiştir. Kripto paralar aracılığıyla finansman sağlama (örneğin El-Kaide'nin kripto para ile bağış toplaması), çevrim içi eğitim materyalleriyle yeni üyelerin eğitilmesi ve dijital kılavuzlarla silahlı eylemler konusunda teknik bilgi aktarımı gibi unsurlar, bu aktörlerin dijital alandaki etkinliğini artırmıştır (ABD Adalet Bakanlığı 2020; Öğün vd. 2021). IŞİD örneğinde olduğu gibi, propaganda kapasitesini kırmak ve finansal ağlarını çökertmek amacıyla devletler ve uluslararası kuruluşlar karşı kampanyalar geliştirmiştir. DEAŞ'a Karşı Küresel Koalisyon'un bu bağlamda yürüttüğü çalışmalar, siber terörizmin önlenmesinde uluslararası iş birliğinin ve çok paydaşlı mücadele stratejilerinin önemini göstermiştir (Global Coalition 2017; 2019).

Sonuç olarak, siber terörizmin aktör yapısı bireylerden örgütlü ağlara, amatör girişimlerden profesyonel saldırı gruplarına doğru evrilmiş; bu evrim, tehditlerin niteliği ve karmaşıklığı üzerinde belirleyici bir rol oynamıştır. Günümüzde, devlet dışı aktörlerin yanı sıra bazı devletlerin bu tür gruplara dolaylı destek verdiğine dair bulgular da mevcuttur. Bu bağlamda, aktörlerin evrimi, siber terörizmin giderek daha stratejik, çok boyutlu ve küresel ölçekli bir tehdit haline gelmesine neden olmuştur.

Siber Terörizmde Güdü ve Niyetlerin Evrimi

Bu bölüm, ilk siber terörist saldırılardan bu yana siber terörizmin güdü ve niyetlerinin evrim geçirip geçirmediğini sorgulamaktadır. Güdüler ve niyetler birbiriyle bağlantılı olduğundan, bu bölümde her iki unsur birlikte ele alınmaktadır.

Güdülerin bir siber saldırının siber terörizm eylemi olarak nitelendirilebilmesi için önceden planlanmış olması ve ideolojik, politik, dini, ırksal, toplumsal ya da ekonomik saiklerle gerçekleştirilmesi gerekmektedir. İdeolojik ve politik güdüler, başlangıçtan bu yana başlıca itici güçler olarak kabul edilirken; son dönemlerde ekonomik güdüler de bu bağlamda dikkate değer hâle gelmiştir (Plotnek and Slay 2021).

Şimdiye kadar gerçekleşen siber terörist saldırıların incelenmesi, bu alanda bir evrim yaşandığını ortaya koymaktadır. Siber teröristler, ilk yıllardan itibaren ideolojik, politik ve ırksal nedenlerle hareket etmişlerdir. Yukarıda ele alındığı üzere, 1996 yılında

Massachusetts'teki bir internet servis sağlayıcısına (ISP) düzenlenen saldırının ardındaki temel güdü ırkçılık olmuştur.

Benzer şekilde, 2007 yılında Estonya hükümetine yönelik gerçekleştirilen siber terörist saldırıların güdüleri de politik nitelikteydi. Bu saldırılar, siber terörizmin uluslararası ilişkiler ve güvenlik açısından neden kritik bir mesele olduğunu somut biçimde ortaya koymuştur. Estonlar ile ülkedeki Rus azınlık arasındaki uzun süredir devam eden gerilim, saldırıların arka planını oluşturmuştur. Sovyetler Birliği'nin 1940 yılında Baltık ülkelerini ilhak etmesinin ardından, Kremlin tarafından yüz binlerce etnik Rus Estonya'ya gönderilmiştir. Bu büyük ölçekli göç hareketi, Estonya'yı Ruslaştırmayı ve kontrol altına almayı amaçlamıştır. Sovyetler Birliği'nin dağılmasının ardından Estonya hükümeti, ülkedeki Rus etkisini azaltmaya yönelik politikalar benimsemiştir. Bu politikalar arasında, 2007 yılı Nisan ayında Sovyetler Birliği'nin, Estonya'yı Nazilerden kurtarmasını simgeleyen bir anıtın başkent Tallinn'de daha az göz önünde bir konuma taşınması da yer almıştır. Bu nakil kararı, Rus azınlık arasında ayaklanmalara ve eş zamanlı olarak Estonya'nın hayati siyasi ve ekonomik altyapısını hedef alan siber terörist saldırılara yol açmıştır (Herzog 2011).

25 Nisan - 4 Mayıs 2007 tarihleri arasında devlet kurumları, siyasi partiler ve büyük gazetelerin sunucuları hizmet engelleme (denial-of-service) saldırılarına maruz kalmıştır. Bu süreçte basın organları haber akışı sağlayamamış, kamu görevlileri birbirlerine e-posta gönderememiş ve ATM ile çevrim içi bankacılık hizmetleri kesintiye uğramıştır. Estonya hükümetindeki bazı yetkililer, bu siber saldırı sırasında bir NATO üyesine yönelik saldırıya tüm üyeler tarafından ortak şekilde karşılık verilmesini öngören 5. Maddesi'nin işletilmesini talep etmiştir. Ancak saldırılarda can kaybı yaşanmamış olması nedeniyle bu talep karşılık bulmamıştır (McGuinness 2017).

Saldırıdan dolayı Rus kökenli bir Estonyalı öğrenci olan Dmitri Galushkevich suçlu bulunmuş olsa da, saldırının kapsamı, olayda başka kişilerin de muhtemelen yer aldığını göstermektedir. Bu olay, Estonya vatandaşlarının, iş insanlarının ve uluslararası yatırımcıların devlete olan güvenini sarsmıştır. Ancak orta ve uzun vadede, hem Estonya'nın ve diğer Baltık ülkelerinin hem de NATO'nun savunma kapasitesi güçlenmiştir. Bu bağlamda, Estonya Savunma Bakanlığı tarafından ulusal bir siber güvenlik stratejisinin oluşturulması ve 2008 yılında Estonya'nın başkenti Tallinn'de NATO Siber Savunma Mükemmeliyet Ortak Girişim Merkezi'nin kurulması önemli adımlar olmuştur (Aday vd. 2019).

NATO'nun en küçük üyelerinden biri olmasına rağmen Estonya, dünyanın en dijitalleşmiş ülkeleri arasında yer almaktadır. Bankacılıktan eğitime, medya erişiminden yerel seçimlerde oy kullanmaya kadar neredeyse tüm işlemler ülkede çevrim içi olarak

yürütülmektedir. Bu dijital bağımlılık nedeniyle Estonya toplumu, günlük yaşamı aksatabilecek siber saldırılara karşı son derece hassastır. 2007 yılındaki saldırılar çok karmaşık olmamakla birlikte, Estonya küçük bir ülke olduğu için siber güvenlik uzmanları hızla karşı önlemler geliştirebilmiştir. Bu nedenle ülkenin bilişim altyapısı ciddi bir zarar görmemiştir.

Bununla birlikte, söz konusu saldırılar NATO için adeta bir uyarı niteliğinde olmuş; bilgi teknolojileri ağlarına büyük ölçüde bağımlı bir ülkenin siber saldırılarla nasıl ciddi biçimde sarsılabileceğini somut bir şekilde açığa çıkmıştır. Bu durum, NATO üyesi ülkeler için yeni bir tehdit alanını gündeme getirmiştir. Ayrıca, kriz yönetimi ve kolektif savunma gibi NATO'nun temel görevlerinin etkin bir şekilde yürütülebilmesi için hayati önem taşıyan bilgi ağlarının güvenilirliği ve işleyişi açısından da ciddi bir meydan okuma oluşturmuştur (Joubert 2012).

2021 yılında Colonial Pipeline'a yönelik gerçekleştirilen siber saldırı, siber terörizm güdülerinin ekonomik saikleri de kapsayacak şekilde evrildiğini gösteren çarpıcı bir örnektir. Bu saldırı, bir fidye yazılımı (ransomware) saldırısı olup, DarkSide adlı grup, Amerika Birleşik Devletleri'nin Doğu Yakası'na yapılan benzin sevkiyatının kesintiye uğratılmasını sonlandırmak için 5 milyon dolar değerinde Bitcoin ödemesi almıştır. Saldırı kamuoyunda paniğe neden olmuş ve insanlar benzin istasyonlarına akın etmiştir (Eliaçık 2022).

Siber terörizme ilişkin vakaların incelenmesi, niyet boyutunda kayda değer bir evrim yaşanmadığını ortaya koymaktadır. Politik, ideolojik ve toplumsal kazanç elde etme niyeti en başından beri vakalarda çoğu zaman açık biçimde görülmektedir. 2007 yılında Estonya'ya yönelik gerçekleştirilen siber saldırıların temel amacı, Estonya Hükümeti karşısında siyasi avantaj sağlamak olup bu vakada ve diğer siber terörizm vakalarında kaos yaratma ve toplumun devlete olan güvenini zedeleme niyeti, siyasi anlamlar taşımaktadır.

2017 yılında gerçekleştirilen WannaCry fidye yazılımı saldırısı da, Birleşik Krallık Ulusal Sağlık Sistemi'ne (NHS) yönelik güveni sarsma girişimiyle hem siyasi hem de toplumsal niyetler taşıyan bir örnek olarak değerlendirilebilir (Greenberg 2018). Askerî avantaj elde etme niyeti, diğer niyetlere kıyasla daha nadir tespit edilebilmektedir. Bununla birlikte, IŞİD'in sosyal medyayı insan kaynağı temini amacıyla kullanması, teröristlerin askerî avantaj elde etmeye yönelik bir girişimi olarak değerlendirilebilir (Schindler 2020).

Siber Terörizmde Hedefler, Araçlar ve Etkilerin Evrimi

Bu bölümde, siber terörizmin hedeflerinin, araçlarının ve etkilerinin evrimi incelenmektedir. Tartışmanın da daha açık hâle getirdiği üzere, bu üç unsur siber terörizmin birbiriyle yakından ilişkili bileşenleridir ve bu nedenle birlikte ele alınmaktadır.

Öncelikle hedeflerin evrimiyle başlamak gerekirse, siber terörizmin bu unsuru, askerî güçler, hükümete ait siber ve fiziksel altyapılar, kritik ulusal altyapılar, toplumsal ve ulusal kimlik ile özel sektör ya da özel kuruluşları kapsamaktadır (Al Mazari *et al* 2018). Hükümetin siber ve fiziksel altyapılarını, toplumsal ve ulusal kimliği ya da özel sektör ve kuruluşları hedef alan siber terörist saldırılar tespit edilebilmekle birlikte, askerî kapasitelere yönelik saldırılarda fail olarak daha çok devlet aktörlerinin yer aldığı görülmektedir. Moonlight Maze ve Stuxnet saldırıları bu olguyu örneklemektedir.

1998 yılında Pentagon, NASA, araştırma laboratuvarları ve üniversiteler, Moonlight Maze adlı siber casusluk saldırısının hedefi olmuştur. Bu saldırılarda, saldırganlar askerî sistemlere, düzeneklere ve tesislere ilişkin önemli gizli verilere erişmiş ve bu verileri ele geçirmiştir. 2010 tarihli Stuxnet saldırısında ise, İran'ın uranyum zenginleştirme faaliyetleri hedef alınmış ve santrifüjleri tahrip edilmiştir. Her ne kadar bu saldırıların ardındaki aktörler kesin olarak doğrulanmamış olsa da, uzmanlar yalnızca devletlerin bu tür saldırıları tasarlayıp gerçekleştirme kapasitesine sahip olabileceği sonucuna varmıştır (Haizler 2017). Bu nedenle, Moonlight Maze ve Stuxnet saldırılarını siber terörizm örnekleri olarak değil, siber savaş vakaları olarak değerlendirmek daha doğru olacaktır.

Teknolojik gelişmelerin devlet dışı aktörlerin de siber terörist saldırılar gerçekleştirmesini mümkün kılmasıyla birlikte, bu aktörlerin hedefleri çoğunlukla hükümetlerin siber ve fiziksel altyapıları olmuştur. Bu tür saldırılar, ulusal güvenlik ve kamu güvenliği açısından ciddi sonuçlar doğurmuştur. 2007 yılında Estonya'daki devlet kurumlarına yönelik gerçekleştirilen siber saldırılar, kritik ulusal altyapıların siber tehditlere karşı ne denli savunmasız olduğunu gözler önüne sermiş ve güçlü bir siber güvenlik sisteminin gerekliliğini ortaya koymuştur.

Benzer şekilde, 2015 yılında ABD Personel Yönetim Ofisi'ne (Office of Personnel Management – OPM) düzenlenen siber saldırı, siber terörizmin gizli ve kişisel bilgilere ulaşma ve devlet operasyonlarını sekteye uğratma potansiyelini ortaya koymuştur. Bu saldırıda, bilgisayar korsanları, milyonlarca federal çalışanın kişisel bilgilerini (sosyal güvenlik numaraları, parmak izleri ve güvenlik soruşturması kayıtları da dâhil olmak üzere) ele geçirmiştir (Fruhlinger 2020).

Son yıllarda ise sivilleri doğrudan hedef alan saldırılar artış göstermiştir. 2017 yılında gerçekleştirilen WannaCry fidye yazılımı saldırısı bu duruma örnek teşkil etmektedir. Bu saldırı, İngiltere'deki hastaneler ve ambulans hizmetlerini hedef alarak sağlık hizmetlerinde ciddi aksamalara yol açmıştır. Fidye yazılımı, bulaştığı bilgisayarlardaki verileri şifrelemiş ve sistemlerin kullanılmasını imkânsız hâle getirmiştir; sistemin yeniden kullanılabilir olması ise

fidye ödenmesine bağlanmıştır. Saldırı sonucunda tıbbi randevular iptal edilmiş, ameliyatlar ertelenmiş ve sağlık hizmetleri genel anlamda ciddi bir tehditle karşı karşıya kalmıştır. Bu durum, siber terörizmin fiziksel zarara yol açma ve kamu sağlığını tehdit etme potansiyelini açıkça ortaya koymuştur (Ghafur *et al* 2019).

Teknolojinin gelişmeye devam etmesiyle birlikte, siber terörizm hedeflerinin daha da çeşitlenmesi ve karmaşık hâle gelmesi muhtemeldir. Dijital altyapıya olan bağımlılığın artması ve Nesnelerin İnterneti'nin (Internet of Things – IoT) yükselişi, siber teröristler için yeni fırsatlar sunmaktadır. Akıllı şehirler, otonom araçlar ve kişisel cihazlar, gelecekte potansiyel hedefler arasında yer alabilir.

Siber terörizmin unsurlarından bir başkası olan araçların evrimi ise oldukça belirgindir. İlk yıllarda, siber teröristler ağları bozmak ve yasa dışı erişim sağlamak için virüsler ve solucanlar gibi basit araçlar kullanmışlardır (Maryville University 2022). Zamanla, siber teröristler fidye yazılımı (ransomware) ve casus yazılım (spyware) gibi daha gelişmiş kötü amaçlı yazılım türlerine yönelmişlerdir (Montasari 2024). Ayrıca, oltalama (phishing) kampanyaları, sosyal mühendislik yöntemleri, DDoS saldırıları, botnetlerin kullanımı ve yapay zekâ gibi daha sofistike araçlar da siber teröristlerin kullandığı yöntemler arasına girmiştir (Montasari 2024).

Son unsur olan siber terörizmin etkilerinin evriminde ise korku yaratma ve sistemleri aksatma etkisinin en başından beri var olduğu söylenebilir. 1996 yılında Massachusetts'teki bir internet servis sağlayıcısını (ISP) hedef alan ve Beyaz Üstünlük Hareketi ile bağlantılı olan hacker, siber terörizmin gelecekte nasıl zarar verebileceği konusunda uyarıda bulunmuş; bu şekilde korku yaratmıştır. IŞİD'in "ölüm listelerini" yayımladığı videolar (Jayakumar 2020) ya da insanları canlı canlı yaktığını gösteren görüntüler (Ayad and Zerrouky 2023) aracılığıyla korku salması, bu etkinin günümüzde de süreklilik gösterdiğini ortaya koymaktadır.

Sistemsel aksatma da benzer şekilde kalıcı bir etki olmuştur. Kosova Savaşı sırasında Sırp hackerların temel amacı, Yugoslavya Federal Cumhuriyeti'ne yönelik NATO bombardımanını sekteye uğratmaktı (Verton 1999). NATO, Associated Press ve Washington Post'a yönelik e-posta bombardımanları, NATO'nun hava saldırılarını durdurmayı hedeflemiş; bu saldırı aynı zamanda siber terörizmin niyet boyutunun politika değişikliklerini zorla sağlamaya doğru evrildiğini göstermiştir (Denning 2001).

Siber terörist eylemlerin etkilerinin çeşitlenmesi, teknolojik gelişmelerle paralel olarak hız kazanmıştır. Bu bağlamda, sosyal medya, siber teröristlerin çeşitli amaçlarını gerçekleştirmeleri için yoğun olarak kullandıkları bir araç hâline gelmiştir. IŞİD'in sosyal medyayı propaganda ve eleman temini amacıyla kullanması buna örnektir (Awan 2017).

Bir diğer siber terörizm etkisi ise sistemlere müdahaledir. Bu etkinin evrimi incelendiğinde, teknolojik ilerlemelerle birlikte siber terörizmin bu yöndeki etkisinin git gide daha korkutucu bir boyuta ulaştığı görülmektedir. 2021 yılında yaşanan bir olay, bu tür etkilerin ne kadar tehlikeli olabileceğini gözler önüne sermektedir. Bu vakada, bir hacker uzaktan erişim yazılımı aracılığıyla Florida'daki bir su arıtma tesisine sızarak içme suyuna karıştırılan sodyum hidroksit miktarını neredeyse 100 katına çıkarmıştır. Sistem operatörü müdahaleyi kısa sürede fark ederek seviyeyi normale döndürse de, bu olay bazı kritik altyapı sistemlerinin müdahaleye ne kadar açık olduğunu göstermektedir (Marquardt 2021).

Teknoloji gelişmeye devam ettikçe, siber terörizmin etkilerinin daha da ağırlaşması muhtemeldir. Dijital altyapıya olan artan bağımlılık ve Nesnelerin İnterneti'nin (IoT) yaygınlaşması, siber teröristler için yeni fırsatlar yaratmaktadır. Gelecekteki saldırılar, akıllı şehirleri, otonom araçları ve kişisel cihazları hedef alabilir; bu da yaygın ölçekte aksamalara ve korkuya yol açabilir. Takip eden bölüm, geçirdiği evrim sonucu daha tehlikeli bir hale gelen siber terörizme karşı verilen mücadelenin evrimini incelemektedir.

Siber Terörizm ile Ulusal ve Uluslararası Mücadelenin Evrimi

Siber terörizmin zamanla daha karmaşık, yıkıcı ve küresel etkiler doğurabilecek bir tehdit haline gelmesi, yalnızca teknik değil; aynı zamanda hukuki, politik ve askeri düzeyde kapsamlı önlemler alınmasını zorunlu kılmıştır. Bu bağlamda, hem uluslararası toplumun hem de devletlerin bu tehdide yönelik yaklaşımları, teknolojinin gelişimine ve tehditlerin niteliğine paralel olarak evrim geçirmiştir.

Siber tehditlerin yeni yeni ortaya çıktığı bu dönemde, devletler ve uluslararası kuruluşlar henüz siber terörizmi ayrı bir kategori olarak tanımlamaktan uzaktı. Siber saldırılar genellikle bilişim suçları ya da siber vandallık olarak ele alınıyordu. 1990'lar ve 2000'lerde uluslararası düzeyde belirgin bir hukukî çerçeve oluşmamıştı. 2001 yılındaki Budapeşte Konvansiyonu (Siber Suçlar Sözleşmesi), ilk defa siber suçlarla mücadelede ortak bir hukuki zemin oluşturmaya yönelik önemli bir adım olmuş; dolaylı olarak siber terörizme karşı da bir temel teşkil etmiştir. Yine de bu yıllarda devletlerin önceliği, bireysel saldırılardan kaynaklı güvenlik açıklarını kapatmak üzerineydi.

2010'lu yıllarda siber terörizmin hem teknik kapasitesi hem de etkileri artmaya başlayınca, birçok ülke ulusal siber güvenlik stratejileri geliştirmiştir. Bu stratejilerde siber terörizm doğrudan bir tehdit olarak tanımlanmaya başlanmış, siber olaylara müdahale ekipleri (CERT/CSIRT) kurulmuş ve siber savunma doktrinleri geliştirilmiştir.

Aynı dönemde NATO, 2014 Galler Zirvesi'nde siber uzayı resmi olarak beşinci operasyon alanı (kara, deniz, hava, uzay, siber) ilan etmiş; bu karar, siber saldırılara kolektif savunma kapsamında (NATO'nun 5. maddesi) yanıt verilebileceği yönünde bir dönüm noktası olmuştur.

2020 sonrası dönemde ise siber terörizmin ulaştığı düzey devletleri çok taraflı işbirliği ile dijital egemenlik arasında denge kurmaya zorlamıştır. Bir yandan Birleşmiş Milletler ve INTERPOL gibi kuruluşlar siber teröre karşı bilgi paylaşımı ve ortak operasyonlar düzenlerken, diğer yandan bazı ülkeler kendi ulusal internet altyapılarını kurma eğilimi göstermiştir. Örneğin, Çin, "siber egemenlik" vurgusu yapmaya başlamıştır. Bu dönemde, Avrupa Birliği, Ağ ve Bilgi Sistemlerinin Güvenliği (NIS) Direktifini yürürlüğe koymuş; ABD'nin 2023 yılındaki Ulusal Siber Güvenlik Stratejisi de dikkat çeken başka bir gelişme olmuştur. Rusya, İran, Kuzey Kore gibi devletlerin ise siber alandaki hibrit tehditlerinin artması öne çıkan gelişmeler arasında yer almıştır.

Aynı zamanda uluslararası hukukta siber saldırılara nasıl yanıt verileceği, hangi durumların "savaş nedeni" sayılabileceği gibi konular tartışılmaya başlanmıştır.

Uluslararası İş Birliği ve Önlemler

Siber terörizm, uluslararası sınırları aşan bir tehdit oluşturduğundan, bu tehdide karşı etkili bir mücadele için küresel ölçekte işbirliği gereklidir. Devletler, özel sektör ve uluslararası organizasyonlar arasında güçlü bir işbirliği, siber güvenlik alanında daha güçlü savunmalar geliştirilmesi ve saldırılara karşı hızlı bir yanıt verilmesi için kritik öneme sahiptir. Ancak, uluslararası işbirliği genellikle hukuk, etik ve teknik zorluklar nedeniyle karmaşık olabilir. Bununla birlikte, siber terörizmle mücadelede uluslararası işbirliği, sadece saldırılara karşı korunmakla kalmayıp, aynı zamanda suçluların adalet önüne çıkarılmasında da önemli bir rol oynamaktadır.

Siber terörizmin önlenmesi için birincil engellerden biri, mevcut uluslararası hukukun siber saldırıları ve terörizmi ne ölçüde kapsayabildiğidir. Siber suçların çoğu, uluslararası sınırları aşan doğası nedeniyle karmaşık hukuki sorunlar yaratmaktadır. Birçok ülke, siber saldırıları terörizmle ilişkilendirerek buna karşı önlemler almaya başlamıştır, ancak uluslararası hukuki normların eksikliği, bu konuda ortak bir çerçevenin oluşmasını engellemektedir. Birçok ülke, siber suçlar ve siber terörizm konusunda işbirliği yapmak adına Budapeşte Konvansiyonu (2001) gibi anlaşmalara imza atmış olsa da, bu anlaşmaların çoğu, yalnızca devletler arası bilgi paylaşımını ve suçluların iadesini kapsayarak, daha derin bir işbirliği yapmayı zorlaştırmaktadır (Brenner 2010). Bununla birlikte, uluslararası hukukta yapılacak reformlar, özellikle siber

suçların tanımını genişleterek, devletler arasında siber terörizmle mücadelede daha güçlü bir işbirliği ortamı yaratabilir.

Siber terörizmin tarihsel gelişimi, dijital teknolojilerin hızla ilerlemesi ve internetin küresel ölçekte yaygınlaşmasıyla paralel bir şekilde evrilmiştir. İlk başlarda bilgisayar suçları ve siber saldırılar yalnızca bireysel ya da küçük ölçekli motivasyonlarla gerçekleştirilirken, zaman içinde bu eylemler daha organize, hedeflenmiş ve stratejik hale gelmiştir. Siber terörizmin evrimini anlamak için, internetin ve bilgisayar teknolojilerinin nasıl şekillendiğine, bunların terörist gruplar tarafından nasıl kullanıldığını ve devletler ile güvenlik organizasyonlarının bu tehditlere nasıl yanıt verdiğine bakmak önemlidir.

Birleşmiş Milletler (BM), siber güvenliği artırmak için dünya çapında çeşitli inisiyatifler başlatmıştır. 2009'da, BM, siber güvenlik alanında daha güçlü bir uluslararası işbirliği için bir siber güvenlik stratejisi geliştirmeyi önerdi. BM Genel Kurulu, siber saldırıların uluslararası barışı tehdit etme potansiyelini kabul ederek, siber saldırılara karşı uluslararası işbirliğini teşvik etmiştir. Ayrıca, 2015 yılında BM, devletlerin siber güvenlik stratejilerini güçlendirmeleri için bir *Uluslararası Siber Güvenlik Yönergesi* yayınlamıştır. Bu yönergeler, üye devletlerin, siber güvenlik tehditlerine karşı daha iyi hazırlıklı olmalarını sağlamayı hedeflemektedir. BM ayrıca, devletler arasında bilgi paylaşımını artırmak ve uluslararası çapta siber güvenlik normlarını oluşturmak için çeşitli konferanslar düzenlemektedir (United Nations 2015).

Avrupa Birliği (AB), siber terörizmle mücadele konusunda büyük bir adım atmıştır ve bu alanda etkin işbirliği mekanizmaları geliştirmiştir. AB, Siber Güvenlik Yasası (2016) gibi düzenlemeler ile üyelerine güçlü bir siber savunma sağlamak için çeşitli önlemler almıştır. AB, siber güvenlik konusunda yalnızca üye ülkeler arasında değil, aynı zamanda üçüncü ülkelerle de işbirliği yapmaktadır. 2017 yılında, AB, EU Cybersecurity Act'ı kabul ederek, Avrupa'da ortak bir siber güvenlik çerçevesi oluşturmuştur. Bu yasalar, AB üye ülkelerinin siber saldırılara karşı daha dayanıklı hale gelmelerini ve siber tehditlere karşı ortak bir yaklaşım benimsemelerini sağlamaktadır. Ayrıca, AB'nin bir diğer önemli girişimi, ENISA (Avrupa Siber Güvenlik Ajansı), siber güvenlik konusunda Avrupa çapında bilgi paylaşımını teşvik etmekte ve acil durumlarda üye devletlerin koordinasyonunu sağlamaktadır (ENISA 2020).

NATO, siber güvenliği, kolektif savunmanın ayrılmaz bir parçası olarak kabul etmektedir. 2016 yılında NATO, siber saldırıları "Müteakip Savunma" (5. Madde) kapsamında değerlendirebileceğini duyurmuştur. Bu, NATO'nun bir üye ülkesine yapılan siber saldırının tüm ittifakın güvenliğini tehdit edebileceği anlamına gelmektedir. NATO, siber tehditlere karşı işbirliği geliştirmek için üye ülkeler arasında ortak eğitimler ve tatbikatlar düzenlemekte, böylece siber saldırılara karşı kolektif savunmayı güçlendirmektedir. NATO, aynı zamanda,

siber terörizmle mücadelede diğer uluslararası organizasyonlarla ve devletlerle de işbirliği yapmaktadır. Bunun yanı sıra, NATO'nun Siber Savunma Merkezi (CCDCOE), siber güvenlik konusunda bilgi paylaşımını ve devletler arası işbirliğini artırmak için küresel bir platform sunmaktadır (NATO 2018).

Siber güvenlik sadece devletlerin sorumluluğunda değildir; özel sektör, küresel çapta siber güvenlik ve siber terörizme karşı mücadelede kritik bir rol oynamaktadır. Özellikle teknoloji şirketleri, internet altyapısını sağlayan firmalar ve finansal kurumlar, küresel siber güvenlik ağlarının önemli unsurlarıdır. Kamu-özel sektör işbirliği, siber saldırılara karşı daha hızlı ve etkili yanıt verilmesini sağlayabilir. Bu işbirliği, siber tehditlerin erken tespit edilmesini ve bunlara karşı daha sağlam önlemler alınmasını mümkün kılmaktadır. Örneğin, ABD'deki CISA (Siber Güvenlik ve Altyapı Güvenliği Ajansı), özel sektörden şirketlerle işbirliği yaparak, siber saldırılara karşı dayanıklılığı artırmaktadır. Bununla birlikte, uluslararası şirketler arasındaki bilgi paylaşımı da siber terörizmle mücadelede önemli bir faktör olmaktadır (Hathaway 2014).

MATERYAL VE METOT

Bu tezde, Türkiye'ye yönelen siber terörizm tehditlerinin nasıl evrildiği vaka çalışması yöntemi kullanılarak analiz edilmiştir. Bu bağlamda, Plotnek and Slay (2021) tarafından geliştirilen kuramsal çerçeve kullanılarak söz konusu tehditlerin aktörlerinin, güdülerinin, niyetlerinin, kullandıkları araçların, yarattıkları etkilerin ve hedeflerinin zaman içerisinde nasıl evrildiği analiz edilmiştir. Bu kuramsal yaklaşım ve yöntem, Türkiye bağlamında siber terörizmin çok boyutlu yapısının sistematik bir şekilde incelenmesine olanak sağlamıştır. Ayrıca, söz konusu kuramsal çerçeve, Türkiye'de vaka çalışması yöntemiyle daha önce uygulanmadığı için sunulan tez çalışması özgünlük kazanmış ve literatürdeki önemli bir boşluğu doldurmuş kanaatindeyiz.

Bu tez çalışması, siber terörizm konusundaki mevcut literatürü kapsamlı bir şekilde analiz etmek ve Türkiye'nin bu tehdit türüne yönelik stratejik yaklaşımlarını değerlendirmek amacıyla yürütülmüştür. Araştırmanın temelini, döküman analizi yöntemi oluşturmaktadır. Döküman analizi, yazılı materyallerin sistematik bir şekilde incelenmesi ve yorumlanması yoluyla elde edilen bilgilerin bir araya getirilmesini sağlayan nitel bir araştırma yöntemidir. Bu bağlamda, çalışma kapsamında birçok farklı kaynaktan elde edilen bilgiler değerlendirilmiştir.

Bu tez çalışmasında kullanılan materyaller, ulusal ve uluslararası düzeyde yayımlanmış akademik çalışmalar, resmi raporlar ve çevrimiçi kaynaklardan oluşmaktadır. Türkiye'deki akademik tezlerin merkezi olan YÖK Tez Merkezi, siber güvenlik ve siber terörizm konularında yapılan lisansüstü çalışmaların incelenmesinde önemli bir kaynak olarak kullanılmıştır. Bu tezler, Türkiye'nin siber terörizmle mücadelede karşılaştığı zorluklar ve önerilen çözüm yolları hakkında kapsamlı bilgiler sunmaktadır. Ayrıca, Türkiye'de yayımlanan hakemli dergilerin toplandığı DergiPark, siber tehditler, ulusal güvenlik politikaları ve uluslararası işbirlikleri konularındaki akademik makalelerin incelenmesinde temel kaynaklardan biri olmuştur. Bu platformdan elde edilen makaleler, siber terörizmin çeşitli boyutlarını anlamada önemli bir referans noktasıdır.

Uluslararası literatürü incelemek amacıyla, Google Akademik ve uluslararası akademik dergilerde yayımlanmış makaleler taranmıştır. Bu kaynaklar, siber terörizmin küresel boyutunu ve diğer ülkelerin bu tehdit türüne karşı geliştirdiği stratejileri anlamak açısından değerli bilgiler sunmuştur. Özellikle, NATO ve Avrupa Birliği gibi uluslararası kuruluşların yayımladığı raporlar, uluslararası işbirliklerinin siber terörizme karşı mücadeledeki önemini vurgulamaktadır. Bunun yanı sıra, siber güvenlik alanındaki en güncel gelişmeleri ve teknolojik

yenilikleri anlamak için çevrimiçi platformlar ve akademik veri tabanları da incelenmiştir. Resmi raporlar ve politika belgeleri de bu çalışmanın önemli bir başvuru kaynağını oluşturmuştur. Türkiye Cumhuriyeti İçişleri Bakanlığı'nın yayımladığı 2019 yılımda Türkiye'de Siber Güvenlik ve Terörizm Raporu, ülkemizin bu alandaki mevcut durumu ve alınan önlemler hakkında kapsamlı bir perspektif sunmaktadır. Ayrıca, Türkiye Siber Güvenlik Kümelenmesi ve NATO Siber Savunma Mükemmeliyet Merkezi tarafından yayımlanan belgeler, siber tehditlerin ulusal ve uluslararası düzeyde ele alınmasına yönelik önemli veriler sağlamaktadır.

Bu dökümanların sistematik bir şekilde analiz edilmesiyle, siber terörizmin tanımı, kullanılan teknikler, ulusal güvenlik üzerindeki etkileri ve Türkiye'nin bu tehditlere karşı geliştirdiği stratejiler derinlemesine incelenmiştir. Döküman analizi yöntemi, geniş bir literatür havuzundan bilgi toplanmasına olanak sağlamakla kalmamış, aynı zamanda bu bilgilerin bağlamsal olarak değerlendirilmesine de imkan tanımıştır. Böylece, siber terörizm konusunda kapsamlı bir bilgi birikimi sunulması hedeflenmiştir. Bu kaynaklardan elde edilen bilgilerin Türkiye'ye vaka çalışması yöntemiyle uygulanması yoluyla elde edilen bulgular bir sonraki bölümde tartışılmaktadır.

BULGULAR

Siber terörizm, dijital çağın getirdiği en karmaşık ve dinamik tehditlerden biri olarak karşımıza çıkmaktadır. Bu tehdit, özellikle dijital altyapıların hızla geliştiği ve internet kullanımının yaygınlaştığı ülkelerde daha belirgin bir hale gelmiştir. Türkiye, hem jeopolitik konumu hem de stratejik önemi nedeniyle siber terörizmin hedef ülkelerinden biri olarak öne çıkmaktadır. Ülkemizde kritik altyapılara yönelik saldırılar, bilgi manipülasyonu ve ekonomik sistemlere zarar verme girişimleri gibi siber terörizm unsurları çeşitli şekillerde kendini göstermektedir. Türkiye'nin bu tehditlere karşı geliştirdiği hukuki düzenlemeler, teknolojik önlemler ve uluslararası işbirlikleri, siber güvenlik stratejilerinin temelini oluşturmaktadır. Bu bölümde,çalışmanın kuramsal temelleri vaka çalışması yöntemiyle Türkiye'nin karşılaştığı siber terörist tehditlere uygulanarak bulgular elde edilmiştir. Bölümün geri kalanında bu bulgular tartışılmaktadır.

Türkiye'ye Yönelik Siber Terörizmde Evrim: Aktörler, Güdüler, Niyetler, Hedefler, Araçlar ve Etkiler

Aktörlerin Evrimi

Türkiye'ye yönelik siber terörizm faaliyetlerinde rol alan aktörlerin zaman içerisinde hem niceliksel hem de niteliksel bir dönüşüm geçirdiği bulgusuna ulaşılmıştır.. 2000'li yılların başlarında, ideolojik saiklerle hareket eden ve teknik kapasitelerini sembolik mesaj iletimi amacıyla kullanan bireysel aktörler ve hacktivist gruplar ön plandayken; 2010'lu yıllardan itibaren bu aktörlerin yerlerini daha kurumsal bir yapıya sahip, hiyerarşik örgütlenmiş ve siyasi hedefleri olan, doğrudan silahlı terör örgütleriyle bağlantılı dijital hücrelerin aldığı görülmüştür. Bu yapısal değişim, siber terörizm tehdidinin Türkiye bağlamında yalnızca politik değil, aynı zamanda operasyonel ve stratejik boyutta da karmaşıklaştığını ortaya koymaktadır.

PKK, DHKP-C ve FETÖ gibi örgütlerin dijital alanda yürüttüğü faaliyetler, aktörler arası çeşitliliği önemli ölçüde artırmış; bu örgütlerin çevrim içi platformlara entegrasyonu, siber terör spektrumunun genişlemesine neden olmuştur. 2020'li yıllarla birlikte, devlet destekli siber kapasiteye sahip yapılar ile vekil aktörlerin (proxy actors) dijital alanda daha görünür hale geldiği; ayrıca, organize siber suç grupları ile siber terörizm yapılanmaları arasındaki sınırların muğlaklaştığı hibrit tehdit biçimlerinin ortaya çıktığı tespit edilmiştir. Bu durum, Türkiye'de siber güvenlik mimarisinin yalnızca konvansiyonel güvenlik paradigması çerçevesinde kurgulanamayacağını, çok katmanlı ve disiplinler arası bir tehdit analizine ihtiyaç duyulduğunu göstermektedir.

Türkiye örneğinde gözlemlenen dönüşüm, küresel ölçekteki siber tehdit dinamikleriyle yüksek düzeyde örtüşmektedir. Dünya genelinde siber terör aktörlerinin bireysel odaklı yapılardan kolektif örgütlenmelere, ardından devlet destekli profesyonel yapılara evrilmesi yaygın bir model oluştururken; Türkiye özelinde bu sürecin, özellikle bölgesel silahlı örgütlerin dijitalleşme kapasitesindeki artış nedeniyle daha hızlı ve agresif bir biçimde yaşandığı dikkate değerdir. Bu özgünlük, Türkiye'nin karşı karşıya olduğu siber terörizm tehdidinin yalnızca küresel dinamiklerin değil, aynı zamanda bölgesel jeopolitik gerilimlerin de bir yansıması olduğunu göstermektedir.

Güdülerin ve Niyetlerin Evrimi

Türkiye'de siber terörist aktörlerin güdü ve niyetleri zamana bağlı olarak yapısal bir dönüşüm geçirdiği bulgusuna ulaşılmıştır. Başlangıç aşamasında gerçekleştirilen eylemler, düşük teknik karmaşıklığa sahip, ideolojik motivasyonlu ve sembolik hedeflere yönelmiş saldırılar şeklinde ortaya çıkmıştır. Bu tür eylemler, özellikle devletin temsili kurumlarına yönelik gerçekleştirilmiş; hedef, kamuoyunun dikkatini belirli bir söylem veya ideolojik yapıya çekmek olmuştur.

Zamanla dijital altyapının yaygınlaşması ve kamu hizmetlerinin büyük oranda sayısallaşması, siber saldırıların teknik kapasitesini ve stratejik derinliğini artırmıştır. Bu dönemde eylemler, sistematik planlamaya dayalı, belirli hedeflere yönelik ve daha yıkıcı sonuçlar doğurabilecek şekilde evrilmiştir. Özellikle kamu kurumlarının dijital altyapılarına yönelik gerçekleştirilen yetkisiz erişim girişimleri, hizmet dışı bırakma (DoS/DDoS), zararlı yazılım (malware) dağıtımı ve veri sızıntıları bu dönüşümün başlıca örnekleri arasında yer almıştır. Eylemlerin temel hedefi; kamu kurumlarının işleyişini sekteye uğratmak, kritik verilerin güvenliğini ihlal etmek ve kamuoyunda bilgi sistemlerine yönelik güveni sarsmak olmuştur.

Son dönemde güdüler çok boyutlu bir hâl almış ve sadece ideolojik temelli eylemlerin ötesine geçmiştir. Ekonomik çıkar sağlama, siyasal baskı oluşturma ve toplumsal psikoloji üzerinde yönlendirici etki yaratma gibi amaçlar ön plana çıkmıştır. Bu çerçevede; siber manipülasyon, bilişsel harp teknikleri, sosyal medya üzerinden yürütülen dezenformasyon kampanyaları ve algı operasyonları gibi yöntemler kullanılarak toplumsal kutuplaşma ve bilgi kirliliği artırılmaktadır. Türkiye'de gözlemlenen bu evrimsel süreç, küresel düzeydeki siber terörizm pratikleriyle büyük ölçüde benzerlik göstermektedir.

Hedeflerin Evrimi

Türkiye'de siber terörizm bağlamında hedef alınan yapılar, zaman içerisinde hem işlevsel hem de stratejik açıdan dönüşüm geçirdiği bulgusu elde edilmiştir. Başlangıçta, sembolik değeri yüksek ve dijital güvenlik seviyesi nispeten düşük olan kamu kurumlarının web siteleri öncelikli hedefler arasında yer almıştır. Bu tür platformlar, hem kamuoyunda görünürlük sağlama açısından elverişli hem de teknik olarak kolay erişilebilir olmaları nedeniyle tercih edilmiştir.

2010'lu yıllardan itibaren hedef yapısında gözle görülür bir değişim yaşanmış; güvenlik birimleri, siyasi partiler, medya organları ve bürokratik sistemlere ait dijital altyapılar saldırıların odak noktasına yerleşmiştir. Bu aşamada hedef seçiminde yalnızca sembolik değil, aynı zamanda operasyonel etkisi yüksek olan kurumlara yönelim söz konusu olmuştur.

2020'li yıllarla birlikte saldırıların yöneldiği alanlar daha da genişlemiş ve enerji, ulaştırma, sağlık ile finans gibi ulusal düzeyde kritik kabul edilen altyapı sistemleri hedef önceliği kazanmıştır. Bu sistemlerin, ülke güvenliği ve toplumsal işleyiş açısından taşıdığı yaşamsal önem, onları siber terör eylemleri açısından stratejik hale getirmiştir.

Bu yönelim, küresel düzlemde siber tehditlerin hedef yapısındaki evrimle benzerlik arz etmektedir. Ancak Türkiye özelinde dikkate değer bir farklılık, saldırıların büyük ölçüde iç güvenlik dengeleriyle ilişkilendirilmesidir. Bu durum, siber terör eylemlerinin yalnızca teknik ya da stratejik saiklerle değil, aynı zamanda mevcut siyasal konjonktürün ve güvenlik dinamiklerinin dijital ortama yansıması şeklinde biçimlendiğini göstermektedir. Hedef seçiminin bu çok katmanlı yapısı, Türkiye'de siber tehditlerin değerlendirilmesinde yalnızca teknolojik değil, toplumsal ve politik parametrelerin de dikkate alınmasını gerektirmektedir

Kullanılan Araçların Evrimi

Siber terörizm kapsamında kullanılan araç ve yöntemler, bilgi ve iletişim teknolojilerinin gelişimine koşut biçimde niteliksel bir dönüşüm geçirmiştir. Başlangıç evresinde çoğunlukla düşük teknik karmaşıklığa sahip, yüksek erişilebilirlik düzeyinde olan saldırı tipleri öne çıkmıştır. Bu dönemde dağıtılmış hizmet engelleme (DDoS) saldırıları, web sitelerinin tahrif edilmesi (defacement) ve elektronik posta yoluyla gerçekleştirilen tehdit iletimleri temel yöntemler arasında yer almıştır. Ancak dijital altyapıların yaygınlaşması ve karmaşıklığının artmasıyla birlikte, siber terör faaliyetlerinde kullanılan araçlar da daha sofistike ve hedef odaklı hale gelmiştir.

Zararlı yazılım türleri (malware), fidye yazılımları (ransomware), casus yazılımlar (spyware) ve sosyal mühendislik tabanlı sızma yöntemleri, bu evrimin sonraki aşamasında öne

çıkan araçlardır. Bu yazılımlar, yalnızca sistemlerin işlevselliğini bozmakla kalmayıp, aynı zamanda hassas verilerin ele geçirilmesi, şifrelenmesi ve maddi kazanç ya da psikolojik baskı unsuru olarak kullanılması gibi çok katmanlı etkiler yaratmaktadır. Bu süreçte, saldırganların teknik yeterlilikleriyle birlikte, operasyonel planlama ve hedef analizi kabiliyetlerinde de belirgin bir artış gözlemlenmiştir.

Günümüzde ise yapay zekâ destekli saldırı vektörleri, otomatikleştirilmiş karar alma sistemlerine yönelik manipülasyon girişimleri, deepfake teknolojisi aracılığıyla üretilen sahte içerikler ve sosyal medya platformlarının algoritmik yapısının istismarı yoluyla yürütülen dezenformasyon kampanyaları dikkat çekmektedir. Bunlara ek olarak, özellikle ulusal güvenlik açısından kritik kabul edilen altyapılara yönelik olarak geliştirilen ve uzun süre tespit edilemeden sistemlerde varlık gösteren gelişmiş kalıcı tehditler (Advanced Persistent Threats – APT), siber terörizm araçlarının geldiği boyutu açık biçimde ortaya koymaktadır.

Bu araçların geçirdiği evrim, uluslararası siber güvenlik literatüründeki yapısal eğilimlerle büyük ölçüde örtüşmektedir. Türkiye özelinde değerlendirildiğinde ise, söz konusu araç ve yöntemlerin ülkenin enerji, ulaştırma, sağlık ve iletişim gibi hayati sektörlerini hedef aldığı ve bölgesel jeopolitik konumun bu tür tehditleri daha da yoğunlaştırdığı gözlemlenmektedir. Dolayısıyla, siber terörist eylemlerde kullanılan araçların teknik çeşitliliği ve etkisinin artması, hem tehdit tespiti hem de müdahale süreçlerinin daha sofistike hale getirilmesini zorunlu kılmaktadır.

Etkilerin Evrimi

Türkiye'de siber terörizm eylemlerinin etkileri zaman içinde belirgin bir dönüşüm geçirmiştir (Tablo 1). İlk dönemlerde bu eylemler, daha çok sembolik hedeflere yönelmiş ve kamuoyunda geçici bir tedirginlik yaratmakla sınırlı kalmıştır. Psikolojik etki ön planda olmuş, medya üzerinden yayılan mesajlarla kamuoyu algısı hedeflenmiş, ancak bu tür girişimlerin yapısal ya da operasyonel düzeyde ciddi bir sonuç doğurduğu söylenemez.

Zamanla dijitalleşmenin hız kazanması, devlet kurumlarının ve kritik altyapıların dijital sistemlere daha fazla entegre olmasıyla birlikte, bu tür saldırıların etkisi de farklı bir boyut kazanmıştır. Özellikle 2010 sonrasında, kamu hizmetlerinde yaşanan kesintiler, veri güvenliğine yönelik tehditler ve kurumsal işleyişin sekteye uğraması gibi durumlar, siber terörizmin doğrudan işlevsel sonuçlar doğurabildiğini göstermiştir. Bu süreçte, sadece sistemlere değil, aynı zamanda güvenlik algısına ve toplumsal huzura yönelik bir baskı da ortaya çıkmıştır.

Günümüzde ise siber terörizm artık çok katmanlı bir tehdit biçimine evrilmiştir. Kritik altyapılara yapılan saldırılar ekonomik kayıplara neden olmakta, bilgi manipülasyonu yoluyla kamuoyu yönlendirilmekte ve mevcut toplumsal kutuplaşma ortamı bu tür tehditlerin etkisini daha da artırmaktadır. Türkiye özelinde düşünüldüğünde, siyasal gerilimlerin ve dijital mecralardaki kırılganlıkların bu saldırıların etkisini büyüttüğü, toplumda güvensizlik ve istikrarsızlık hissini derinleştirdiği görülmektedir. Bu bağlamda siber terörizm, artık sadece anlık bir güvenlik problemi değil; uzun vadeli, yapısal ve stratejik sonuçlar doğuran bir tehdit alanı hâline gelmiştir.

Tablo 1. Türkiye'de Siber Terörizm Vakaları

Yıl	Aktör	Güdü	Niyet	Araç	Etkiler	Hedef
2015	Hacktivist grup (Anonymous)	Siyasi protesto / Türkiye'ye karşı siber savaş	Kamu hizmetlerini aksatmak ve tepki oluşturmak	DDoS saldırıları	.tr uzantılı sitelere erişim kesildi	DNS altyapısı / kamu ve bankalar
2016	Hacktivist grup (RedHack)	Siyasi ifşa / yolsuzluk ifşası	Kamuoyu yaratmak ve siyasi baskı kurmak	Veri sızıntısı (hack + sızdırma)	57 bin e-posta ve belge sızdırıldı	Bakan e-posta hesapları
2017	Devlet destekli grup (Kuzey Kore bağlantılı Lazarus - olası)	Finansal kazanç ve istihbarat toplama	Zararlı yazılım ile yayılma ve veri rehin alma	Fidye yazılımı (WannaCry)	Binlerce bilgisayar kilitlendi	Kamu ve özel sektör bilgisayar sistemleri
2018	APT (spekülatif)	Finansal ve stratejik bilgi elde etme	Finansal sistemlere sızma ve istihbarat toplama	İleri seviye kalıcı tehdit (APT)	Finansal verilerin sızdırıldığı iddia edildi	Merkez Bankası sistemleri
2019	Hacktivist grup (Anonymous)	Politik motivasyon / kamuoyu etkisi	Bankacılık altyapısını sekteye uğratmak	DDoS	Bankalarda hizmet kesintisi yaşandı	Bankacılık ve telekom altyapısı
2020	(muhtemelen organize bireysel saldırganlar)	Hizmet kesintisi yaratma / test amaçlı saldırılar	Devlet hizmetlerini kesintiye uğratmak	DDoS ve Web hizmet kesintisi	E-devlet hizmetlerinde erişim aksadı	Devlet kurumları web siteleri
2021	(muhtemelen bireysel saldırganlar)	Veri hırsızlığı / kişisel çıkar	Sağlık verilerine ulaşmak / satmak	Yetkisiz erişim ve veri sızdırma	Sağlık verileri tehlikeye girdi	Sağlık Bakanlığı sistemleri
2022	APT (İran bağlantılı MuddyWater)	Devlet istihbaratı toplama	Kritik altyapıdan istihbarat elde etmek	Kimlik avı ve zararlı yazılım	Kurumsal bilgiler dışarı sızdırıldı	Kamu kurumları ve telekom altyapısı
2023	(Çin veya Rusya bağlantılı APT iddiası)	Kapsamlı veri toplama / istihbarat	Devletin tüm vatandaşlık verilerine ulaşmak	Veri tabanı sızdırma	85 milyon vatandaşın verisi ifşa oldu	E-Devlet altyapısı
2024	(muhtemelen fidye amaçlı bireysel grup)	Finansal kazanç	Sağlık verilerini rehin alıp fidye istemek	Fidye yazılımı	Radyolojik veriler tamamen silindi	Hastane bilgi sistemleri
2025	(siber suç grubu olasılığı yüksek)	Kişisel veri hırsızlığı / finansal çıkar	Müşteri bilgilerini çalmak ve satmak	Veri ihlali araçları (muhtemelen içerden sızdırma)	Kişisel bilgiler sızdırıldı	İnternet servis sağlayıcısı altyapısı

2015–2025 Arası Türkiye'de Gerçekleşen Önemli Siber Saldırılar: Bir Siber Terörizm Perspektifi

Son on yıl içerisinde Türkiye, küresel çapta artan siber güvenlik tehditlerinden ciddi biçimde etkilenmiş; kamu kurumları, altyapı sistemleri, finansal kuruluşlar ve sağlık sektörü gibi kritik alanlara yönelik çok sayıda siber saldırıya maruz kalmıştır. Bu saldırıların bir kısmı, sadece teknik ya da ekonomik zararlarla sınırlı kalmamış, aynı zamanda devlet otoritesini ve kamu güvenliğini hedef alarak siber terörizm kapsamında değerlendirilmiştir.

Anonymous'un 2015 yılında .tr DNS Altyapısına Saldırısı

2015 yılında uluslararası hacker grubu Anonymous tarafından gerçekleştirilen Dağıtık Hizmet Kesintisi (DDoS) saldırısı, Türkiye'nin NIC.tr altyapısını hedef almış ve .tr uzantılı web sitelerine erişimi tamamen engellemiştir. Bu saldırı sonucunda kamu kurumları, bankalar ve özel sektör ciddi kesintiler yaşamış, kamu hizmetlerinin dijital erişimi sekteye uğramıştır. Anonymous, saldırıyı Türkiye'nin internet üzerindeki faaliyetlerine karşı bir "siber savaş" ilanı olarak duyurmuştur. Bu eylem, politik bir amaç doğrultusunda yapılan ve ulusal altyapıyı hedef alan bir saldırı olması nedeniyle siber terörizm tanımına yaklaşmaktadır.

2016 RedHack Saldırısı ve Enerji Bakanı'nın e-postalarının Sızdırılması

2016 yılında sol eğilimli siber aktivist grup RedHack, dönemin Enerji Bakanının e-posta hesaplarını ele geçirerek 57 binin üzerinde e-postayı sızdırmış ve Wikileaks aracılığıyla kamuoyuna sunmuştur. Saldırı, hem siyasi hem de psikolojik etkiler yaratmış, hükümet üyelerine yönelik ciddi bir itibar zedelenmesine neden olmuştur. Saldırının bilgi sızdırma ve kamuoyunu yönlendirme amacı taşıması, onu klasik bir hacktivizm örneğinden çıkarıp siber terör eylemi olarak değerlendirmeye açık hale getirmektedir.

2017 WannaCry Fidye Yazılımı Saldırısı

2017 yılında dünya genelinde etkili olan WannaCry adlı fidye yazılımı, Türkiye'de kamu ve özel sektördeki binlerce bilgisayarı etkisiz hale getirmiştir. Bu saldırı, üretim tesislerinin durmasına ve ekonomik kayıplara yol açmıştır. Türkiye, etkilenen ülkeler arasında üst sıralarda yer almıştır. Saldırı her ne kadar doğrudan bir siyasi motivasyona dayanmasa da, geniş çaplı etkisi nedeniyle ulusal güvenlik kapsamında değerlendirilmiştir.

2023 e-Devlet Veri Sızıntısı

2023 yılında, Türkiye Cumhuriyeti vatandaşlarına ait yaklaşık 85 milyon kişinin kişisel verilerinin sızdırılmasıyla sonuçlanan saldırı, Cumhuriyet tarihinin en büyük veri ihlali olarak kayıtlara geçmiştir. Bu olayda e-Devlet altyapısı hedef alınmış; ad, soyad, adres, T.C. kimlik numarası gibi kritik bilgiler karaborsada satışa çıkarılmıştır. Saldırı, bireysel gizlilik ve kamu

güvenliği açısından büyük bir tehdit oluşturmuş, siber terörizm bağlamında ele alınması gereken bir vaka niteliği kazanmıştır.

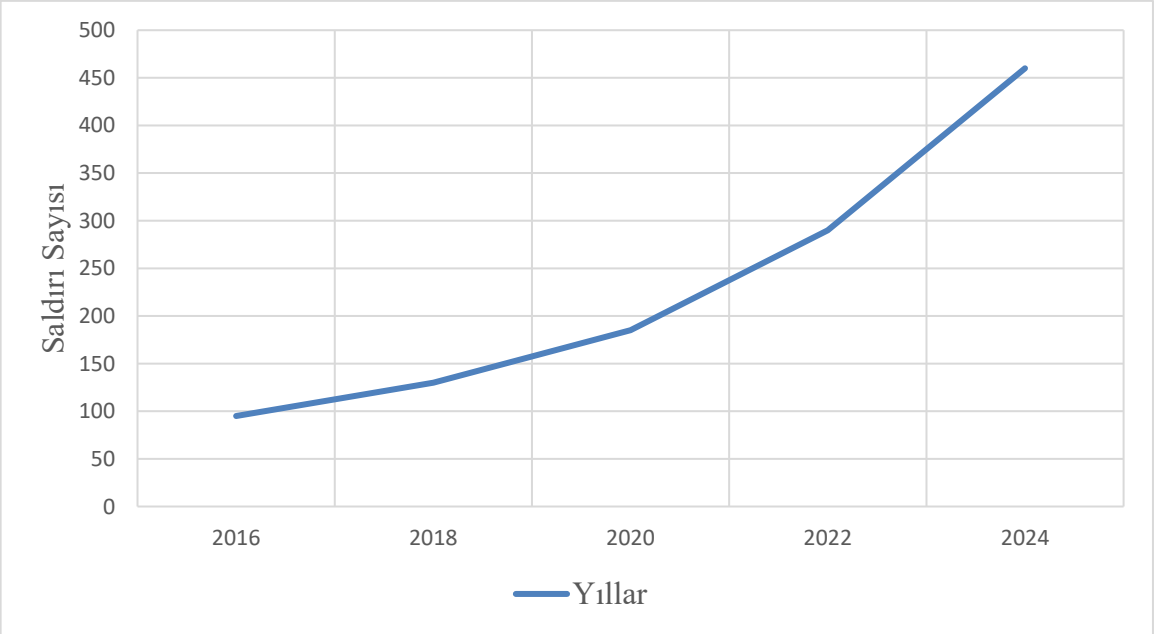
Sağlık ve Telekom Sektörüne Yönelik Diğer Saldırılar

2021 yılında Sağlık Bakanlığı bilgi sistemlerine yönelik yetkisiz erişim girişimi, sağlık verilerinin güvenliği açısından tehlike yaratmıştır. 2024'te ise Bağcılar Eğitim ve Araştırma Hastanesi'nin tüm radyolojik görüntü arşivi fidye yazılımı sonucu kaybolmuş, yedekleme yapılmadığı için veri kaybı kalıcı olmuştur. 2025'te TurkNet'in kullanıcı verileri sızdırılmış, kişisel verilerin korunması ve ilgili mevzuat yeniden gündeme gelmiştir. Bu saldırıların çoğu, bireysel hak ve özgürlükler kadar ulusal dijital egemenliğe de tehdit oluşturur niteliktedir.

2015–2025 yılları arasında Türkiye'ye yönelik siber saldırılar, hem teknik hem de stratejik düzeyde çok boyutlu tehditler doğurmuştur. Bazı saldırılar doğrudan devlet otoritesini hedef almış; kamu düzenini, siyasi aktörleri ya da kritik altyapıları hedefleyerek siber terörizm tanımına yaklaşmıştır. Türkiye'nin bu süreçte geliştirdiği ulusal siber güvenlik stratejileri, saldırılara karşı koyma kapasitesini artırsa da; özellikle kamu-özel iş birliğinin, toplumsal farkındalığın ve mevzuatın sürekli olarak güncellenmesi gerektiği açıktır.

Enerji Altyapılarına Yönelik Saldırılar

Enerji altyapılarına yönelik siber saldırılar, son yıllarda artan dijitalleşme ve otomasyon sistemlerinin yaygınlaşmasıyla birlikte kritik bir güvenlik tehdidi haline gelmiştir. Bu tür saldırılar, elektrik, doğal gaz, petrol ve yenilenebilir enerji gibi sistemleri hedef alabilir ve hem ekonomik hem de ulusal güvenlik açısından ciddi sonuçlar doğurabilir.



Şekil 1. Türkiye'de enerji altyapılarına yönelik siber saldırı sayıları

Şekil 1’de, 2015 ile 2024 yılları arasında Türkiye’de enerji altyapılarına yönelik gerçekleşen siber saldırıların yıllık sayısal dağılımını göstermektedir. Şekil 1 incelendiğinde, bu dönemde siber saldırı sayısında düzenli ve dikkat çekici bir artış gözlemlenmektedir.

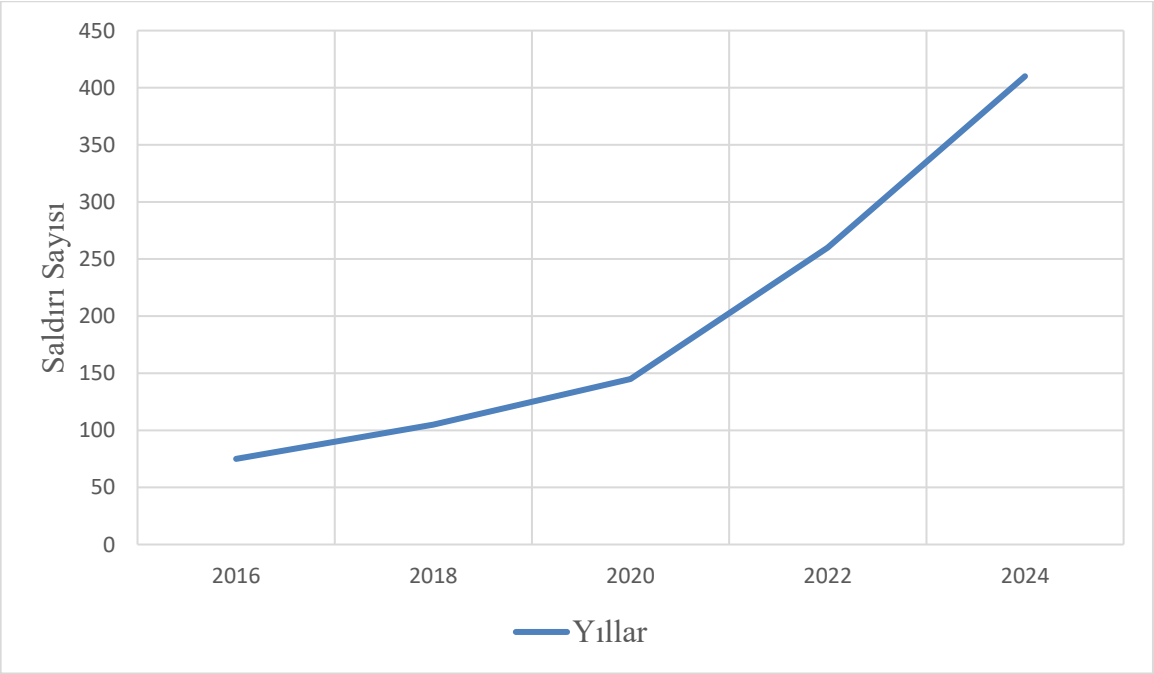
2015 yılında 80 civarında olan saldırı sayısı, her yıl artarak 2024 yılı itibarıyla 460 seviyesine ulaşmıştır. Bu veriler, Türkiye'de özellikle kritik altyapılar arasında yer alan enerji sektörünün siber tehditler karşısında giderek daha fazla hedef haline geldiğini ortaya koymaktadır. 2021 yılına kadar nispeten kademeli bir artış yaşanırken, 2021 sonrası dönemde (özellikle 2022–2024 arası) saldırı sayılarında belirgin bir sıçrama görülmektedir. Örneğin, 2021 yılında yaklaşık 210 olan saldırı sayısı, 2023'te 400’ün üzerine çıkmış, 2024’te ise 460’a ulaşarak Şekil 1’de ki en yüksek değeri temsil etmiştir. Bu hızlı artış, dijitalleşmenin enerji altyapılarında daha yaygın hale gelmesiyle birlikte risklerin de çeşitlendiğine işaret etmektedir.

Bu bağlamda değerlendirildiğinde, enerji sektörüne yönelik siber saldırılar yalnızca ekonomik ve teknik bir sorun olmanın ötesinde, ulusal güvenlik perspektifinden ele alınması gereken bir tehdit alanıdır. Özellikle siber terörizm bağlamında, enerji altyapılarına yöneltilen saldırılar; toplumda panik yaratma, ekonomik zarar verme ve kamu otoritesini zayıflatma gibi stratejik hedeflerle ilişkilendirilebilir. Bu durum, Türkiye’nin enerji güvenliği stratejileri içinde siber güvenliğin merkezi bir konumda ele alınmasını gerektirmektedir.

Nitekim, Ulusal Siber Güvenlik Strateji Belgeleri ve Enerji ve Tabii Kaynaklar Bakanlığı’nın yayımladığı raporlar, enerji altyapılarının siber tehditlere karşı korunmasının öncelikli politika alanlarından biri haline geldiğini göstermektedir. Bununla birlikte, artan saldırı sayıları, yalnızca teknik savunma önlemlerinin yeterli olmayacağını, aynı zamanda yasal, kurumsal ve uluslararası iş birliğini içeren çok katmanlı bir yaklaşımın benimsenmesi gerektiğini ortaya koymaktadır.

Sağlık Altyapılarına Yönelik Saldırılar

Son yıllarda dijitalleşme ile birlikte sağlık sektörünün siber tehditlere karşı daha savunmasız hale geldiği gözlemlenmektedir. Özellikle kritik altyapıların hedef alınması, sadece bilgi güvenliğini tehdit etmekle kalmamakta, aynı zamanda kamu sağlığını da riske atmaktadır. Türkiye özelinde yapılan analizler, bu durumun giderek ciddi bir boyut kazandığını ortaya koymaktadır.



Şekil 2. Türkiye'de sağlık altyapılarına yönelik siber saldırı sayıları

Şekil 2, 2016–2024 yılları arasında Türkiye'de sağlık altyapılarına yönelik gerçekleştirilen siber saldırıların sayısındaki değişimi göstermektedir. Verilere göre, 2016 yılında oldukça sınırlı sayıda olan saldırı vakaları, izleyen yıllarda ciddi bir artış sergilemiştir. 2020 yılı itibarıyla saldırı sayısında dikkat çekici bir sıçrama gözlenmekte olup, bu artış eğilimi 2024 yılına kadar sürmektedir. Özellikle COVID-19 pandemisinin etkili olduğu 2020 sonrası dönemde, sağlık sistemlerinin dijitalleşmesinin hız kazanması, siber saldırganlar için yeni fırsat alanları yaratmıştır.

Bu artışın temel nedenleri arasında sağlık altyapılarının yetersiz siber güvenlik önlemleri ile korunması, kişisel sağlık verilerinin yüksek ticari ve istihbari değer taşıması ve sağlık hizmetlerinin sürekliliğinin kamu güvenliği açısından kritik olması gösterilebilir. Nitekim, saldırganlar açısından sağlık sistemlerini hedef almak, aynı zamanda kamuoyunda korku ve panik yaratma amacı da taşıyabilir. Bu yönüyle bu tür eylemler, siber suç kapsamında değerlendirildiği gibi, siber terörizm boyutuna da ulaşabilmektedir.

Birleşmiş Milletler'e göre siber terörizm, "siyasi ya da ideolojik amaçlarla korku yaratmak için bilgi teknolojileri kullanılarak gerçekleştirilen şiddet eylemleri" olarak tanımlanmakta olup, sağlık sistemlerine yönelik saldırılar da bu tanım kapsamında değerlendirilebilecek nitelikler taşıyabilir. Türkiye'de özellikle kamu hastanelerinin dijital altyapılarına yönelik fidye yazılımı (ransomware) saldırıları, bu kapsamdaki en güncel örnekler arasında yer almaktadır.

Bu veriler ışığında, Türkiye'nin sağlık sektörünü hedef alan siber saldırılara karşı daha bütüncül ve ulusal çapta bir siber güvenlik stratejisi geliştirmesi gerektiği açıktır. Aksi takdirde bu tür saldırılar yalnızca bireysel mahremiyetin ihlaline değil, aynı zamanda ulusal güvenliğin tehdit edilmesine de yol açabilir.

Türkiye'nin Siber Güvenlik Politikasının Evrimi

Siber güvenlik, dijitalleşmenin küresel ölçekte hız kazanmasıyla birlikte yalnızca teknik bir mesele olmaktan çıkarak, ulusal güvenlik, ekonomik istikrar ve toplumsal düzen açısından stratejik bir öncelik haline gelmiştir. Türkiye de bu dönüşüm sürecinde siber güvenliği, başlangıçta bireysel ve sektörel ölçeklerde ele alırken, zamanla devletin kurumsal politikalarına entegre edilen, çok boyutlu bir güvenlik alanı olarak değerlendirmeye başlamıştır.

Türkiye'de siber güvenliğe yönelik ilk sistematik adımlar, 2000'li yılların başlarında, bilgi teknolojilerinin hızlı yayılımı ve internet kullanımının artmasıyla birlikte atılmıştır. Bu dönemde siber güvenlik, daha çok özel sektör kuruluşlarının kendi altyapılarını koruma çabalarıyla sınırlı kalmıştır. Ancak internetin yaygınlaşmasıyla beraber dijital tehditler, kamu otoritelerinin de dikkatini çekmiş; 2004 yılında Bilgi Teknolojileri ve İletişim Kurumu (BTK) öncülüğünde, internet tabanlı siber saldırılara karşı ilk kurumsal tedbirlerin planlanmasına yönelik çalışmalar başlatılmıştır. Aynı dönemde çeşitli kamu kurumları ve özel sektör aktörleri, kendi iç güvenlik mekanizmalarını oluşturarak siber tehditlere karşı teknik altyapılarını güçlendirme yoluna gitmişlerdir.

2010'lu yıllar, Türkiye'nin siber güvenliği stratejik düzeyde bir devlet politikası olarak ele almaya başladığı bir döneme işaret etmektedir. Bu süreçte kurumlar arası koordinasyon ön plana çıkmış, siber güvenlik alanındaki politikalar bütüncül bir yaklaşımla oluşturulmaya başlanmıştır. 2013 yılında yayımlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, Türkiye'nin siber güvenliğe yönelik ilk ulusal ölçekli politika belgesi olmuş; bu strateji ile siber güvenliğin teknik bir sorun olmanın ötesinde, ulusal güvenliği doğrudan ilgilendiren bir mesele olduğu vurgulanmıştır. Bu belgeyle birlikte, kamu, özel sektör, akademi ve sivil toplum aktörlerinin katılımıyla geliştirilen siber güvenlik politikalarının kurumsallaşması hedeflenmiştir.

Bu stratejik açılım, Türkiye'nin uluslararası düzeyde de siber güvenlik alanında iş birliğini artırmasına zemin hazırlamıştır. Avrupa Birliği, NATO ve Birleşmiş Milletler gibi uluslararası kuruluşlarla siber güvenlik alanında yürütülen iş birlikleri, Türkiye'nin uluslararası güvenlik mimarisi içindeki konumunu güçlendirmiştir. Özellikle 2016 yılında Türkiye'nin

NATO Siber Savunma Kooperasyon Merkezi'ne (CCDCOE) katılımı, uluslararası düzeyde kolektif siber savunma perspektifine entegre olma kararlılığının bir göstergesi olmuştur.

2020'li yıllara gelindiğinde Türkiye, siber güvenlik politikasını daha geniş çaplı bir dijital dönüşüm stratejisinin temel bir bileşeni olarak konumlandırmıştır. 2020 yılında Cumhurbaşkanlığına bağlı olarak kurulan Dijital Dönüşüm Ofisi, hem kamu bilişim altyapılarının modernizasyonu hem de bu altyapıların siber tehditlere karşı korunması amacıyla çeşitli strateji belgeleri ve eylem planları hazırlamıştır. Aynı yıl yayımlanan Ulusal Siber Güvenlik Stratejisi ve 2020–2023 Eylem Planı, kritik altyapıların korunması, siber farkındalık eğitimlerinin yaygınlaştırılması, siber güvenlik ekosisteminin yerli ve milli yazılımlarla desteklenmesi gibi konuları öncelikli hedefler arasında belirlemiştir.

Bu stratejiler çerçevesinde Türkiye, siber güvenlik alanında yerli yazılım ve teknolojilerin geliştirilmesini stratejik bir öncelik olarak ele alınırken; özellikle kritik altyapılarda dışa bağımlılığı azaltmak amacıyla siber güvenlikte teknolojik bağımsızlık vizyonunu benimsemiştir. Bu yaklaşım, hem ulusal güvenliğin sağlanması hem de siber terörizm gibi asimetrik tehditlere karşı dayanıklılığın artırılması açısından kritik bir rol oynamaktadır.

Öte yandan Türkiye, siber güvenlik politikalarının yalnızca ulusal güvenlik odaklı değil, aynı zamanda uluslararası norm ve iş birlikleri ile uyumlu olmasına da önem vermektedir. Bu bağlamda, Avrupa Birliği'nin siber güvenlik düzenlemeleri, NATO'nun kolektif savunma perspektifi ve BM'nin dijital güvenlik ilkeleri çerçevesinde çok taraflı iş birlikleri sürdürülmektedir. Türkiye, ayrıca bölgesel ölçekte siber suçlarla mücadele ve siber terörizmle ilgili deneyim paylaşımı gibi konularda da aktif rol üstlenmektedir.

Sonuç olarak, Türkiye'nin siber güvenlik politikaları, ilk yıllarda sınırlı ölçekli tedbirlerle şekillenirken, günümüzde kurumsallaşmış, çok aktörlü, stratejik düzeyde ve uluslararası entegrasyona açık bir yapıya dönüşmüştür. Bu dönüşüm, yalnızca dijital altyapıların korunması açısından değil, aynı zamanda siber terörizm gibi yeni nesil tehditlerin önlenmesi ve yönetilmesi bakımından da kritik bir öneme sahiptir. Türkiye'nin siber güvenlik alanındaki bu çok katmanlı stratejisi, ulusal güvenliğin sürdürülebilirliğini sağlamakla kalmayıp, küresel düzeyde dijital güvenliğin inşasında da etkin bir rol üstlenmesini sağlamaktadır.

Türkiye'nin Uluslararası İlişkileri Bağlamında Siber Terörizm

Siber terörizm, uluslararası sınırları aşan karmaşık ve çok boyutlu bir tehdit niteliği taşıdığından, bu tehditle etkin mücadele, yalnızca ulusal düzeyde alınacak önlemlerle sınırlı

kalamaz. Bu bağlamda, devletler, uluslararası kuruluşlar ve özel sektör aktörleri arasında çok katmanlı ve sürekli bir iş birliği gerekmektedir. Siber güvenlik alanındaki uluslararası iş birliği, sadece savunma kapasitelerinin güçlendirilmesi açısından değil, aynı zamanda siber terör saldırılarının faillerinin tespiti, adalet önüne çıkarılması ve caydırıcılık sağlanması bakımından da kritik öneme sahiptir.

Bununla birlikte, uluslararası düzlemde iş birliğinin sağlanması; teknik, hukuki ve etik birçok engel nedeniyle çoğu zaman karmaşık bir yapı arz etmektedir. Siber suçların ve özellikle siber terör eylemlerinin, ulusal sınırları aşan doğası; yargı yetkisi, suçun tanımı, delil toplama ve adli süreçlerde büyük zorluklar yaratmaktadır. Mevcut uluslararası hukuk düzeni, siber terörizmi açık biçimde tanımlamakta yetersiz kalmakta ve bu durum, devletler arasında ortak bir normlar rejimi oluşturulmasını zorlaştırmaktadır.

Uluslararası Hukuki Çerçeve ve İş Birliği Mekanizmaları

Siber suçlara ve dolayısıyla siber terörizme karşı geliştirilen en önemli uluslararası hukuki düzenlemelerden biri Budapeşte Siber Suçlar Sözleşmesi'dir (2001). Türkiye'nin de taraf olduğu bu sözleşme, özellikle uluslararası bilgi paylaşımı, adli yardımlaşma ve suçluların iadesi gibi alanlarda temel bir çerçeve sunmaktadır. Ancak söz konusu sözleşmenin kapsamı, çoğu zaman siber terörizmin çok boyutlu doğasını karşılamakta yetersiz kalmakta; özellikle devlet destekli saldırılar, kritik altyapılara yönelik tehditler ve ideolojik amaç güden dijital sabotajlar açısından eksiklikler barındırmaktadır.

Birleşmiş Milletler (BM), siber güvenlik konusunda küresel iş birliğini geliştirmeyi hedefleyen çeşitli inisiyatifler geliştirmiştir. 2009 yılında BM Genel Kurulu tarafından siber güvenliğin uluslararası barış ve güvenliğe etkisi vurgulanarak, bu alanda devletlerarası eşgüdümün artırılması gerektiği dile getirilmiştir. 2015 yılında yayımlanan Uluslararası Siber Güvenlik Yönergesi, üye devletlere siber tehditlere karşı ulusal stratejiler oluşturma ve uluslararası normları benimseme çağrısında bulunmuştur.

Bölgesel Yapılanmalar: AB ve NATO Örnekleri

Avrupa Birliği (AB), siber güvenlik ve siber terörizmle mücadelede etkili mekanizmalar geliştirmiştir. AB'nin Siber Güvenlik Yasası (2016) ve EU Cybersecurity Act (2019) gibi düzenlemeleri, üye ülkeler arasında ortak bir güvenlik protokolü oluşturmayı hedeflemekte; üçüncü ülkelerle de iş birliği zemini sunmaktadır. Ayrıca, Avrupa Siber Güvenlik Ajansı (ENISA), siber tehditlere karşı erken uyarı sistemleri, bilgi paylaşımı ve kriz yönetimi açısından önemli bir rol oynamaktadır.

NATO ise, siber tehditleri kolektif savunma anlayışı içinde değerlendiren bir yaklaşım benimsemiştir. 2016 yılında yapılan açıklama ile siber saldırıların Washington Antlaşması'nın 5. Maddesi (Ortak Savunma İlkesi) kapsamında değerlendirilebileceği ilan edilmiştir. Bu gelişme, siber saldırıların bir üye devlete yapılması halinde, tüm ittifak üyelerinin kolektif savunma mekanizmasını devreye sokabileceği anlamına gelmektedir. NATO'nun CCDCOE (Cooperative Cyber Defence Centre of Excellence) adlı kurumu ise siber güvenlik konusunda teknik eğitimler, senaryo tatbikatları ve uluslararası bilgi paylaşımı açısından önemli bir platform sunmaktadır.

Özel Sektörün ve Kamu-Özel İş Birliğinin Rolü

Siber güvenliğin yalnızca devletlerin inisiyatifine bırakılması yeterli değildir; özel sektör, özellikle teknoloji şirketleri, telekomünikasyon firmaları ve finansal kurumlar, dijital altyapının temel taşıdır. Bu nedenle, kamu-özel sektör iş birliği, siber terörizmle mücadelede stratejik bir gereklilik haline gelmiştir. ABD'deki CISA (Cybersecurity and Infrastructure Security Agency) gibi örnekler, özel sektör ile doğrudan iş birliği kurarak ulusal güvenliğe katkı sağlayan bir model ortaya koymaktadır.

Uluslararası düzeyde faaliyet gösteren teknoloji firmalarının tehdit istihbaratlarını paylaşması, saldırıların daha erken tespit edilmesi ve etkili müdahale sağlanması açısından büyük öneme sahiptir. Ayrıca, bu firmaların geliştirdiği siber güvenlik standartları, ülkelerarası teknik uyumluluk açısından da kritik bir role sahiptir.

Türkiye'nin Uluslararası İş Birliği Politikası

Türkiye, siber güvenlik alanında uluslararası iş birliğine önem veren ülkeler arasında yer almaktadır. Budapeşte Sözleşmesi'ne 2014 yılında taraf olan Türkiye, uluslararası hukuk ve teknik iş birliği mekanizmalarına dâhil olmuştur. Ayrıca, NATO üyesi olarak, İttifak'ın siber güvenlik stratejilerine aktif biçimde katkı sunmakta ve NATO tatbikatlarında düzenli olarak yer almaktadır. Türkiye, ayrıca AB ile yürüttüğü Gümrük Birliği çerçevesinde dijital güvenlik alanında teknik uyum süreçlerini sürdürmektedir. Ancak, Türkiye'nin uluslararası siber güvenlik iş birliklerini derinleştirmesi, sadece yasal katılım değil, aynı zamanda teknik kapasitenin artırılması ve özel sektörle koordinasyonun güçlendirilmesi ile mümkündür. Bu noktada, Türkiye'nin siber güvenlik alanında faaliyet gösteren kurumlarının (örneğin USOM ve SOME'ler) uluslararası ağlara entegre olması ve küresel tehdit istihbarat zincirine katkı sunması büyük önem arz etmektedir.

Siber terörizmle etkin mücadele, ulusal kapasitelerin ötesine geçen küresel bir yaklaşımı gerektirmektedir. Uluslararası hukukun geliştirilmesi, ortak normların oluşturulması ve iş

birliği mekanizmalarının güçlendirilmesi, bu alandaki temel ihtiyaçlar arasında yer almaktadır. Türkiye'nin, siber güvenlik politikalarını uluslararası standartlara uygun biçimde geliştirmesi ve çok taraflı platformlarda daha aktif rol üstlenmesi, hem ulusal güvenlik hem de bölgesel istikrar açısından stratejik bir zorunluluktur. Konuya ilişikin hukuki düzenlemeler ve mevzuat Tablo 2'de verilmiştir.

Tablo 2. Hukuki Düzenlemeler ve Mevzuat

Yıl	Düzenleme/Mevzuat	Kapsam	Amaç	Notlar
2007	Türk Ceza Kanunu (TCK) 243, 244 ve 245. Maddeleri	Bilişim sistemlerine yetkisiz erişim, sistemlerin bozulması, veri hırsızlığı ve dolandırıcılık	Siber suçların tanımlanması ve cezai yaptırımların uygulanması	Siber suçlar için temel yasal çerçeve
2007	Budapeşte Siber Suçlar Sözleşmesi	Uluslararası iş birliği ve siber suçlarla mücadele	Sınır ötesi siber suçlarla ilgili koordinasyonun sağlanması	Türkiye'nin imzaladığı önemli bir uluslararası sözleşme
2007	5651 Sayılı Kanun	İnternet yayınlarının düzenlenmesi ve suç içeriklerinin kontrolü	Çevrimiçi içerik kontrolü, bireysel hakların korunması	Sosyal medya ve internet içeriği düzenlemelerinde sıkça başvurulan kanun
2016	Ulusal Siber Güvenlik Stratejisi ve Eylem Planı	Kamu kurumları ve özel sektörü kapsayan kapsamlı bir strateji	Kritik altyapıların korunması, siber güvenlik kapasitesinin artırılması	Kamu-özel sektör iş birliğini teşvik eden bir eylem planı
2019	Türkiye'de Siber Güvenlik ve Terörizm Raporu (İçişleri Bakanlığı)	Siber tehditlere karşı ulusal politikalar	Siber güvenlik önlemlerinin belirlenmesi, siber terörizmle mücadelede izlenecek politikaların tanımı	Ulusal güvenlik için yol gösterici bir rapor
2020	Kişisel Verilerin Korunması Kanunu (KVKK)	Bireylerin kişisel verilerinin korunması	Bireysel hakların korunması, veri güvenliği ve mahremiyetin sağlanması	Veri güvenliği ve mahremiyeti ön planda tutan güncel bir düzenleme
2024	Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028)	Siber dayanıklılık, proaktif siber savunma ve caydırıcılık, insan odaklı siber güvenlik yaklaşımı	Türkiye'nin siber güvenlik alanındaki stratejik hedeflerinin ve eylem planlarının belirlenmesi	7 Eylül 2024 tarihli 32655 sayılı Resmi Gazete'de yayımlanan 2024/11 sayılı Genelge ile yürürlüğe girmiştir.
2025	7545 Sayılı Siber Güvenlik Kanunu	Kamu kurumları, özel sektör ve bireyleri kapsayan geniş bir düzenleme	Ulusal siber güvenliği güçlendirmek, siber tehditlere karşı korunma sağlamak	19 Mart 2025 tarihli Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Siber Güvenlik Başkanlığı'nın kurulması gibi yenilikler içermektedir.

Siber terörizm, dijital teknolojilerin sağladığı olanaklar çerçevesinde gelişen ve klasik terörizm biçimlerinden farklı dinamiklere sahip olan karmaşık bir tehdit türü olarak değerlendirilmektedir. Plotnek and Slay (2021) tarafından önerilen altı bileşenli taksonomik model (aktör, güdü, niyet, araç, etki ve hedef), siber terörizmin ayırt edici unsurlarını sistematik

biçimde analiz etme imkânı sunmakta ve bu model üzerinden geliştirilen yaklaşımlar, devletlerin hukuki ve stratejik politikalarının şekillenmesinde belirleyici rol oynamaktadır. Türkiye'de siber terörizmle mücadele bağlamında geliştirilen yasal ve kurumsal düzenlemeler, bu kuramsal çerçeveye uygun biçimde değerlendirildiğinde daha anlamlı bir bütün oluşturmaktadır.

Siber Terörizmin Hukuki Tanımlanabilirliği: Ceza Hukuku ve Uluslararası İş Birliği

Siber terörizm eylemlerinin cezalandırılabilir hâle gelmesi, öncelikle bu eylemlerin mevzuat içinde tanımlanmasını gerektirir. Bu bağlamda, 2007 yılında Türk Ceza Kanunu'na (TCK) eklenen 243, 244 ve 245. maddeler; bilişim sistemlerine yetkisiz erişim, sistemlerin işleyişine müdahale, veri hırsızlığı ve bilişim yoluyla dolandırıcılık gibi eylemleri suç sayarak, dijital ortamda işlenen fiillerin cezai sorumluluk kapsamında değerlendirilmesini mümkün kılmıştır. Bu düzenleme, Plotnek and Slay (2021)'ın "araç" (means) ve "etki" (effect) bileşenleriyle örtüşmektedir; çünkü söz konusu düzenlemeler, siber saldırıların hangi araçlarla gerçekleştirildiğini ve bu araçların doğurabileceği toplumsal sonuçları hedef almaktadır.

Aynı yıl Türkiye, Budapeşte Siber Suçlar Sözleşmesi'ni imzalayarak uluslararası ceza hukuku çerçevesinde siber suçlarla mücadelede iş birliğini artırma taahhüdünde bulunmuştur (Tablo 2.). Bu sözleşme, sınır aşan siber suçların ortak tanımlarla ele alınmasını ve delil paylaşımı gibi konularda devletler arası koordinasyonu mümkün kılmaktadır. Böylece, siber terörizmin "aktör" ve "niyet" unsurları uluslararası düzlemde daha açık biçimde takip edilebilmiştir.

Bilgi Güvenliği, Dezenformasyon ve Dijital Haklar: Regülasyonun Genişlemesi

Siber terörizm yalnızca fiziksel sistemlere yönelik saldırılarla değil, aynı zamanda toplumların bilgiye erişim hakkını hedef alan dezenformasyon kampanyalarıyla da etkili olmaktadır. 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi Hakkında Kanun, internet içeriklerinin kontrolü ve suç teşkil eden yayınların engellenmesi gibi düzenlemeleri içermekte olup, siber terörizmin "niyet" ve "hedef" bileşenlerini önleme amacı taşımaktadır. Bu yasa, özellikle çevrimiçi radikalleşme, dijital propaganda ve bilgi manipülasyonu gibi terörizmin dijital türevlerine karşı önemli bir yasal araç olarak işlev görmektedir.

2020 yılında yürürlüğe giren 6698 sayılı Kişisel Verilerin Korunması Kanunu (KVKK) ise bireylerin dijital mahremiyetini koruma amacı taşımakta, siber teröristlerin hedef aldığı bireysel dijital alanları güvence altına almaktadır. Bu kanun, siber terörizmin toplumu korkutma (effect) ve araçlar yoluyla zarar verme (means) yönlerine karşı savunma mekanizmaları geliştirmeyi hedeflemektedir.

Ulusal Strateji Belgeleri ve Kurumsallaşma Süreci

Siber terörizmle etkin mücadele, yalnızca bireysel eylemlerin cezalandırılmasıyla sınırlı kalmamalı; aynı zamanda kurumsal düzeyde koordinasyonu ve planlamayı da içermelidir. Bu bağlamda 2016 yılında yayımlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ile Türkiye, kamu kurumları ile özel sektör arasında iş birliği esasına dayalı bir yaklaşım benimsemiş; kritik altyapıların korunması ve siber kapasitenin artırılması yönünde stratejik hedefler belirlemiştir. Bu belge, Plotnek and Slay modelindeki "hedef" (target) unsurunu doğrudan referans almaktadır. Çünkü kritik altyapılar, siber terörizmin en sık hedef aldığı alanlar arasındadır.

2024-2028 Ulusal Siber Güvenlik Stratejisi ise insan merkezli güvenlik yaklaşımı, siber dayanıklılık ve proaktif savunma kavramlarını ön plana çıkararak, Türkiye'nin siber tehditler karşısındaki kurumsal refleksini güçlendirmeyi hedeflemektedir. Bu strateji belgesi, aynı zamanda "güdü" (motive) ve "niyet" (intent) unsurlarına karşı önleyici bir anlayış geliştirmeyi amaçlamaktadır.

Entegre Güvenlik Yapısı: 7545 sayılı Siber Güvenlik Kanunu

7545 Sayılı Siber Güvenlik Kanunu, Türkiye'deki siber güvenlik altyapısının kurumsal düzeyde yeniden yapılandırılmasını sağlayan bir dönüm noktası niteliğindedir. 2025 yılında yürürlüğe giren bu kanun, kamu kurumları, özel sektör ve bireyleri kapsayan kapsamlı bir düzenleme öngörmekte; "Siber Güvenlik Başkanlığı" gibi yapılar aracılığıyla çok aktörlü bir güvenlik mimarisi oluşturmaktadır. Bu düzenleme, taksonomideki "aktör" ve "araç" unsurlarına doğrudan karşılık gelmekte ve tehditlerin bütüncül biçimde izlenmesini ve yönetilmesini olanaklı kılmaktadır.

Ayrıca, bu kanun ile birlikte tehdit analizi, erken uyarı sistemleri ve koordinasyon mekanizmaları gibi proaktif önlemler hayata geçirilmiş; böylece yalnızca olay sonrası müdahale değil, olay öncesi risk azaltma ve caydırıcılık da hukuki güvenlik çerçevesine entegre edilmiştir. Bu yaklaşım, siber terörizmin giderek evrilen ve sofistike hale gelen doğasına uygun biçimde "önleyici hukuk" perspektifinin benimsendiğini göstermektedir.

Türkiye'nin Siber Terörizm ile Mücadelesi

21. yüzyılda dijitalleşmenin hız kazanmasıyla birlikte devletler, sadece fiziksel değil dijital alanlarda da güvenlik tehditleriyle karşı karşıya kalmaktadır. Bu kapsamda, siber terörizm, ulusal güvenliği tehdit eden asimetrik tehditlerin başında gelmektedir. Türkiye de jeopolitik konumu, terörizmle mücadelesi ve bölgesel çatışmalardaki rolü itibariyle siber terörizme açık bir ülke konumundadır.

Teknolojik Kapasite ve Kamu-Özel İşbirlikleri

Siber terörizmle mücadelede teknolojik kapasitenin geliştirilmesi ve kamu-özel sektör işbirliğinin güçlendirilmesi, ulusal güvenlik politikalarının önemli bir parçasıdır. Türkiye, siber güvenlik alanında teknolojik altyapısını güçlendirmek ve bu alandaki insan kaynağını artırmak amacıyla çeşitli adımlar atmaktadır. Özellikle dijital dönüşüm sürecinde kamu kurumları ve özel sektör kuruluşlarının ortak çalışması, siber tehditlere karşı daha güçlü bir savunma hattı oluşturulmasını sağlamaktadır. Teknolojik kapasite açısından Türkiye, kritik altyapıların korunması için hem yerli hem de uluslararası düzeyde çözümler geliştirmektedir. Yerli teknoloji şirketleri, siber güvenlik yazılımları, yapay zeka tabanlı tehdit algılama sistemleri ve ağ güvenliği çözümleri üreterek ülkenin bu alandaki bağımlılığını azaltmayı hedeflemektedir. Özellikle TÜBİTAK ve Türkiye Siber Güvenlik Kümelenmesi gibi kuruluşlar, siber güvenlik alanındaki Ar-Ge projelerine destek sağlayarak teknolojik yeniliklerin önünü açmaktadır. Örneğin, TÜBİTAK tarafından geliştirilen yerli güvenlik yazılımları, kamu kurumlarının siber güvenliğini sağlamak ve ulusal verilerin korunmasını temin etmek amacıyla kullanılmaktadır. Bu tür projeler, Türkiye'nin siber tehditlere karşı daha dirençli hale gelmesine katkı sağlamaktadır.

Kamu-özel işbirliği, Türkiye'nin siber güvenlik stratejilerinde merkezi bir öneme sahiptir. Özellikle özel sektörün teknik bilgi birikimi ve yenilikçi çözümleri, kamu kurumlarının siber güvenlik kapasitelerini artırmak için kritik bir kaynak sağlamaktadır. Bu işbirliği, hem kamu hizmetlerinin dijitalleşmesinde hem de özel sektör altyapılarının korunmasında karşılıklı fayda sağlamaktadır. Türkiye'deki büyük teknoloji firmaları, bankalar ve enerji şirketleri, kamu kurumlarıyla ortak projeler yürüterek kritik altyapıların korunmasında aktif rol oynamaktadır. Örneğin, enerji sektörü için geliştirilen akıllı güvenlik sistemleri, saldırının önceden tesbiti ve önleyici tedbirlerin hızlı bir şekilde alınmasını sağlamaktadır.

Türkiye'nin siber güvenlik stratejilerinde uluslararası işbirlikleri de önemli bir yer tutmaktadır. Özellikle NATO ve Avrupa Birliği gibi uluslararası kuruluşlarla yürütülen çalışmalar, Türkiye'nin siber güvenlik kapasitesinin artırılmasına destek olmaktadır. NATO Siber Savunma Mükemmeliyet Merkezi ve diğer benzer organizasyonlarla yürütülen projeler, uluslararası bilgi paylaşımı ve saldırı analizinde Türkiye'ye önemli avantajlar sağlamaktadır. Ayrıca, özel sektörün uluslararası teknoloji şirketleriyle işbirlikleri, siber tehditlere karşı daha gelişmiş çözümler üretilmesine olanak tanımaktadır.

Bu işbirliklerinin bir diğer önemli boyutu ise eğitim ve insan kaynağı geliştirmeye yönelik çalışmalardır. Türkiye, siber güvenlik uzmanlarının yetiştirilmesi için üniversiteler ve teknoloji şirketleriyle işbirliği içinde çeşitli eğitim programları düzenlemektedir. Örneğin,

üniversitelerde açılan siber güvenlik lisans ve yüksek lisans programları, bu alanda yetişmiş insan kaynağını artırmayı hedeflemektedir. Aynı zamanda, teknoloji şirketleri tarafından düzenlenen sertifikalı eğitim programları ve atölyeler, siber güvenlik uzmanlarının teknik bilgi düzeyini artırmak için önemli bir katkı sunmaktadır. Türkiye'nin teknolojik kapasitesini artırma ve kamu-özel sektör işbirliklerini güçlendirme çabaları, siber tehditlere karşı daha dirençli bir ulusal güvenlik yapısı oluşturulmasında kritik bir rol oynamaktadır (Tablo 3.). Ancak, siber tehditlerin sürekli evrim geçiren doğası ve teknolojinin hızla gelişmesi, bu alanlardaki çalışmaların sürekli olarak yenilenmesini ve genişletilmesini gerektirmektedir. Hem kamu hem de özel sektörün ortak çabaları, Türkiye'nin siber güvenlik alanında güçlü bir konuma ulaşmasına katkı sağlamaktadır. Bu doğrultuda, yerli teknolojilerin geliştirilmesi, uluslararası işbirliklerinin artırılması ve insan kaynağının güçlendirilmesi, Türkiye'nin siber güvenlik stratejisinin temel taşlarını oluşturmaktadır.

Tablo 3. Teknolojik Kapasite ve Kamu-Özel İşbirliklerinin Gelişimi

Alan	Yapılan Çalışmalar (2015–2025)	Etkileri ve Sonuçları
Teknolojik Kapasite	-TÜBİTAK tarafından geliştirilen yerli güvenlik yazılımları - Yapay zeka tabanlı tehdit algılama ve ağ güvenliği çözümleri - Türkiye Siber Güvenlik Kümelenmesi'nin Ar-Ge destekleri - Blokzincir tabanlı kimlik doğrulama sistemleri	- Ulusal verilerin korunması, dışa bağımlılığın azaltılması - Siber tehditlerin erken tespiti ve önleyici tedbirlerin alınması - Yerli teknoloji üretiminin artması ve inovasyon kapasitesinin güçlenmesi - Veri bütünlüğü ve kullanıcı güvenliğinde ilerleme
Kamu-Özel İşbirlikleri	- Kamu kurumları ile özel sektör arasında ortak güvenlik projeleri - Banka, enerji ve ulaştırma sektörlerinde geliştirilen akıllı güvenlik sistemleri - Kritik altyapılara yönelik siber tatbikatlar ve senaryo çalışmaları - Siber tehdit bildirim platformlarının geliştirilmesi	- Kritik altyapıların güvenliğinin sağlanması - Finansal ve enerji sistemlerinde saldırı tespiti ve dayanıklılığın artırılması - Tehdit farkındalığı ve hızlı müdahale kapasitesinde gelişme
Uluslararası İşbirlikleri	- NATO Siber Savunma Mükemmeliyet Merkezi ile ortak çalışmalar - Avrupa Birliği projeleriyle uyumlu siber güvenlik faaliyetleri - Uluslararası teknoloji firmaları ile Ar-Ge projeleri - Global siber güvenlik tatbikatlarına aktif katılım	- Uluslararası bilgi paylaşımı ve saldırı analizinde gelişmiş çözümler - Türkiye'nin siber güvenlik stratejilerinin uluslararası standartlarla uyumu - Gelişmiş siber güvenlik çözümlerinin ülke çapında uygulanması
İnsan Kaynağı Gelişimi	- Üniversitelerde siber güvenlik lisans ve yüksek lisans programları - Kamu-özel sektör işbirliği ile yürütülen staj ve eğitim programları - Sertifikalı teknik eğitim programları - Ulusal CTF yarışmaları ve siber güvenlik etkinlikleri	- Yetişmiş insan kaynağı sayısının artırılması - Teknik bilgi düzeyinin yükseltilmesi - Genç yeteneklerin sektöre kazandırılması - Toplumsal siber güvenlik farkındalığının artması

2015–2025 dönemi, Türkiye'nin siber güvenlik alanındaki teknolojik kapasitesini artırmaya yönelik sistematik ve çok boyutlu adımlar attığı bir evre olarak değerlendirilebilir.

Bu süreçte hem kamu hem de özel sektör aktörlerinin iş birliğiyle hayata geçirilen projeler, ulusal güvenliğin dijital boyutunu güçlendirmeye odaklanmıştır.

Teknolojik Kapasite

Türkiye'nin siber güvenlik alanında teknolojik kapasitesini artırmaya yönelik en önemli gelişmelerden biri, TÜBİTAK tarafından geliştirilen yerli güvenlik yazılımlarıdır. Bu yazılımlar, ulusal veri güvenliğini sağlamaya yönelik ilk savunma hattını oluşturmaktadır. Buna ek olarak, yapay zekâ tabanlı tehdit algılama sistemleri ile ağ güvenliği çözümlerinin geliştirilmesi, olası tehditlerin proaktif biçimde tespitine imkân sağlamıştır.

Türkiye Siber Güvenlik Kümelenmesi tarafından sağlanan Ar-Ge destekleri, blokzincir tabanlı kimlik doğrulama sistemleri gibi yenilikçi teknolojilerin geliştirilmesine olanak tanımış; böylece veri bütünlüğü, kullanıcı güvenliği ve yerli teknoloji üretimi konularında önemli ilerlemeler kaydedilmiştir. Bu gelişmelerin temel çıktıları arasında dışa bağımlılığın azaltılması, inovasyon kapasitesinin artırılması ve stratejik teknolojilerde ulusal hâkimiyetin sağlanması yer almaktadır.

Kamu-Özel İşbirlikleri

Siber güvenliğin sürdürülebilirliğinde kamu-özel işbirliklerinin rolü giderek artmaktadır. 2015–2025 döneminde, kamu kurumları ile özel sektör arasında başta bankacılık, enerji ve ulaştırma olmak üzere kritik sektörlerde ortak güvenlik projeleri yürütülmüştür. Bu projeler kapsamında akıllı güvenlik sistemleri, saldırı tespit mekanizmaları ve tehdit analiz altyapıları geliştirilmiştir.

Kritik altyapıların korunmasına yönelik olarak düzenlenen siber tatbikatlar ve senaryo çalışmaları, sektörel farkındalığı artırmış, aynı zamanda tehditlere hızlı müdahale kapasitesini de önemli ölçüde güçlendirmiştir. Ayrıca, siber tehdit bildirim platformları sayesinde kamusal ve özel aktörler arasında etkili bir bilgi paylaşımı mekanizması kurulmuştur. Bu tür işbirlikleri, yalnızca güvenliği artırmakla kalmamış; aynı zamanda ulusal düzeyde dayanıklılığı ve kurumsal hazırlık seviyesini de iyileştirmiştir.

Uluslararası İşbirlikleri

Türkiye, bu dönemde yalnızca ulusal değil, aynı zamanda uluslararası düzeyde de önemli iş birliklerine imza atmıştır. NATO Siber Savunma Mükemmeliyet Merkezi (CCDCOE) ile sürdürülen ortak çalışmalar, Türkiye'nin çok uluslu siber güvenlik çabalarına entegrasyonunu sağlamıştır. Aynı şekilde, Avrupa Birliği'nin Dijital Avrupa Programı

çerçevesinde yürütülen projeler, Türkiye'nin siber güvenlik politikalarının uluslararası norm ve standartlarla uyumlu hâle getirilmesini desteklemiştir.

Uluslararası teknoloji firmalarıyla yürütülen Ar-Ge projeleri ve küresel siber güvenlik tatbikatlarına aktif katılım, Türkiye'nin küresel bilgi ağlarına erişimini kolaylaştırmış, siber tehditlere karşı daha sofistike çözümler geliştirmesine katkı sağlamıştır.

İnsan Kaynağı Gelişimi

Siber güvenlik alanında sürdürülebilir kalkınmanın temel dayanaklarından biri, nitelikli insan kaynağıdır. Bu bağlamda üniversitelerde açılan siber güvenlik lisans ve yüksek lisans programları, hem akademik hem de uygulamalı bilgi birikiminin artırılmasına hizmet etmiştir. Bunun yanında, kamu-özel sektör ortaklığında düzenlenen staj ve teknik eğitim programları, genç yeteneklerin sektöre kazandırılmasında etkili olmuştur.

Sertifikalı eğitim programları ile teknik uzmanlık alanları desteklenmiş, düzenlenen CTF (Capture The Flag) yarışmaları ve diğer etkinlikler sayesinde toplumsal farkındalık da artırılmıştır. Sonuç olarak, Türkiye'nin siber güvenlik ekosisteminde nitelikli insan kaynağı sayısı artmış ve sektörün teknik kapasitesi güçlenmiştir.

TARTIŞMA

Bu bölümde araştırma bulguları, kuramsal çerçeve ve ilgili literatür ışığında yorumlanmış; elde edilen sonuçlar bütüncül bir yaklaşımla değerlendirilerek siber terörizm olgusuna dair çıkarımlar yapılmıştır. Tartışma kapsamında önce kullanılan kuramsal modelin (Plotnek and Slay (2021)'ın altı bileşenli taksonomisi) bulgularla nasıl örtüştüğü ya da ayrıştığı ele alınmış ve Türkiye örneği uluslararası literatürle karşılaştırılmıştır. Kritik altyapılara yönelik saldırıların anlamı ve Türkiye'nin siber güvenlik politikalarındaki dönüşüm tartışılarak; siber terörizmin sınır aşan doğası bağlamında uluslararası işbirliği kapasitesi değerlendirilmiştir. Son olarak, bulgulardan yola çıkarak geleceğe yönelik politika ve strateji önerileri sunulmuştur. Bu sayede, çalışmanın sonuçları hem kuramsal modele uygunluk açısından hem de pratik uygulamalar bakımından kapsamlı bir şekilde yorumlanabilmiştir.

Araştırmada kuramsal temel olarak benimsenen Plotnek and Slay (2021)'ın altı bileşenli modeli (aktör, güdü, niyet, araç, hedef, etki), elde edilen bulguların analizine sistematik bir çerçeve sağlamıştır. Bulgular genel olarak bu modelin öngördüğü unsurlarla büyük ölçüde örtüşmektedir. İncelenen siber saldırı vakalarının önemli bir kısmında, saldırıyı gerçekleştiren aktör (örneğin uluslararası bir hacktivist grup olan Anonymous ya da belli ideolojik gruplarla bağlantılı hacker kümeleri) tespit edilebilmiştir. Bu durum, kuramsal modelde "aktör" unsurunun eklenmesinin yerinde olduğunu göstermektedir; zira geleneksel beş bileşenli taksonomi (aktör öğesi olmaksızın) incelenen vakalardaki tehdidin kaynağını tam yansıtmakta yetersiz kalabilirdi. Nitekim Türkiye örneğinde siber terör eylemleri, sadece tanınmış terör örgütleri tarafından değil, bazen anonim hacktivist kolektifler veya devlet destekli olduğu düşünülen gruplar tarafından da gerçekleştirilmiştir. Bu çeşitlilik, modelin aktör boyutunun bulgularla desteklendiğini göstermektedir. Öte yandan, bazı saldırılarda failin kesin olarak belirlenememesi, siber uzayın saldırganlara tanıdığı anonimlik avantajından kaynaklanmaktadır; bu da literatürde vurgulandığı üzere klasik güvenlik yaklaşımlarıyla tehdidin kontrol altına alınmasını zorlaştıran bir etmendir. Dolayısıyla, modelin aktör bileşeninin pratikte karşılaşılan anonimlik sorunu nedeniyle her zaman kolaylıkla doldurulamadığı görülmüştür.

Modelin bir diğer boyutu olan güdü (motive) ve buna bağlı niyet (intent) unsurları da bulgular kapsamında incelenen vakalarda büyük ölçüde karşılık bulmaktadır. Çalışma bulguları, Türkiye'de 2015–2025 döneminde gerçekleşen ciddi siber saldırıların önemli bir kısmının ideolojik veya siyasi güdüler taşıdığını göstermektedir. Örneğin, 2015 yılında

Anonymous tarafından Türkiye'nin .tr DNS altyapısına gerçekleştirilen DDoS saldırısının ardında, Türkiye'nin belirli politikalarına tepki niteliğinde ideolojik bir mesaj verme niyeti olduğu değerlendirilmektedir. Bu tür vakalar, siber terörizm ile sıradan siber suçlar arasındaki ayrımın modelde belirtildiği gibi güdü ve niyet boyutlarında ortaya çıktığını doğrulamaktadır. Nitekim literatürde de siber terör eylemlerinin ayırt edici özelliğinin finansal kazanç gibi kişisel motivasyonlar değil, politik veya ideolojik amaçlar olduğu vurgulanmaktadır. Bulgular, enerji altyapısını hedef alan saldırılar veya kamu kurumlarına yönelik sistematik veri sızıntılarının arka planında hükümet politikalarını protesto etme, korku ve kaos ortamı yaratma gibi niyetler bulunduğunu göstermiştir. Bu bağlamda, hedef alınan kurum ya da sektör ile saldırganın güdüsü arasında kuramsal modelin öngördüğü ilişki doğrulanmaktadır: İdeolojik güdüye sahip aktörler, seslerini duyurmak veya baskı oluşturmak için stratejik önemdeki hedefleri seçmektedir. Bununla birlikte, güdü unsuru bakımından model ile kısmen çelişen bulgular da vardır. Özellikle son yıllarda sağlık sektörüne yönelik fidye yazılımı saldırılarında, saldırganların öncelikli motivasyonunun maddi çıkar olduğu görülmektedir. Bu tür saldırılar ilk bakışta terörizm kapsamına girmese de (zira ideolojik bir amaç güdülmemektedir), yarattıkları etki itibarıyla hastane hizmetlerinin aksaması, halkta panik oluşması siber terörizm boyutuna yaklaşmaktadır.

Bu durum, kuramsal modelde net biçimde tanımlanan "ideolojik güdü" kriterinin pratikte gri alanlara sahip olabileceğine işaret etmektedir. Yani, bir eylemin terörizm sayılması için güdü ideolojik olmalıdır şeklindeki yaklaşım, sağlık sektöründeki fidye yazılımı örneklerinde olduğu gibi bazı vakalarda tartışmaya açıktır. Bu bulgu, güdü ve etki bileşenleri arasında modelin öngörmediği bir gerilimi ortaya koymaktadır. Maddi güdü ile başlayan bir saldırı, etkileri bakımından terör eylemine dönüşebilmektedir.

Modelin araç (means) ve hedef (target) bileşenleri, araştırmada incelenen vakalarda oldukça belirgin bir biçimde gözlenmiştir. Bulgular, Türkiye'de siber terörizm kapsamında kullanılan araçların dağıtılmış hizmet kesintisi (DDoS) saldırıları, zararlı yazılımlar (özellikle fidye yazılımları) ve gelişmiş kalıcı tehdit (APT) teknikleri gibi geniş bir yelpazede olduğunu ortaya koymuştur. Bu çeşitlilik, literatürde ifade edilen küresel eğilimlerle uyumludur; örneğin Rid and Buchanan (2015), siber saldırganların giderek daha sofistike APT araçlarına yöneldiğini belirtirken Türkiye de benzer araçların hedefi olmuştur. Model "araç" unsurunu açıkça tanımlayarak her bir saldırıda hangi teknik yöntemlerin kullanıldığını sınıflandırmaya imkân tanımıştır. Nitekim çalışmada enerji sektörüne yönelik bir saldırı, zararlı yazılım yoluyla kritik bir SCADA sisteminin sabote edilmesi biçiminde gerçekleşirken; başka bir vakada devlet kurumlarına karşı DDoS saldırısı aracı kullanılmıştır. Bu farklı araçlar, hepsinin siber terörizm

şemsiyesi altında değerlendirilebilmesini model sayesinde sistematik hale getirmiştir. Hedef boyutunda ise bulgular, model ile tam bir örtüşme sergilemektedir. İncelenen eylemlerde sıklıkla kritik altyapılar (enerji şebekeleri, hastane bilişim sistemleri gibi) ile kamu otoritesini temsil eden kurumların (bakanlıklara ait web siteleri, ulusal DNS altyapısı vb.) hedef alındığı saptanmıştır. Bu da modelde vurgulanan "hedefin stratejik önemi" ilkesinin gerçek dünyada karşılığını bulduğunu göstermektedir. Özellikle enerji ve sağlık gibi sektörlerin tercih edilmesi, saldırganların toplumda maksimum etkiyi hedeflediğinin göstergesidir ki bu, teorik olarak siber terörizmin temel amaçlarından biridir (korku ve zarar verme maksimizasyonu). Modelin son bileşeni olan etki (effect) de bulgular kapsamında değerlendirilmiştir. Türkiye'de gerçekleşen vakaların etkisi, çoğu zaman hizmet kesintileri, veri sızıntıları veya maddi kayıplar şeklinde somut olarak gözlenmiştir. Örneğin, 2015'teki Anonymous saldırısı sonucu .tr uzantılı sitelere erişimin kesilmesi, binlerce kurum ve kuruluşun faaliyetlerini aksatmış; bu da ekonomi ve kamu hizmetleri üzerinde ölçülebilir bir etki yaratmıştır. Benzer şekilde bir devlet bankasına yönelik siber saldırı girişiminin kamuoyunda yarattığı tedirginlik, psikolojik etki boyutunun önemini ortaya koymaktadır. Kuramsal model, etki unsurunu çerçeveye dahil ederek bu tip sonuçların analizine imkân tanımıştır. Bulgular, hemen her ciddi vakanın en az bir somut (teknik veya ekonomik) etkiye ve bir de soyut (toplumsal korku, güvensizlik) etkiye sahip olduğunu göstermektedir ki bu da modelin öngörüsüyle uyumludur.

Genel olarak, Plotnek and Slay (2021)'ın altı bileşenli modeli çalışmamızdaki bulguları kategorize etme ve anlama konusunda faydalı ve geçerli bir model olduğunu kanıtlamıştır. Aktör, araç, hedef ve etki unsurlarında model ile bulgular bütünüyle örtüşürken; güdü ve niyet unsurlarında, özellikle bazı finansal motivasyonlu saldırıların terörizm kavramına dahil edilip edilmeyeceği konusunda, modelin öngörmediği karmaşık durumlar ortaya çıkmıştır. Bu durum, siber terörizmin tanımında hala gri alanlar olduğunu ve kuramsal modellerin gerçek hayattaki tüm olguları tam olarak kapsamasının güç olduğunu göstermektedir. Yine de altı bileşenli çerçevenin kullanımı, bu tez çalışmasında disiplinli bir analiz süreci sağlamış; hem literatürdeki kavramsal tartışmaların somut verilere uygulanmasını kolaylaştırmış hem de politika tartışmalarına sistematik bir temel oluşturmuştur. Bu sayede, bulguların değerlendirilmesi ve sonraki önerilerin geliştirilmesi kuramsal açıdan tutarlı bir zemine oturtulmuştur.

Türkiye'de 2015–2025 yılları arasında gözlemlenen siber terörizm örüntüleri, büyük ölçüde küresel literatürde tanımlanan eğilimlerle paralellik göstermektedir. Dünya genelinde siber terörizm olgusunun ilk ortaya çıkışı ve gelişimi incelendiğinde, saldırgan aktörlerin profillerinin bireysel hacker'lardan örgütlü yapılara ve oradan da devlet destekli profesyonel gruplara evrildiği görülmektedir. Araştırma bulgularımız, Türkiye'de de benzer bir evrim

yaşandığına işaret etmektedir. 2010'ların ortalarında daha çok bireysel veya dağınık gruplar halinde gerçekleşen siber saldırılar, yıllar içinde daha örgütlü ve koordineli nitelik kazanmıştır. Örneğin, 2015'te Anonymous gibi görece gevşek örgütlenmiş bir hacktivist grup Türkiye'yi hedef alırken, 2020'lere gelindiğinde ülke, ileri seviye sürekli tehdit (APT) teknikleri kullanan ve bazen devletlerin desteğini almış olabilecek grupların saldırılarına maruz kalmaya başlamıştır.

Literatürde Rid and Buchanan (2015) tarafından vurgulanan küresel ölçekte siber saldırı araçlarının karmaşıklığının artması olgusu, Türkiye örneğinde de doğrulanmaktadır. Bu tez çalışmasında vakalarda tespit edilen karmaşık zararlı yazılımlar, o gün açıklarından faydalanma girişimleri ve uzun soluklu sızma (infiltrasyon) teşebbüsleri, Türkiye'nin de küresel siber tehdit dalgasının bir parçası olduğunu göstermektedir. Nitekim Çakır ve Yıldırım (2022), Türkiye'nin hem bu tür sofistike araçların hedefi olduğunu hem de bölgesel rekabet bağlamında benzer tekniklerle karşı karşıya kaldığını belirtmektedir. Bu durum, Türkiye'deki siber terör vakalarının teknik yönünün, literatürde belgelenen uluslararası örneklerle büyük ölçüde benzerlik taşıdığını ortaya koymaktadır.

Küresel literatürle karşılaştırıldığında Türkiye örneğini özgün kılan bazı noktalar da dikkat çekmektedir. Weimann (2016) her ne kadar siber terörizmin uluslararası gelişim çizgisini ortaya koymuşsa da, Türkiye'deki benzersiz durum, bölgesel silahlı terör örgütlerinin dijitalleşme süreçlerinin hızla seyretmesidir.

Özellikle Ortadoğu ve yakın coğrafyamızda faaliyet gösteren bazı terör örgütlerinin, propaganda ve iletişim faaliyetlerinin ötesine geçerek siber saldırı kapasitesi geliştirme çabaları Türkiye'ye yansımıştır. Örneğin, Suriye ve Irak'taki çatışmaların bir uzantısı olarak ortaya çıkan bazı radikal gruplar, Türk devlet kurumlarının web sitelerine veya sosyal medya hesaplarına saldırılar düzenlemiş; bu gruplar siber uzayı geleneksel terör eylemlerini tamamlayıcı bir cephe olarak kullanmışlardır. Bu açıdan bakıldığında, Türkiye'deki siber terör vakaları, çoğu Batı ülkesindeki örneklerden daha "hibrit" bir nitelik sergileyebilmektedir. Fiziksel terör faaliyetleri yürüten örgütlerle bağlantılı siber saldırılar görülme sıklığı bakımından Türkiye, literatürde pek çok ülkenin deneyiminden ayrışmaktadır. Bunun bir nedeni, Türkiye'nin coğrafi ve jeopolitik konumu gereği hem Orta Doğu'daki istikrarsızlıklardan etkilenmesi hem de Avrupa ve Asya güvenlik ortamının bir parçası olmasıdır. Bu çift yönlü etki, Türkiye'yi hem küresel siber terör ağlarının bir hedefi hem de bölgesel aktörlerin dijital alandaki çatışmalarının bir cephesi haline getirmektedir. Türkiye'deki mevcut politik ve toplumsal kutuplaşmanın, siber saldırıların etkisinin toplumda daha geniş yankı bulmasına zemin hazırladığını belirtmiştir.

Gözlemlenen bazı dezenformasyon kampanyaları ve hacktivist eylemler, toplumdaki mevcut gerilim hatlarını hedef alarak psikolojik etkiyi büyütmeyi amaçlamıştır. Bu durum, uluslararası örneklerde de görülmekle birlikte (örn. seçim dönemlerinde yabancı aktörlerin sosyal medya manipülasyonları), Türkiye'deki toplumsal duyarlılıklar nedeniyle etkilerin daha derin olabildiğini göstermektedir. Dolayısıyla, siber terörizmin sosyopolitik etkileri açısından Türkiye, literatürde bahsedilen genel eğilimlerin ötesinde kendine has bir kırılganlık profiline sahip görünmektedir.

Bir diğer karşılaştırma boyutu da saldırıların hedefleri ve sonuçları üzerinedir. Uluslararası örneklerde sıkça tartışılan bir konu, siber terörizmin şimdiye dek büyük ölçüde potansiyel bir tehdit olarak kalması ve gerçek anlamda yıkıcı bir "dijital 11 Eylül" yaşanmamış olmasıdır. Literatürde birçok uzman, bugüne dek gerçekleşen siber saldırıların terörizm boyutuna yaklaşsa da kitlesel can kaybı veya uzun süreli fiziksel yıkım gibi sonuçlar doğurmadığına dikkat çekmektedir. Türkiye'de 2015–2025 yılları arasında yaşanan olaylar da benzer şekilde, ciddi olmakla birlikte kontrollü etkiler yaratmış; örneğin elektrik altyapısına yönelik saldırılar hizmet kesintilerine yol açsa da kalıcı hasar yaratmamıştır, sağlık sektöründeki saldırılar ise hasta bilgilerinin çalınması veya randevu sistemlerinin bloke edilmesi gibi sonuçlarla sınırlı kalmıştır. Bu bakımdan, Türkiye'nin deneyimi küresel tabloyla örtüşmektedir. Siber terörizm tehdidi ciddi bir ulusal güvenlik sorunu olarak algılanmakla birlikte gerçekleşen saldırılar çoğunlukla kısa vadeli aksama ve korku yaratma etkisinde kalmıştır. Ancak bu durum rehavete yol açmamalıdır; zira hem literatürde hem de bulgularımızda görüldüğü üzere saldırıların sayısı ve karmaşıklığı artma eğilimindedir.

Birçok ülke gibi Türkiye de, kritik altyapılara yönelik giderek artan sayıda ve yetkinlikte saldırılarla karşı karşıyadır. Örneğin, Türkiye'de enerji sektörüne yönelik tespit edilen saldırı sayısı 2015'te yaklaşık 80 civarında iken 2024'te 460'a ulaşmıştır. Benzer şekilde dünya genelinde de enerji altyapılarına saldırılar son on yılda katlanarak artmıştır. Bu paralel artış trendi, Türkiye'nin siber tehditler konusundaki tecrübesinin tekil bir vakadan ziyade küresel bir sorunun parçası olduğunu göstermektedir. Uluslararası literatürle kıyaslandığında Türkiye'deki bir özgün nokta da devletin karşı koyma kabiliyetinin hızlı gelişimidir. Pek çok ülke siber terörizm tehdidine karşı kurumsal yapılanmalarını yeni yeni oluştururken, Türkiye bulgularımızın ortaya koyduğu üzere 2020'lerin ilk yarısında kapsamlı yasal ve kurumsal adımlar atmıştır. Bu yönüyle Türkiye, tehditlere karşı proaktif politika geliştirme konusunda literatürde incelenen bazı ülkelere göre daha hızlı yol almış görünmektedir. Sonuç itibarıyla Türkiye örneği ile uluslararası örnekler arasında hem benzerlikler hem farklılıklar bulunmaktadır. Kullanılan yöntemler, hedef alınan sektörler ve aktör tipolojileri bakımından

ciddi benzerlikler söz konusu iken; bölgesel dinamikler, toplumsal bağlam ve karşı tedbirler açısından Türkiye kendine has bir görünüm sergilemektedir. Bu da siber terörizmle mücadelede evrensel stratejilerin yanı sıra ülke özelinde uyarlanmış yaklaşımların gerekliliğini ortaya koymaktadır.

Araştırma bulguları, enerji ve sağlık gibi kritik altyapıların siber teröristler tarafından öncelikli hedefler arasında görüldüğünü net biçimde ortaya koymaktadır. Bu durum kuramsal olarak beklendik bir sonuçtur; zira literatürde enerji santralleri, elektrik şebekeleri, hastaneler ve benzeri kritik altyapılar, modern toplumun işleyişi vazgeçilmez oldukları için terör amaçlı saldırılarda maksimum etki yaratacak hedefler olarak tanımlanmaktadır. Enerji sektörüne yönelik siber saldırıların anlamı, yalnızca teknik bir arıza yaratmanın ötesine geçer. Toplumun her kesimini etkileyebilecek geniş çaplı karartmalar ve enerji kesintileri, ekonomik faaliyeti felç edebilecek ve günlük hayatı durma noktasına getirebilecek güçtedir. Nitekim 2015 yılında Türkiye genelinde yaşanan ve uzun süreli elektrik kesintilerine yol açan olay her ne kadar resmi olarak siber saldırı kaynaklı olduğu doğrulanmasa da kamuoyunda bir "siber saldırı" algısı yaratmış ve kritik altyapıların ne denli hayati olduğunu göstermiştir. Bulgularımızda da 2015 sonrası dönemde enerji altyapısına yönelik saldırı girişimlerinin düzenli bir artış gösterdiği ve 2020'lerin ortalarına gelindiğinde ciddi boyutlara ulaştığı görülmektedir.

Bu saldırıların ardındaki amaç, ülke genelinde hayatı aksatmak, ekonomik zarara yol açmak ve dolaylı olarak devlet otoritesine meydan okumak şeklinde değerlendirilebilir. Kuramsal çerçevede bakıldığında, enerji altyapısının hedef alınması, siber teröristlerin "düşmanı stratejik olarak zayıflatma" hedefiyle örtüşmektedir. Geleneksel terörizmde nasıl ki enerji nakil hatları, petrol rafinerileri gibi hedefler saldırıya uğrayarak bir ülkenin can damarı kesilmeye çalışılırsa, siber uzayda da benzer bir mantıkla hareket edildiği anlaşılmaktadır. Üstelik siber yöntemlerle bu hedeflere saldırmak, fiziki saldırılara nazaran daha az riskli fakat etkisi benzer derecede yüksek bir yöntemdir. Bu nedenle enerji altyapıları, siber teröristler için adeta bir "stratejik kaldıraç" işlevi görmektedir. Kendi kapasitesi sınırlı bir saldırgan dahi kritik bir enerji düğüm noktasını hedef alarak orantısız büyüklükte bir etki yaratabilir. Bu noktada Yılmaz ve Karakaş (2020)'ın belirttiği üzere kritik altyapılara sızma ve onları işlemez hale getirme en sık başvurulan siber terörizm yöntemleri arasındadır.

Sağlık sektörüne yönelik siber saldırılar, enerji sektörü kadar öncelikli bir hedef haline gelmiş olup, bunun arkasında yatan nedenler hem pratik hem de psikolojik boyutlarıyla tartışmaya değerdir. Son yıllarda sağlık hizmetlerinin dijital sistemlere bağımlılığının artması (e-sağlık uygulamaları, dijital hasta kayıtları, entegre hastane bilgi yönetim sistemleri vb.), bu alanı siber saldırılara karşı kırılgan hale getirmiştir. Elde edilen bulgulara göre Türkiye'de 2016

yılında oldukça sınırlı sayıda olan sağlık sektörü siber saldırı vakaları, 2020 yılı sonrasında keskin bir artış göstermiştir.

Özellikle COVID-19 pandemisiyle sağlık altyapılarının yükünün ve dijitalleşmesinin artması, saldırganlara yeni fırsatlar sunmuştur. Sağlık sektörünün hedef alınmasının pratik nedenleri arasında kişisel sağlık verilerinin taşıdığı yüksek ticari ve istihbari değer ile hastane gibi kurumların kesintiye tahammülsüz olması bulunmaktadır.

Bir hastanenin bilgi sisteminin çökmesi, sadece dijital veriye erişilememesi demek değildir; aynı zamanda acil servis işlemez hale gelebilir, ameliyatlar durabilir ve insan hayatı doğrudan tehlikeye girebilir. Bu yüzden saldırganlar açısından hastaneler "fidye" için de ideal hedeflerdir. Zira kurumlar hayat kurtarma zorunluluğu nedeniyle çoğu zaman fidye ödemeyi bile düşünebilirler. Ancak sağlık altyapılarına saldırıların siber terörizm boyutundaki anlamı, salt para kazanma amaçlı siber suçun ötesine geçmektedir. Özellikle kamu hastanelerine yönelik fidye yazılımı saldırıları, kritik zamanlarda sağlık hizmetlerini aksatarak toplumda korku ve güvensizlik yaratma potansiyeline sahiptir.

Birleşmiş Milletler'in tanımına göre siber terörizm, "siyasi veya ideolojik amaçlarla, korku yaratmak için bilgi teknolojilerinin kullanıldığı şiddet eylemleri" olarak belirtilmektedir. Bu açıdan bakıldığında, doğrudan can kaybına yol açmasa da bir hastanenin sistemlerini çökerten ve acil hastaları tedavi edilemez duruma getiren bir siber saldırı, terör eylemlerinin amacına benzer bir şekilde toplumda panik yaratacaktır. Bu tez çalışmasında tespit edilen sağlık sektörüne yönelik bazı büyük ölçekli saldırılar, her ne kadar fail gruplar fidye talebiyle hareket etseler de yan ürün olarak kamuda ciddi bir endişe ortamı oluştuğunu göstermiştir. Bu da bize sağlık altyapılarına yönelik saldırıların terörizm literatüründeki "korku salma" amacıyla örtüşen yönlerini ortaya koyar. Teorik açıdan, hastanelerin ve sağlık sistemlerinin hedef alınması, siber teröristlerin toplumsal moral ve güven duygusunu zedeleme stratejisinin bir parçası olarak görülebilir. Nasıl ki geleneksel terörizmde sivillerin yoğun olarak bulunduğu alanlara saldırılar düzenleyerek halkın devlete olan güveni sarsılmak isteniyorsa, siber terörizmde de halkın en temel ihtiyaçlarından olan sağlık hizmetine erişimini engelleyerek benzer bir güvensizlik ortamı yaratılmaya çalışılmaktadır. Sunulan tez bu bağlamda, Güler (2019) ve Çelik (2021)'in vurguladığı üzere, sağlık ve enerji gibi kritik sektörlere yönelik bu tür saldırılar teknik birer eylem olmanın ötesinde, toplumsal sürdürülebilirliğe ve kamu güvenliğine yöneltilmiş bir meydan okuma niteliği taşıdığı bulgusuna ulaşmıştır.

Özetle, enerji ve sağlık altyapılarına yönelik siber saldırıların öncelikli hedefler olması tesadüf değildir; bilakis, terör stratejisi açısından rasyonel bir hedef seçimidir. Bu alanlar, modern toplumda "kritik" addedilen ve işlevsellikleri kesintiye uğradığında geniş çaplı panik

yaratabilecek sektörlerdir. Türkiye'de bu sektörlere yönelen tehditlerin arttığını ve çeşitlendiğini ortaya koyarken, literatürdeki kuramsal açıklamalar bu durumu anlamlandırmamıza yardımcı olmaktadır. Siber teröristler, asimetrik avantaj elde etmek için zayıf noktalar olarak gördükleri kritik altyapıları vurmakta, böylece küçük ölçekli bir saldırıyla büyük ölçekli neticeler doğurmayı hedeflemektedirler. Bu gözlem, enerji ve sağlık altyapılarının korunmasının neden ulusal güvenlik siyasetinin merkezinde yer alması gerektiğini de açıklamaktadır. Nitekim sonraki bölümde ele alınacağı üzere, Türkiye'nin son yıllarda siber güvenlik politikalarını dönüştürmesinin ardındaki itici güçlerden biri de bu kritik sektörlere yönelik artan tehdittir.

Türkiye'nin siber güvenlik politikaları, son on yılda belirgin bir dönüşüm ve olgunlaşma sürecinden geçmiştir. Ülkemizin 2010'ların ilk yarısında siber tehditler karşısında daha çok sınırlı ölçekli ve tepkisel önlemlerle yetindiğini ancak zamanla daha stratejik ve kurumsal bir yaklaşım benimsediğini göstermektedir.

2013 yılında yayımlanan ilk Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ile (2013–2014) başlayan bu süreçte, siber güvenlik konusu ulusal güvenlik gündemine dahil edilmeye başlanmıştır. 2015 yılına gelindiğinde Bilgi Teknolojileri ve İletişim Kurumu (BTK) öncülüğünde hazırlanan siber güvenlik strateji belgesi, siber tehditlerin milli güvenliği ilgilendiren bir mesele olduğunu vurgulamış ve bu alanda kamu, özel sektör, akademi ve sivil toplumun eşgüdüm içinde çalışmasını hedefleyen politikaların kurumsallaşmasına zemin hazırlamıştır.

Nitekim ilk strateji belgeleri ve kurulan kurullar (Ulusal Siber Güvenlik Kurulu gibi) sayesinde, enerji, finans, telekomünikasyon gibi kritik sektörlerin temsilcileriyle devlet kurumları aynı masa etrafında toplanarak ulusal düzeyde bir farkındalık oluşturulmuştur. Bu aşama, Türkiye'nin siber güvenlik politikasında farkındalık ve koordinasyon dönemidir. Saldırıların artan sıklığına karşı dağınık önlemler yerine koordineli bir savunma hattı oluşturma gayreti ön plana çıkmıştır. Bu tez çalışmasında 2015 ve 2016 yılları arasında yaşanan bazı önemli siber olayların (örneğin bankacılık sistemine yönelik bir DDoS dalgası veya kritik bir bakanlığın veritabanına sızılması girişimi) bu farkındalık sürecini hızlandırdığını ima etmektedir. Zira bu olayların hemen akabinde, resmi strateji belgelerinde siber terörizm ifadesi ilk kez açıkça kullanılmaya başlanmış ve terör amaçlı siber faaliyetlere karşı hem teknik hem hukuki tedbirler geliştirilmesi gereği belirtilmiştir.

2016 sonrası dönem, Türkiye'nin siber güvenlik politikalarında kurumsallaşma ve kapasite geliştirme dönemidir. Bu süreçte, bir yandan hukuki altyapı güçlendirilmiş, diğer yandan fiili mücadele kapasitesi artırılmıştır. 2016'da yürürlüğe konulan Ulusal Siber Olaylara

Müdahale Ekibi (USOM) yapılanması ile sektörel SOME'lerin (Siber Olaylara Müdahale Ekipleri) kurulması, ülke genelinde bir erken uyarı ve hızlı reaksiyon sistemi oluşturmuştur. Bu sayede farklı kurumlar arası bilgi paylaşımı mekanizmaları tesis edilmiş ve olası saldırılara karşı daha hazırlıklı bir duruma geçilmiştir. Eşzamanlı olarak, Türk Ceza Kanunu ve ilgili mevzuatta yapılan değişikliklerle siber suçlara ve siber terörizm eylemlerine yönelik cezai müeyyideler netleştirilmiş, bilişim sistemlerine saldırı suçunun karşılığı ağırlaştırılmıştır. Bu dönemdeki önemli bir gelişme de siber güvenlik konusunun üst düzey yönetişim yapıları içinde ele alınmaya başlanmasıdır. Örneğin, 2017'de kurulan Dijital Dönüşüm Ofisi bünyesinde siber güvenlik birimi oluşturulması ve 2018'de Milli Savunma Bakanlığı çatısı altında Siber Savunma Komutanlığı teşkilatlanması, siber tehditlerle mücadelenin kurumsal hiyerarşi içinde sağlam bir yer edindiğini göstermiştir. Uluslararası entegrasyonun derinleşmesi de bu dönemin özelliklerindendir. Türkiye, 2019'da NATO Kooperatif Siber Savunma Mükemmeliyet Merkezi'ne (CCDCOE) katılarak uluslararası düzeyde kolektif siber savunma çabalarına dahil olmuştur.

Bu adım küresel işbirliği prensibinin ulusal politikaya yansımasıdır ve Türkiye'nin siber güvenlik stratejisini daha geniş bir perspektife taşıdığına işaret eder. 2020'ye gelindiğinde Türkiye'nin siber güvenlik yaklaşımının artık sadece teknik tedbirlerle sınırlı kalmayıp çok katmanlı (teknik, idari, hukuki ve uluslararası boyutları birleştiren) bir yapıya dönüştüğünü teyit etmektedir. Bu dönüşüm sadece dijital altyapıların korunması açısından değil, aynı zamanda siber terörizm gibi yeni nesil tehditlerin önlenmesi ve yönetilmesi bakımından kritik öneme sahip olmuştur.

2020'li yılların ilk yarısı, Türkiye'nin siber güvenlik politikalarında stratejik atılım ve merkezileşme dönemine denk gelmektedir. Özellikle 2020 sonrasında artan fidye yazılımı saldırıları, kritik kurumlara yönelik veri ihlalleri ve kamuoyuna yansıyan diğer siber olaylar, kapsamlı bir yasal düzenleme ihtiyacını gündeme getirmiştir. Bu ihtiyaç neticesinde hazırlanan ve 2025 yılında yürürlüğe giren 7545 sayılı Siber Güvenlik Kanunu, Türkiye'nin siber güvenlik mimarisinde bir dönüm noktası teşkil etmektedir. 19 Mart 2025 tarihli Resmî Gazete'de yayımlanarak yürürlüğe giren bu Kanun ile Cumhurbaşkanlığı bünyesinde Siber Güvenlik Başkanlığı kurulmuş ve ulusal siber güvenlik yönetiminin tek elden yürütülmesi hedeflenmiştir. Kanun, kritik altyapı işletmecilerinin sorumluluklarından ulusal siber olay yönetim merkezinin yetkilerine kadar pek çok alanda düzenlemeler getirmiş; siber terörizmle mücadeleye yönelik olarak da cezai hükümler ve uluslararası işbirliği mekanizmalarına dair hükümler içermiştir. Bu tez çalışmasının başından beri vurguladığı kuramsal ihtiyacın yani siber terörizm olgusuna bütüncül ve kurumsal cevap verme ihtiyacının somut bir karşılığı olarak değerlendirilebilir.

Artık Türkiye, siber güvenlik alanında da tıpkı konvansiyonel güvenlikte olduğu gibi merkezi bir otorite (Siber Güvenlik Başkanlığı) aracılığıyla politika belirlemekte ve uygulamaktadır. Bu dönüşümün arkasında, bulgularımızda belgelenen çok katmanlı tehditlerin payı büyüktür. Enerji ve sağlık başta olmak üzere kritik sektörlere yönelen saldırıların artışı, geleneksel kurumların ayrı ayrı gayretleriyle başa çıkılamayacak bir risk alanı yaratmıştır. Dolayısıyla 7545 sayılı Siber Güvenlik Kanunu ile sembolleşen politik dönüşüm, esasen 2015'ten itibaren birikerek gelen tecrübelerin ve derslerin sonucudur. Plotnek and Slay (2021)'ın vurguladığı üzere siber terörizmle mücadele salt teknik tedbirlerle sınırlı kalamaz; hukuki, politik ve toplumsal boyutlarıyla da ele alınmalıdır.

Türkiye'nin politikalarındaki dönüşümünde tam olarak bu çok boyutlu perspektifin benimsendiğini göstermektedir. Artık ulusal stratejiler, saldırgan aktörlerin caydırılmasından toplumsal etkinin yönetilmesine kadar geniş bir skalada önlemleri içermekte; siber güvenlik, ulusal güvenliğin ayrılmaz bir parçası kabul edilmektedir.

Türkiye'nin son on yıldaki siber güvenlik politikalarının evrimi, siber terörizm tehdidine karşı öğrenen ve adapte olan bir yaklaşım sergilendiğini ortaya koymaktadır. İlk dönemde farkındalık oluşturma ve koordinasyon sağlama hedeflenmiş, ikinci aşamada kurumsal kapasite ve uluslararası işbirliği geliştirilmiş, son aşamada ise merkezi ve kapsamlı bir stratejiye geçilmiştir. Bu dönüşümün ardındaki itici gücün doğrudan yaşanan saldırı deneyimleri olduğunu göstermektedir. Her önemli siber olay, politika cephesinde bir karşılık bulmuş; ya yeni bir düzenlemeye ya da mevcut yapının revizyonuna yol açmıştır. Bu uyarlanabilirlik, siber tehditlerin dinamik doğası göz önünde bulundurulduğunda, Türkiye'ye önemli bir esneklik kazandırmaktadır. Bununla birlikte politikaların uygulanmasında ve kurumlar arası eşgüdümde sürekliliğin sağlanması, tıpkı kuramsal modelin önerdiği gibi, bütüncül yaklaşımın sürdürülmesiyle mümkün olacaktır. Türkiye örneği, siber terörizm gibi karmaşık bir tehditle mücadelenin, strateji ve politika düzeyinde sürekli güncellenen, proaktif bir duruş gerektirdiğini açıkça ortaya koymaktadır.

Siber terörizmin sınır aşan ve küresel doğası, bu tehditle mücadelede uluslararası işbirliğini zorunlu kılmaktadır. Hiçbir ülke, tamamen uluslararası bağlantılardan bağımsız bir siber güvenlik stratejisiyle başarılı olamaz. Zira siber saldırılar coğrafi sınır tanımamakta ve çoğu zaman bir ülkede başlayan bir saldırı başka ülkelerdeki altyapıları da etkileyebilmektedir. Bu gerçek, bu tez çalışmasında kendini göstermektedir. Türkiye'ye yönelik siber terör eylemlerinin önemli bir kısmı, yurt dışı kaynaklı IP adreslerinden gelmekte veya küresel hacker ağlarının parçası olan gruplar tarafından üstlenilmektedir. Örneğin, 2015'teki Anonymous saldırısı doğrudan uluslararası bir aktörün eylemi idi ve Türkiye tek başına bu ağı durdurmakta

zorlandı. Bu gibi vakalar, uluslararası düzeyde anlık bilgi paylaşımı, ortak savunma ve suçluların takibi konusunda işbirliğinin önemini ortaya koymaktadır. Türkiye, son on yılda uluslararası siber güvenlik camiasına giderek daha entegre bir yaklaşım sergilemiştir. Ülkemiz 2010'ların başında Budapeşte Siber Suçlar Sözleşmesi'ne taraf olarak, siber suçlarla (ve dolaylı olarak siber terörizmle) mücadelede temel bir hukuki işbirliği zemini yaratmıştır. Bu sözleşme, üye ülkeler arasında bilgi paylaşımı, adli yardımlaşma ve iade konularında mekanizmalar sunmakta olup, Türkiye de bu mekanizmaları çeşitli vakalarda kullanmıştır. Özellikle uluslararası yakalama kararı çıkartılması gereken siber suçluların iadesi veya delil toplanması gerektiğinde, Budapeşte Sözleşmesi'nin sağladığı çerçeve devreye girmiştir. Bununla birlikte Ghernaouti-Hélie (2010), tarafından ifade edildiği üzere, sözleşmenin kapsamı siber terörizmin tüm boyutlarını kapsamakta yetersiz kalabilmektedir. Zira devlet destekli saldırılar veya açıkça terör amacı güden dijital sabotajlar gibi konular, bu sözleşmenin hazırladığı dönemde öngörülen siber suç tanımlarının dışında kalabilmektedir.Bu nedenle Türkiye uluslararası hukuk açısından mevcut araçları kullansa da pratikte bunların bazen eksik kaldığı durumlarla karşılaşmaktadır.

Türkiye'nin uluslararası işbirliği boyutundaki performansı, NATO ve Birleşmiş Milletler gibi çok taraflı platformlardaki etkinliğinde de görülmektedir. NATO bağlamında, üye ülkeler arasında siber savunma konusunda kolektif bir güvenlik anlayışı geliştirilmeye çalışılmaktadır. Türkiye, bir NATO üyesi olarak ittifakın siber tatbikatlarına (örn. Locked Shields gibi) düzenli katılım sağlamakta ve müttefiklerle ortak savunma planlamaları yapmaktadır. 2014 Galler Zirvesi'nde NATO'nun siber saldırıları 5. madde kapsamında değerlendirebileceğini açıklaması sonrasında, Türkiye de ulusal stratejilerini bu kolektif savunma doktrinine uyumlu hale getirmiştir. 2019'da Milli Savunma Üniversitesinde kurulan Siber Güvenlik Mükemmeliyet Merkezi, hem NATO konseptlerine uygun eğitimler vermekte hem de müttefiklerle bilgi paylaşımına katkı sunmaktadır. Bir diğer işbirliği cephesi de Avrupa Birliği ile yürütülen çalışmalardır. Her ne kadar Türkiye AB üyesi olmasa da siber güvenlik alanında ENISA (Avrupa Birliği Siber Güvenlik Ajansı) ve benzeri kurumlarla ilişkiler geliştirilmiştir. Özellikle kritik altyapıların korunması ve CERT ekipleri arasındaki iletişim konusunda AB standartları takip edilmektedir. Türkiye'nin 2020 sonrasında AB'nin NIS (Network and Information Security) Direktifi ilkelerini kendi düzenlemelerine entegre etmeye başladığını, böylece bölgesel düzeyde de uyum sağlandığını göstermektedir. Birleşmiş Milletler nezdinde ise Türkiye, BM Genel Kurulu bünyesinde siber güvenlikle ilgili çalışmalar yapan Açık Uçlu Çalışma Grubu (OEWG) ve Hükümet Uzmanları Grubu (GGE) tartışmalarına katılarak, küresel normların şekillendirilmesine katkıda bulunmaktadır. Bu platformlarda Türkiye'nin temel vurgusu, siber uzayın barışçıl kullanımı, devletlerin egemenlik haklarına

saygı ve terörist faaliyetlerin dijital mecrada da engellenmesi yönündedir. Tikk-Ringalar (2015), siber terörizmle mücadelede uluslararası işbirliğinin, saldırı faillerinin tespiti ve adalet önüne çıkarılması hususunda kritik önem taşıdığını belirtmiştir.

Türkiye'nin pratik deneyimleri de bu görüşü destekler niteliktedir. Özellikle sınır ötesi operasyonel işbirliği olmadan, siber saldırıları gerçekleştiren grupların yakalanması veya etkisiz hale getirilmesi çoğunlukla mümkün olamamaktadır. Bu bağlamda ülkemiz, INTERPOL'ün siber suç birimi ile yakın temaslar kurmuş, çeşitli siber suç operasyonlarına ortak olmuştur. Örneğin, 2021 yılında gerçekleştirilen ve uluslararası bir dolandırıcılık/siber saldırı şebekesinin çökertildiği operasyon, Türk emniyet birimlerinin Europol ve FBI ile koordinasyon içinde çalışmasının başarılı bir örneğidir. Bu tür örnekler, sınır ötesi dayanışmanın somut faydalarını ortaya koyarken, işbirliğinin sürekliliğinin önemini de göstermektedir.

Her ne kadar Türkiye uluslararası işbirliği konusunda önemli adımlar atmış olsa da karşılaşılan zorluklar ve eksiklikler de mevcuttur. Araştırma bulgularımız ve literatür, uluslararası işbirliğinin önünde hem teknik hem de hukuki engeller bulunduğunu işaret etmektedir. Öncelikle farklı ülkelerin siber terörizm ve siber suç tanımlarındaki uyumsuzluklar, ortak hareket etmeyi güçleştirmektedir. Brenner (2010), mevcut uluslararası hukuk düzeninin siber terörizmi açık biçimde tanımlamakta yetersiz kaldığını ve devletler arasında ortak bir normlar rejimi oluşturulmasını zorlaştırdığını vurgulamaktadır.

Bu durum Türkiye'nin de maruz kaldığı bir problemdir. Örneğin, Türkiye'de kritik altyapıya saldırı terör suçu kategorisinde ele alınabilirken, başka bir ülkede bu eylem organize siber suç kapsamında değerlendirilebilmektedir. Sonuç olarak, saldırganın iadesi veya yargılanması gibi süreçlerde suçun tanımı konusundaki farklılıklar işbirliğini sekteye uğratabilir. Bir başka engel, yargı yetkisi ve delil toplama konularında ortaya çıkmaktadır. Bir siber terör eyleminin dijital izleri birden fazla ülkede dağılmış halde bulunabilir; sunucular farklı ülkelerde, saldırganlar başka bir ülkede ikamet ediyor olabilir. Bu durum da her bir ülkede ayrı hukuk prosedürlerinin işlemesi gerekir ki bu da çok zaman alan ve karmaşık bir süreçtir. Örneğin, Türkiye'de gerçekleşen bir banka sistemine sızma olayının failinin Avrupa'da bulunması halinde, delillerin toplanması ve failin yakalanması için aylarca süren yazışmalar ve hukuki süreçler gerekebilmektedir. Bu tür gecikmeler caydırıcılık etkisini azaltmakta ve saldırganların yakalanma ihtimalinin düşüklüğü nedeniyle siber terör eylemlerine girişme kararını kolaylaştırabilmektedir. Literatürde, ortak bir uluslararası siber güvenlik standartları ve tanımları setinin eksikliği sıkça dile getirilir. Türkiye'nin yaşadığı deneyimler de bu tespiti doğrular mahiyettedir. Özellikle devlet destekli olduğu düşünülen saldırılar söz konusu

olduğunda, uluslararası işbirliği neredeyse imkânsız hale gelebilmektedir. Zira saldırının kaynağı olarak görülen ülke, bu faaliyetleri resmen üstlenmediği gibi soruşturulmasına da izin vermemektedir. Bu, uluslararası siyasetin siber işbirliği önünde bazen aşılmaz bir engel oluşturduğunu gösterir. Örneğin, 2020'de Türk devlet kurumlarını hedef alan bir dizi gelişmiş siber casusluk kampanyasının arkasında yabancı bir istihbarat yapılanmasının olduğuna dair şüpheler oluşmuş, ancak diplomatik ilişkiler gözetilerek bu konuda alenî bir suçlama getirilememiştir. Bu durumda Türkiye, uluslararası platformlarda meseleyi gündeme getirmek yerine iç savunma mekanizmalarını güçlendirmeye odaklanmıştır. Bu tür örnekler, uluslararası düzeydeki güç politikasının siber terörizmle mücadelede işbirliği ruhunu zaman zaman gölgeleyebildiğini göstermektedir.

Bununla birlikte Türkiye'nin uluslararası işbirliği kapasitesini artırma yönünde atabileceği adımlar da bulunmaktadır. Türkiye'nin halihazırda dahil olduğu mekanizmalardan (NATO, BM, INTERPOL vb.) daha etkin faydalanması gerektiğini ortaya koymaktadır. Örneğin, NATO içindeki istihbarat paylaşım ağlarında siber tehdide ilişkin daha fazla veri alışverişi yapmak, müttefiklerin tecrübelerinden yararlanmak ve ortak tatbikat sayısını artırmak Türkiye'nin kapasitesini yükseltecektir. Keza, bölgesel ölçekte; örneğin Orta Doğu ve Avrasya ülkeleriyle siber olaylara müdahale konusunda ikili veya çoklu anlaşmalar geliştirmek de sınır ötesi tehditlere karşı komşu ülkelerle dayanışma ortamı yaratabilir. Türkiye, coğrafi konumu itibarıyla birden fazla bölgesel örgütün (Avrupa Konseyi, AGİT, Şangay İşbirliği Örgütü gibi) etki alanına dahildir ve bu çeşitlilik, farklı platformlarda siber güvenlik inisiyatifleri geliştirmek için bir fırsat sunar. Örneğin, Avrasya bölgesindeki bazı ülkelerle siber suçlar konusunda ortak eğitim programları veya bilgi paylaşım anlaşmaları yapmak, Türkiye'ye hem teknik kapasite kazandıracak hem de olası saldırı kaynaklarına yakın temasta bulunma imkânı sağlayacaktır. Uluslararası işbirliği boyutu, siber terörizmle mücadelenin belki de en karmaşık fakat en kritik yanını oluşturmaktadır. Türkiye'nin bu alandaki mevcut çabaları kayda değerdir ancak sürekli geliştirilmesi gereken bir alandır. Literatürde ve bulgularımızda altı çizildiği üzere, küresel işbirliği olmadan ulusal çabalar eksik kalacak; bu da saldırganların hareket alanını geniş tutmaya devam edecektir. Türkiye, kendi güvenliği için olduğu kadar bölgesel ve küresel dijital güvenliğin tesisi için de uluslararası işbirliği mekanizmalarını güçlendirmeye ve yenilikçi çözüm arayışlarına öncülük etmeye devam etmelidir.

SONUÇ VE ÖNERİLER

Bu tez çalışmasında, siber terörizm olgusu Türkiye özelinde ele alınmış; 2015–2025 yılları arasında gerçekleşen vakalar üzerinden, bu eylemlerin kapsamı, motivasyonu, hedefleri ve etkileri analiz edilmiştir. Çalışmanın kuramsal çerçevesi olarak Plotnek and Slay (2021)'ın altı bileşenli taksonomisi benimsenmiş ve elde edilen bulgular bu model doğrultusunda değerlendirilmiştir. Analizler, Türkiye'de siber terörizm eylemlerinin karmaşık, çok aktörlü ve giderek artan bir boyuta ulaştığını ortaya koymuştur. Söz konusu saldırıların çoğunda belirli bir ideolojik ya da politik güdüyle hareket edildiği, kritik altyapıların (özellikle enerji ve sağlık sektörlerinin) sistematik biçimde hedef alındığı ve bu saldırıların toplumsal düzeyde ciddi etkiler yarattığı tespit edilmiştir.

Türkiye örneği, siber terörizmin yalnızca teknik bir güvenlik sorunu olmadığını; aynı zamanda toplumsal, siyasal ve jeopolitik boyutları bulunan çok katmanlı bir tehdit alanı olduğunu göstermektedir. Çalışmanın bulguları, Türkiye'nin siber tehditlere karşı zamanla daha kurumsallaşmış, merkezi ve stratejik bir güvenlik politikası geliştirdiğini ortaya koymaktadır. Özellikle 2025 yılında yürürlüğe giren 7545 sayılı Siber Güvenlik Kanunu ve bu kanunla kurulan Siber Güvenlik Başkanlığı, Türkiye'nin bu alandaki yönetişim kapasitesini güçlendirmiştir. Bu politik gelişmelere karşın, siber terörizm tehdidinin dinamik doğası, güvenlik stratejilerinin sürekli güncellenmesini ve çok paydaşlı bir mücadele anlayışının benimsenmesini zorunlu kılmaktadır.

Bu tez çalışmasının bulgularına ve analizlerine dayalı olarak aşağıdaki politika ve strateji önerileri sunabiliriz.

1. **Kritik Altyapıların Güvenliği Öncelikli Hale Getirilmelidir:** Enerji, sağlık, finans ve ulaştırma gibi sektörler, siber teröristlerin öncelikli hedefleri arasında yer almaktadır. Bu alanlarda faaliyet gösteren kamu ve özel sektör kuruluşları için zorunlu siber güvenlik standartları belirlenmeli; düzenli denetim, tatbikat ve simülasyon süreçleri kurumsallaştırılmalıdır.
2. **Siber Tehdit İstihbaratı Geliştirilmelidir:** Siber teröristlerin kimliklerinin tespiti ve motivasyonlarının anlaşılması, etkili bir mücadele için elzemdir. Bu kapsamda, siber istihbarat alanında hem teknik kapasite hem de insan kaynağı bakımından nitelikli gelişim sağlanmalıdır. Açık ve insan kaynağı isithbaratı, makine öğrenimi ve tehdit analitiği gibi ileri düzey teknolojiler bu alana entegre edilmelidir.

3. **Toplumsal Farkındalık ve Dijital Okuryazarlık Artırılmalıdır:** Siber terörizm yalnızca teknik altyapıya değil, toplumun psikolojik direncine de yöneliktir. Bu nedenle, kamuoyunun siber tehditlere karşı bilinç düzeyinin artırılması, dezenformasyonla mücadele kapasitesinin güçlendirilmesi ve medya okuryazarlığının teşvik edilmesi gerekmektedir. Eğitim kurumlarında siber güvenlik farkındalığına yönelik müfredat geliştirilmesi önemlidir.
4. **Uluslararası İşbirlikleri Derinleştirilmelidir:** Siber terörizmin sınır aşan niteliği göz önünde bulundurulduğunda, Türkiye'nin NATO, INTERPOL ve Budapeşte Siber Suçlar Sözleşmesi gibi uluslararası mekanizmalarla daha etkin işbirlikleri geliştirmesi elzemdir. Özellikle siber tehdit istihbaratının paylaşımı, ortak tatbikatlar ve adli yardımlaşma konularında ikili ve çok taraflı ilişkiler güçlendirilmelidir.
5. **Hukuki ve Stratejik Çerçeve Güncel Tutulmalıdır:** Teknolojik gelişmeler doğrultusunda ortaya çıkan yeni tehdit türleri (örneğin yapay zekâ destekli saldırılar, nesnelerin interneti açık kaynakları vb.) mevcut mevzuatın ötesinde düzenleme gerektirmektedir. Bu nedenle, Siber Güvenlik Kanunu ve ilgili ikincil mevzuat, periyodik olarak gözden geçirilmeli ve yeni gelişmelere hızla uyum sağlayacak biçimde esnekleştirilmelidir.
6. **Akademik Araştırmalar Teşvik Edilmelidir:** Siber terörizmin karmaşık doğası, farklı disiplinlerin işbirliğini zorunlu kılmaktadır. Bu nedenle hukuk, siyaset bilimi, uluslararası ilişkiler ve bilişim gibi alanlarda disiplinlerarası çalışmalar desteklenmeli; kamu kurumları ile akademi arasında bilgi paylaşımı ve veri erişimi kolaylaştırılmalıdır.

Sonuç olarak, Türkiye'nin siber terörizmle mücadelesi, yalnızca ulusal güvenlik açısından değil; aynı zamanda demokratik istikrar, toplumsal direnç ve uluslararası güvenlik ortamı açısından da stratejik bir öneme sahiptir. Bu tehdit türünün doğası gereği sürekli dönüşen ve yeni biçimlerde ortaya çıkan yapısı, siber güvenliğin teknik kapasitenin ötesine geçerek yönetişim, hukuk, etik ve toplumla bütünleşik bir perspektifle ele alınmasını gerekli kılmaktadır. Bu çalışma, Türkiye örneği üzerinden hem kuramsal hem de uygulamalı düzeyde bu ihtiyacın altını çizmektedir.

KAYNAKLAR

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

Akbaş, H. (2018). Türkiye'de Siber Güvenlik ve Siber Terörizm. İstanbul: Beta Yayınları.

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

Anadolu Ajansı (2015 22 Nisan) Haber Sitesi

Atasever, S., Özçelik, İ., ve Sağıroğlu, Ş. (2019). Siber Terör ve DDoS. Journal of Natural and Applied Sciences, 23(1).

Avrupa Birliği (2016) Ağ ve Bilgi Güvenliği Yönergesi.

Avrupa Birliği (2019) Siber Güvenlik Yasası

Avrupa Konseyi (2001) Budapeşte Siber Suç Sözleşmesi.

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

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

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

Brenner, S. W. (2010). Cybercrime and the Law: Challenges and Opportunities. Springer.

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

Chesney, R. (2017). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.

Cohen, H. (2020). Encryption and Its Role in Cyber Attacks. International Journal of Cybersecurity and Privacy.

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

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

Çakır İ. ve Yıldırım Y. (2022) Türkiye'nin Siber Tehdit Ortamı ve Bölgesel Rekabet. Akademik Strateji Makalesi.

Çelik, B. (2019). Siber Güvenlik ve Uluslararası İşbirlikleri. Siber Güvenlik ve Uluslararası Politikalar Dergisi.

Çelik, R. (2021). Siber Terörle Mücadelede Türkiye'nin Uluslararası İşbirliği. Uluslararası Güvenlik Araştırmaları Dergisi, 6(3), 115-130.

Demirtaş, N. (2019). Siber Saldırıların Ekonomik Yansımaları ve Türkiye'deki Durum. Ekonomi ve Güvenlik Dergisi.

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

Denning, D. E. (2000). Information Warfare and Security. Addison-Wesley.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. In J.

Diken (2015 24 Aralık) Haber Sitesi

Ekinci, S. (2018). Siber Saldırıların Ulusal Güvenlikteki Yeri ve Türkiye. İstanbul: Bilgi Üniversitesi Yayınları.

ELDER – Elektrik Dağıtım Hizmetleri Derneği. (2017). ELDER E-Bülten Sayı 22 – Haziran 2017.https://www.elder.org.tr/ebulten/issue22.html

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

Emniyet Genel Müdürlüğü (2021) İdare Faaliyet Raporu.

ENISA. (2020). European Cybersecurity Policy and Strategy. European Union Agency for Cybersecurity.

Erdem, R. (2018). Türkiye'de Siber Güvenlik ve Kamu Kurumları Üzerindeki Tehditler. Siber Güvenlik Araştırma Dergisi.

Euronews (2015 10 Temmuz) Haber Sitesi

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

Gallagher, D. (2014). Sony Hackers Leak Personal Data and Emails. The Guardian.

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

Ghernaouti-Hélie, Solange. (2010). Cyberpower: Crime, Conflict and Security in Cyberspace. EPFL Press.

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

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

Goodin, D. (2012). Hackers launch massive attack on US banks. The Register.

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

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

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

Güler, F. (2019). Dijital Çağda Siber Tehditler ve Uluslararası Güvenlik. Ankara: Nobel Yayınları.

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

Hassan, S., and Chen, H. (2020). Cybersecurity in Critical Infrastructure Protection: A Systematic Review. Springer.

Hathaway, O. A. (2014). The Cybersecurity Dilemma: Hacking, Deterrence, and International Law. Oxford University Press.

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

Hussain, S. (2021). AI and Machine Learning in Cyber Security. Cyber Security and Technologies Journal.

Iftikhar (2024) Cyber Terrorism as a global threat: a review on repercussions and countermeasures. PeerJ Combuter Science, Cilt 10

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

Kaspersky. (2016). Mirai Botnet and DDoS Attacks. Kaspersky Labs.

Kılınç, M. (2020). Siber Saldırıların Uluslararası İlişkiler Üzerindeki Etkisi. Uluslararası İlişkiler ve Güvenlik Araştırmaları.

Kızılkaya, N. (2021). Siber Suçlar ve Terörle Mücadele. Ceza Hukuku ve Kriminoloji Dergisi, 5(2), 75-89.

Kocatepe, B. (2017). Türkiye'deki Büyük Siber Saldırılar ve Ulusal Güvenlik. Journal of Turkish Security Studies.

Kriter Dergi. (2016). FETÖ Siber Güvenliği de Hedef Aldı. Kriter Dergi. Erişim adresi: https://kriterdergi.com/siyaset/feto-siber-guvenligi-de-hedef-aldi

Libicki, M. C. (2007). Conquest in Cyberspace: National Security and Information Warfare. Cambridge University Press.

Liu, J. (2020). Cyber Terrorism and International Law: The Need for Global Cooperation. International Cyber Security Law Journal.

Liu, Y. (2020). Cloud Computing and Cybersecurity Risks. Cloud Computing and Cybersecurity Review.

Marquardt, A., Levenson, E.,Tal, A. (2021). Florida water treatment facility hack used a dormant remote access software, sheriff says. *CNN*.

https://abc17news.com/news/national-world/2021/02/10/florida-water-treatmentfacility-hack-used-a-dormant-remote-access-software-sheriff-says/

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

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

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

NATO Cooperative Cyber Defence Centre of Excellence. (2007). Cyber Attacks and National Security: A Case Study of Turkey. Estonia: NATO.

NATO. (2018). NATO Cyber Defence Policy. NATO Communications and Information Agency.

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

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

Özdemir, B. (2020). Türkiye'nin Siber Güvenlik Stratejileri. Journal of National Defense, 12(3), 100-115.

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

Resül, Y. (2020). Türkiye'nin Siber Güvenlik Sorunları. Akademik Akıl Dergisi, 4(1), 45-55.

Rid, T., and Buchanan, B. (2015). Attributing Cyber Attacks. Journal of Strategic Studies, 38(1-2), 4–37.

Sarı, B. (2017). Siber Terörizm ve Kamu Güvenliği Üzerindeki Etkileri. Ankara Üniversitesi Hukuk Fakültesi Dergisi.

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

Shackelford, S. (2014). International Law and the Global Cybersecurity Crisis. Cambridge University Press.

Shalaby, H. (2017). WannaCry Ransomware Attacks on Windows Systems: A Case Study. Springer.

Sullivan, B. (2020). The SolarWinds Hack: A National Security Crisis. The Wall Street Journal.

Symantec. (2011). Stuxnet: A New Era of Cyber Warfare. Symantec Corporation. T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2021). Ulusal Siber Güvenlik Stratejisi ve Eylem Planı.

T.C. İçişleri Bakanlığı. (2019). Türkiye'de Siber Güvenlik ve Terörizm Raporu. Ankara: İçişleri Bakanlığı Yayınları.

T.C. Resmî Gazete (2024) Cumhurbaşkanlığı Genelgesi 2024/11

T.C. Resmî Gazete (2025) 7545 sayılı Siber Güvenlik Kanunu

Tafoya, W. L. (2011). Cyber terror. FBI Law Enforcement Bulletin,

TASAM. (2024). Türkiye Siber Güvenlik Forumu 2023: Yeni Siber Ekonomi ve Türk Ürünleri. İstanbul: TASAM Yayınları.

Tikk, E., Kaska, K., Vihul, L. (2008). Cyber Attacks Against Estonia: Legal, Strategic, and Policy Lessons. NATO Cooperative Cyber Defence Centre of Excellence.

Tolk, A., and Diallo, S. Y. (2019). Modeling and Simulation Support for System of Systems Engineering Applications. Wiley.

Tosoff, S. (2016). Cyber Attacks and Energy Infrastructure: The Case of Ukraine. International Journal of Cyber Security.

Türkiye Siber Güvenlik Kümelenmesi. (2020). Siber Tehditler ve Ulusal Politika. İstanbul: Türkiye Bilişim Derneği Yayınları.

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

Uzman Posta (2023) Türkiye'de Kritik Altyapıya Yönelik Siber Saldırı İddiası İnceleme (İnternet Haberi)

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

Weimann, G. (2016). Cyber Terrorism: The Challenge of the New Threat. Journal of International Security Studies, 5(1), 23-36.

Weimann, G. (2016). The Globalization of Cyber Terrorism. International Journal of Cyber Warfare and Terrorism.

Yılmaz, M. ve Karakaş, Z. (2020). Siber Tehditler: Türkiye'nin Hukuki ve Politik Yaklaşımları. Cybersecurity Journal, 5(2), 45-65.

Yüksel, M. (2011). Siber Savaşlar ve Siber Güvenlik. Türkiye Bilişim Derneği.

Zeng, M. (2019). The Role of Social Media in Cyber Terrorism. Journal of Digital Security.

Zetter, K. (2015). Ukrainian Power Grid Hacked in Suspected Russian Attack. Wired.

ÖZGEÇMİŞ

Kişisel Bilgiler
Adı Soyadı: Mücahit ERGÜN **Doğum tarihi:** **Doğum Yeri:** **Uyruğu:** **Adres:** **Tel:** **E-mail:**
Eğitim
Lise: **Lisans:** **Yüksek lisans:** **Doktora:**
Yabancı Dil Bilgisi
Üye Olunan Mesleki Kuruluşlar
Tezden Üretilmiş Yayınlar
Journal of International Relations Studies / 2024 4(2): 64-73 / DOI: 10.62425/jirs.1589559