



**T.C.
YALOVA ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ**

**ULUSLARARASI İLİŞKİLER ANABİLİM DALI
ULUSLARARASI İLİŞKİLER BİLİM DALI**

**SİBER GÜVENLİĞİN KÜRESEL YÖNETİŞİMİNDE BİR AKTÖR OLARAK
KOLLUK KUVVETLERİ: TÜRKİYE, FRANSA VE ABD ÖRNEKLERİ**

YÜKSEK LİSANS TEZİ

ŞEYDA ERTÜRK

DANIŞMAN: DOÇ. DR. ÖVGÜ KALKAN KÜÇÜKSOLAK

**YALOVA
ŞUBAT 2025**



T.C.
YALOVA ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER ANABİLİM DALI
ULUSLARARASI İLİŞKİLER BİLİM DALI

SİBER GÜVENLİĞİN KÜRESEL YÖNETİŞİMİNDE BİR AKTÖR OLARAK KOLLUK
KUVVETLERİ: TÜRKİYE, FRANSA VE ABD ÖRNEKLERİ

YÜKSEK LİSANS TEZİ

ŞEYDA ERTÜRK
218131023

DANIŞMAN: DOÇ.DR. ÖVGÜ KALKAN KÜÇÜKSOLAK

YALOVA
ŞUBAT 2025

ETİK BEYAN

Yalova Üniversitesi Lisansüstü Eğitim Enstitüsü Tez/Proje Yazım Kuralları'na uygun olarak hazırladığım “SİBER GÜVENLİĞİN KÜRESEL YÖNETİŞİMİNDE BİR AKTÖR OLARAK KOLLUK KUVVETLERİ: TÜRKİYE, FRANSA VE ABD ÖRNEKLERİ” başlıklı bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu bildirir, aksinin tespiti halinde doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi taahhüt ve beyan ederim.

ŞEYDA ERTÜRK



ÖNSÖZ

Yüksek lisans eğitimim boyunca benden yardımlarını esirgemeyen, akademik anlamda bana her zaman destek olan ve doğru yolu gösteren sayın danışman hocam Doç. Dr. Övgü KALKAN KÜÇÜKSOLAK'a teşekkür ederim. Her zaman yanımda olan, nikahımızdan çıkıp şehirlerarası yolculukla beni yüksek lisans dersimin sınavına yetiştiren kıymetli eşim Seydi Ahmet ERTÜRK'e ve yalnız yüksek lisans değil bütün eğitim hayatım boyunca beni her anlamda destekleyen biricik ablam Gülizar TOPDEMİR'e ve benden desteklerini hiçbir zaman esirgemedikleri için aileme ve arkadaşlarıma teşekkür ederim.

Şubat– 2025

Şeyda ERTÜRK



İÇİNDEKİLER

ETİK BEYAN	i
ÖNSÖZ.....	ii
İÇİNDEKİLER.....	iii
KISALTMALAR LİSTESİ.....	v
TABLolar LİSTESİ	vi
ÖZET	vii
ABSTRACT	viii
1. GİRİŞ	1
1.1. Tez Çalışmasının Amacı.....	2
1.2. Tez Çalışmasının Literatüre Katkısı	3
1.3. Çalışmanın Yöntemi ve Teknikleri.....	3
1.4. Literatür İncelemesi	4
2. TEORİK VE TARİHSEL ÇERÇEVEDE SİBER GÜVENLİK VE KÜRESEL YÖNETİŞİM KAVRAMLARI.....	7
2.1. Siber Güvenlik Kavramının Gelişimi ve Önemi	7
2.2. Kopenhag Ekolü Çerçevesinde Siber Güvenlik	14
2.3. Küresel Yönetişim Kavramı ve Siber Güvenlik	19
3. SİBER GÜVENLİK ve KOLLUK İLİŞKİSİ.....	23
3.1. Siber Suç Nedir?	24
3.2. Siber Suçlarla Mücadelede Kolluk Kuvvetlerinin Rolü ve Karşılaştıkları Sorunlar	25
3.3. Küresel Siber Güvenlik Endeksi ve Kolluk Kuvvetlerinin Rolü.....	27
3.4. Kamu Kurumlarının Kurumsal Siber Güvenliği	30
4. TÜRKİYE’DE KOLLUĞUN SİBER GÜVENLİK YÖNETİŞİMİ	33
4.1. Türkiye’de Kolluk Yapılanması	33
4.2. Türkiye’nin Kolluk Teşkilatlarında Siber Güvenliğin Yeri ve Geliştirilen Stratejiler .	35
4.3. Uluslararası İş birliği Örnekleri ve Küresel Yönetişime Katkısı.....	41
4.4. Küresel Siber Güvenlik Endeksinde Türkiye'nin Yeri ve Kolluk Kuvvetlerinin Etkisi	44
5. FRANSA’DA KOLLUĞUN SİBER GÜVENLİK YÖNETİŞİMİ	47
5.1. Fransa’da Kolluk Yapılanması	48
5.2. Fransa’nın Kolluk Teşkilatlarında Siber Güvenliğin Yeri ve Geliştirilen Stratejiler ...	49
5.3. Uluslararası İş birliği Örnekleri ve Küresel Yönetişime Katkısı.....	54
5.4. Küresel Siber Güvenlik Endeksinde Fransa’nın Yeri ve Kolluk Kuvvetlerinin Etkisi	55
6. ABD’DE KOLLUĞUN SİBER GÜVENLİK YÖNETİŞİMİ	57
6.1. ABD’de Kolluk Yapılanması	59

6.2. ABD’nin Kolluk Teşkilatlarında Siber Güvenliğin Yeri ve Geliştirilen Stratejiler	61
6.3. Uluslararası İş birliği Örnekleri ve Küresel Yönetişime Katkısı.....	63
6.4. Küresel Siber Güvenlik Endeksinde ABD’nin Konumu ve Kolluk Kuvvetlerinin Etkisi	65
7. SONUÇLAR VE ÖNERİLER	67
KAYNAKLAR.....	73
ÖZGEÇMİŞ	83



KISALTMALAR LİSTESİ

ANSSI	: Ulusal Bilgi Sistemleri Güvenliği Ajansı
APEC	: Asya-Pasifik Ekonomik İş birliği
BM	: Birleşmiş Milletler
C3N	: Fransa Jandarma Siber Suçlarla Mücadele Birimi
CAT	: Siber Eylem Timi
CERT	: Bilgisayar Acil Müdahale Ekibi
CCDCOE	: Siber Savunma Mükemmeliyet Merkezi
CFAA	: Dolandırıcılık ve Kötüye Kullanım Yasası
DHS	: ABD İç Güvenlik Bakanlığı
DJPJ	: Adli Polis Merkez Müdürlüğü
EGM	: Emniyet Genel Müdürlüğü
ENISA	: Avrupa Birliği Siber Güvenlik Ajansı
EUROPOL	: Avrupa Polis Teşkilatı
FBI	: Federal Soruşturma Bürosu
FCC	: Federal İletişim Komisyonu
FISMA	: ABD Federal Bilgi Güvenliği Modernizasyonu Yasası
FiEP	: Uluslararası Jandarmalar ve Askeri Statülü Kolluk Kuvvetleri Birliği
GCI	: Küresel Siber Güvenlik Endeksi
GDPR	: Avrupa Birliği Genel Veri Koruma Yönetmeliği
HSIN	: Güvenlik Bilgi Ağı
IC3	: İnternet Suçları Şikâyet Merkezi
INTERPOL	: Uluslararası Kriminal Polis Teşkilatı
ITU GCA	: Uluslararası Telekomünikasyon Birliği Küresel Güvenlik Ajansı
ITU	: Uluslararası Telekomünikasyon Birliği
LCEN	: Dijital Ekonomide Güven Yasası
NATO	: Kuzey Atlantik Antlaşması Teşkilatı
NIST	: Siber Güvenlik Çerçevesi
NYPD	: New York Polis Departmanı
OECD	: Ekonomik İş Birliği ve Kalkınma Örgütü
SSMDB	: Siber Suçlarla Mücadele Daire Başkanlığı
UNODC	: BM'nin Uyuşturucu ve Suç Ofisi
OCLCTIC	: Bilgi ve İletişim Teknolojileri ile İlgili Suçlarla Mücadele Merkez Ofisi

TABLÖLAR LİSTESİ

Tablo 3. 1. Küresel Siber Güvenlik Endeksinde Rol Model Ülkeler	29
Tablo 4. 1. Türkiye’de Kolluk Kuvvetlerinin Yapısı	34
Tablo 5. 1. Fransa’da Kolluk Kuvvetlerinin Yapısı.....	48
Tablo 6. 1. ABD’de Kolluk Kuvvetlerinin Yapısı	60



SİBER GÜVENLİĞİN KÜRESEL YÖNETİŞİMİNDE BİR AKTÖR OLARAK KOLLUK KUVVETLERİ: TÜRKİYE, FRANSA VE ABD ÖRNEKLERİ

ÖZET

Siber güvenlik ve yönetim kavramları uluslararası ilişkilerde yeni sayılabilecek kavramlardır. Geleneksel güvenlik kavramı küreselleşme ile büyük değişikliğe uğramış çevre güvenliği, ekonomik güvenlik, siber güvenlik gibi çeşitli güvenlik alt dalları ortaya çıkmıştır. Devletlerin yanı sıra uluslararası örgütler, sivil toplum kuruluşları, çok uluslu şirketler, alanında uzman kişiler gibi yeni aktörler uluslararası güvenlik çevresinde etkili hale gelmişlerdir. Çeşitlenen aktörler ve sorunlara getirilmeye çalışılan yeni diyalog ve çözüm mekanizmalarıyla da küresel yönetim farklı alanlarda kendini göstermiştir.

Uluslararası güvenlik çevresinin önemli bir bileşeni olarak öne çıkan siber güvenlik, asimetrik tehditleri gündeme getirmekte ve bunlarla mücadelede küresel yönetim çerçevesinde paydaşlık, çok yönlülük, iş birliği ve koordinasyon gibi konular büyük önem arz etmektedir. Siber güvenlik kapsamında ortaya çıkan çok boyutlu konuların ve sorunların çözümünde çeşitli aktörlerin gittikçe önem kazanmaya başladığı ve etkili hale gelen söz konusu aktörler arasında kolluk kuvvetlerinin de yer aldığı görülmektedir. İç güvenliği sağlamakla görevli kolluk kuvvetleri, artan siber tehditlerle mücadele edebilmek, kurumsal siber güvenliklerini sağlamak, gelişen bilgi teknolojilerinde güncel teknolojileri takip edebilmek amaçları doğrultusunda küresel boyutta çalışmalar yapmakta ve iş birliklerine dahil olmaktadır. Geleneksel nokta itibarıyla değerlendirildiğinde, internet erişiminin neredeyse bir zorunluluk halini almış olması ve karşılıklı bağımlılıkları gittikçe güçlendirmesi sebebiyle küresel toplumun, sınır aşan ve karmaşık bir yapı arz eden siber güvenlik tehditleri ile mücadelesinde küresel yönetim unsurlarının ve artan iş birliklerinin önem arz ettiği aşikardır.

Bu çalışmada, siber güvenliğin küresel yönetimi çerçevesinde kolluk kuvvetlerinin rolünün, Türkiye, Fransa ve ABD örnekleri üzerinden incelenmesi amaçlanmaktadır. Kopenhag Ekolü'nün çok boyutlu güvenlik anlayışı, çalışmanın teorik yaklaşımı olarak ele alınmıştır ve her üç ülkenin siber güvenlik uygulamalarını analiz etmek için bir temel sunmuştur. Uluslararası ilişkiler literatürünün öne çıkan konuları arasında olan Siber Güvenlik ve Küresel Yönetim kavramları bu ekol çerçevesinde incelenecek, tarihsel gelişimleri, literatürde artan önemleri çeşitlenen konular bazında ve konunun aktörü olarak kolluk kuvvetleri çerçevesinde tartışılacaktır.

Anahtar Kelimeler: Yönetişim, Siber Güvenlik, Uluslararası Güvenlik, Uluslararası İş birliği, Kolluk Kuvvetleri

LAW ENFORCEMENT AGENCIES AS AN ACTOR IN THE GLOBAL GOVERNANCE OF CYBER SECURITY: CASES OF TÜRKİYE, FRANCE AND THE USA

ABSTRACT

Cybersecurity and governance are relatively new concepts in international relations. The traditional concept of security has undergone significant changes with globalization, leading to the emergence of various security subfields such as environmental security, economic security, and cybersecurity. Alongside states, new actors such as international organizations, non-governmental organizations, multinational corporations, and experts in the field have become influential in the international security environment. With the diversification of actors and the introduction of new dialogue and solution mechanisms, global governance has manifested itself in different areas.

Cybersecurity, which stands out as a crucial component of the international security environment, brings asymmetric threats to the agenda. In combating these threats, issues such as partnership, multidimensionality, cooperation, and coordination within the framework of global governance are of great importance. The resolution of the multidimensional issues and challenges arising within the scope of cybersecurity increasingly relies on various actors, among which law enforcement agencies have gained significance. Law enforcement agencies, responsible for maintaining internal security, engage in global efforts and partnerships to combat rising cyber threats, ensure institutional cybersecurity, and stay up to date with emerging information technologies. At this point, considering the growing necessity of internet access and the increasing interdependencies it fosters, it is evident that global governance elements and expanding collaborations are crucial in the global society's fight against transnational and complex cybersecurity threats.

This study aims to examine the role of law enforcement agencies in global cybersecurity governance through the cases of Turkey, France, and the United States. The Copenhagen School's multidimensional security approach serves as the theoretical framework of this study, providing a basis for analyzing the cybersecurity practices of the three countries. Cybersecurity and global governance, which have become prominent topics in international relations literature, will be explored within the framework of this school. Their historical development, increasing significance in the literature, and the diversified issues surrounding them will be discussed, particularly in the context of law enforcement agencies as key actors in this domain.

Keywords: Governance, Cybersecurity, International Security, International Cooperation, Law Enforcement

1. GİRİŞ

Dijitalleşme süreci, dünya genelinde internetin, veri paylaşımının ve iletişimin hızla yayılmasına olanak tanımaktadır. Bu gelişmeler, pek çok fayda sağlasa da aynı zamanda siber güvenlik tehditlerinin artmasına yol açmaktadır. Siber suçlar, küresel ölçekte geniş bir tehdit alanı oluşturmakta, devletlerin ulusal güvenliğini tehdit ettiği gibi, bireylerin mahremiyetini de ihlal etmektedir (Hassan, 2019). Bu tehditlerin önlenmesinde ve güvenlik politikalarının uygulanmasında siber suçlarla mücadeleyle yönelik kolluk kuvvetlerinin rolü gittikçe daha etkin bir hal almaktadır. Son yıllarda, kolluk kuvvetlerinin siber güvenlik stratejilerine entegrasyonu, yalnızca ulusal sınırlar kapsamında değil, uluslararası iş birlikleri ve küresel siber yönetim çerçevesinde de kritik bir öneme haiz olmaktadır.

Kolluk kuvvetlerinin siber güvenlikteki rolü, dijital suçların soruşturulması ve suçluların yakalanmasının yanı sıra siber tehditlerin izlenmesi, önlenmesi ve siber güvenlik stratejilerinin geliştirilmesi alanlarında da önemli bir yer tutmaktadır. Bu bağlamda, kolluk kuvvetlerinin etkinliği, küresel siber güvenlik yönetişiminin temel taşlarından biri haline gelmektedir (Zetter, 2020). Her ne kadar siber güvenlik ulusal bir mesele olarak ele alınsa da siber suçların küresel doğası, devletlerin uluslararası iş birliklerini güçlendirmelerini ve bu iş birliklerine kolluk kuvvetlerini dahil etmelerini gerektirmektedir. Bu durum, kolluk kuvvetlerinin küresel siber güvenlik yönetişiminde önemli bir aktör olarak konumlanmasına yol açmaktadır. (Vermesan ve Friess, 2018).

Bu tez, Türkiye, Fransa ve ABD örnekleri üzerinden, siber güvenlikte kolluk kuvvetlerinin rolünü incelemeyi amaçlamaktadır. Farklı coğrafi, kültürel ve politik bağlamlarda yer alan Türkiye, Fransa ve ABD kolluk kuvvetlerinin siber güvenlikteki stratejik rollerinin nasıl geliştiğini gösteren değerli örnekler sunmaktadırlar. Türkiye, 2013 yılında kurduğu Ulusal Siber Güvenlik Kurumu (USGK) ve 2016'da oluşturduğu Siber Suçlarla Mücadele Daire Başkanlığı ile kolluk kuvvetlerinin kapasitesini güçlendirmiştir (Öztürk, 2020). Fransa, 2015 yılında kabul ettiği Siber Güvenlik Stratejisi ile kolluk kuvvetlerinin dijital alandaki etkinliğini arttırmış ve siber suçlarla mücadele alanında önemli adımlar atmıştır (Lemoine ve diğ., 2019). ABD ise, Federal Soruşturma Bürosu (FBI) ve İç Güvenlik Bakanlığı (DHS) gibi kurumlarla küresel siber suçlara karşı geniş bir iş birliği ağı kurmuş, yerel ve ulusal düzeyde siber güvenlik stratejileri geliştirmiştir (Smith, 2021).

Bu tezin teorik çerçevesi, Kopenhag Ekolü'nün genişletilmiş güvenlik anlayışı üzerine inşa edilmiştir. Kopenhag Ekolü, güvenliği sadece askeri bir mesele olarak değil, ekonomik,

çevresel, toplumsal ve siyasi boyutlarıyla çok boyutlu bir kavram olarak ele almaktadır. Bu yaklaşım, siber güvenliğin yalnızca teknik bir konu değil, aynı zamanda toplumsal güven ve iş birliğiyle çözülebilecek bir yönetim meselesi olduğuna işaret etmektedir. Çalışma, Kopenhag Ekolü'nün çok boyutlu güvenlik anlayışı çerçevesinde, kolluk kuvvetlerinin siber tehditlere müdahale yetkinliklerinin yanı sıra, toplum ve özel sektörle iş birliği içinde nasıl daha geniş bir güvenlik ekosistemi oluşturabileceğini analiz etmektedir (Waever, 1995).

Bu çalışma, Türkiye, Fransa ve ABD'nin siber güvenlik stratejileri çerçevesinde kolluk kuvvetlerinin rollerini ele alacak ve bu ülkelerin küresel siber güvenlik yönetişimine nasıl katkı sağladıklarını tartışmaktadır. Kolluk kuvvetlerinin siber suçlarla mücadeledeki önemi, yalnızca suçların çözülmesiyle sınırlı kalmayıp, uluslararası düzeydeki iş birliklerinin güçlendirilmesi, siber suçluların sınır ötesi takibi ve dijital delillerin toplanması gibi alanlarda da kendini göstermektedir (Zetter, 2020). Tez kapsamında her üç ülkenin siber güvenlik politikaları, kolluk kuvvetlerinin bu politikalar içindeki yeri ve küresel yönetişime sağladıkları katkılar karşılaştırılmakta ve bu iş birliklerinin ne yönde güçlendirilebileceği üzerine öneriler sunulmaktadır. Siber güvenliğin küresel yönetişimde kolluk kuvvetlerinin stratejik rolü, ulusal ve uluslararası düzeydeki iş birlikleri çerçevesinde farklı yönlerden analiz edilmektedir.

1.1. Tez Çalışmasının Amacı

Bu tezde, siber güvenliğin küresel yönetişiminde kolluk kuvvetlerinin rolünün Türkiye, Fransa ve ABD örnekleri üzerinden incelenmesi amaçlanmaktadır. Tez çerçevesinde cevap bulunması amaçlanan araştırma soruları şunlardır:

- Siber güvenliğin küresel yönetişiminde hangi aktörler yer almaktadır?
- Kolluk kuvvetleri siber güvenliğin küresel yönetişiminde hangi çerçevede hareket etmektedir?
- Kolluk Kuvvetlerinin siber güvenlik politikalarında hangi unsurlar belirleyici olmaktadır?
- Genişleyen güvenlik çerçevesine paralel olarak kolluk kuvvetlerinin rollerinde bir değişim yaşanmakta mıdır?
- Siber güvenliğin küresel yönetişimden hangi mülahazalar doğrultusunda uluslararası iş birlikleri gerçekleşmektedir?
- Türkiye, Fransa ve ABD'nin siber güvenlik politikalarının oluşumunda hangi unsurlar belirleyici olmaktadır?

- Türkiye, Fransa ve ABD örnekleri çerçevesinde kolluk kuvvetleri siber güvenliğin yönetiminde hangi kapsamda yer almaktadır?
- Türkiye, Fransa ve ABD örneklerinde kolluk kuvvetlerinin siber güvenlikte oynadığı rollerde ne gibi farklılıklar bulunmaktadır?
- Hangi çerçevede uluslararası iş birlikleri gerçekleşmektedir, belirleyici unsurlar nelerdir?

Yukarıdaki sorulara verilecek yanıtlar üzerinden konunun temel unsurları tartışılacak ve kolluk kuvvetlerinin farklı ülkelerdeki uygulamaları ve çeşitlenen iş birlikleri incelenecektir. Kopenhag Ekolü'nün çerçevesinde siber güvenlik kavramı açıklanacak, çeşitlenen iş birlikleri doğrultusunda siber güvenliğin küresel yönetiminde etkili olan faktörler irdelenecek ve özellikle de Türkiye'nin eksik noktalara işaret edilecektir.

1.2. Tez Çalışmasının Literatüre Katkısı

Kolluk Teşkilatları açısından değerlendirildiğinde, siber güvenliğin küresel yönetimi hem kurumsal teşkilatların siber tehditlerden korunması hem de siber suçlarla mücadelede artan iş birlikleri açısından önem arz etmektedir. Bu tezde Kopenhag Ekolü'nün genişleyen güvenlik anlayışı kapsamında siber güvenlik kavramı gelişimi açıklanmakta, çok paydaşlı yapının önemi vurgulanmakta ve küresel yönetimin siber güvenlik alanındaki uygulanabilirliği ve Türkiye, Fransa ve ABD tarafından ortaya konan katkıları irdelenmektedir. Kolluk kuvvetlerinin farklı ülkelerdeki uygulamaları kapsamında küresel siber güvenlik yönetiminde yükselen rolü iş birliklerindeki eksiklikler, olumlu gelişmeler ve etkili unsurlar ortaya konarak geleceğe yönelik projeksiyon yapılmasına ve böylelikle literatüre katkı sağlanmasına çalışılmaktadır.

1.3. Çalışmanın Yöntemi ve Teknikleri

Bu çalışmada siber güvenlik politikalarının artan önemi ve kamu-özel sektör iş birliklerinin bu süreçte hangi etkenler çerçevesinde önem kazandığı Kopenhag Ekolü ve yönetim perspektifinden incelenmektedir. Realist yaklaşımın devlet politikalarıyla sınırlı kalan güvenlik yaklaşımı karşısında Kopenhag Ekolü'nün güvenliğin değişen yapısının açıklanmasındaki işlevselliğinden yararlanılmaktadır. Kopenhag Ekolü'nün genişletilmiş güvenlik kavramı kapsamında siber alanda çeşitlenen güvenlik tehditleri ile aktörlerin önemi vurgulanmakta ve yönetim kavramı çerçevesinde siber tehditlerin karşısında oluşturulması gereken çok paydaşlı yapının unsurlarının altı çizilmektedir.

Bu çalışmanın yazımı sırasında birincil ve ikincil kaynaklardan bilgi toplama tekniği uygulanmış, analitik yorumlar yapılarak bu üç devletin siber alanda şekillendirdikleri güvenlik politikaları küresel yönetişimin çok paydaşlı yaklaşımı kapsamında incelenmeye çalışılmıştır. Bu amaç doğrultusunda, üniversite kütüphanelerinde bulunan eserler ile birçok Yüksek Lisans ve Doktora Tezi taranmıştır. Konuya ilişkin kitaplar, internet siteleri, ulusal ve uluslararası hakemli dergilerdeki makaleler ile alanında uzman kişilerin çeşitli platformlardaki çalışmaları incelenmiştir. Türkiye, Fransa ve ABD örneklerinin incelenmesi aşamasında bu ülkelerin resmi internet sitelerinde yer alan yıllık raporlardan ve stratejik planlamalardan yararlanılmıştır. Çalışma yapılırken İngilizce ile Türkçe eser ve yayınlardan faydalanılmıştır.

1.4. Literatür İncelemesi

Günümüzün dijitalleşen dünyasında, siber güvenlik giderek daha kritik bir öneme sahip olmaktadır. Siber tehditlerin artışıyla birlikte, kolluk kuvvetlerinin bu alandaki rolü de literatürde geniş bir şekilde ele alınmaktadır. Kolluk kuvvetleri, bireylerin, kurumların ve devletlerin dijital varlıklarını koruma konusunda önemli bir görev üstlenmektedir (Wall, 2007). Bu bağlamda, literatürde kolluk kuvvetlerinin siber güvenlikteki rolü, kapasite geliştirme, iş birliği ve mevzuat boyutlarıyla incelenmektedir (Bossler ve Holt, 2012).

Literatürde, siber suçlarla mücadelede kolluk kuvvetlerinin karşılaştığı zorluklara dikkat çekilmektedir. Özellikle teknik bilgi eksikliği, yasal düzenlemelerin yetersizliği ve uluslararası iş birliğinin karmaşıklığı, bu alandaki başlıca sorunlar arasında yer almaktadır (Holt ve diğ., 2010). Ayrıca, siber suçların sınır ötesi doğası, kolluk kuvvetlerinin etkili müdahale stratejileri geliştirmesini zorlaştırmaktadır (Brenner, 2010). Kolluk kuvvetlerinin siber güvenlikteki görevlerini yerine getirebilmesi için teknolojik altyapı ve insan kaynağı yatırımları büyük önem taşımaktadır. Literatürde, bu yatırımların, siber suçların tespiti ve önlenmesindeki etkinliği artırdığı vurgulanmaktadır (Grabosky, 2001; Yar, 2013). Ayrıca, siber suçlarla mücadelede özel sektör ve akademik kuruluşlarla iş birliğinin önemine de değinilmektedir (Broadhurst, 2006). Bir diğer önemli literatür konusu, siber suçlarla mücadelede eğitim ve farkındalık çalışmalarının rolüdür. Kolluk kuvvetlerinin bu alandaki bilgi ve becerilerini artırmak için düzenlenen eğitim programlarının, siber tehditlere karşı daha etkili bir mücadele sağladığı belirtilmektedir (Leukfeldt ve diğ., 2017). Örneğin, Avrupa Polis Teşkilatı (EUROPOL) ve Uluslararası Kriminal Polis Teşkilatı (INTERPOL-International Criminal Police Organization) gibi uluslararası kuruluşlar, siber güvenlik eğitimlerine öncülük etmektedir (Clough, 2010). Literatürde kolluk kuvvetlerinin siber güvenlikteki rolü, küresel yönetişim kavramı çerçevesinde oluşturduğu iş birlikleri konunun anlaşılması açısından önemli olması sebebiyle

daha geniş bir şekilde ele alınmıştır. Teknolojik gelişmelere uyum sağlama, iş birliği ağlarını genişletme ve uluslararası mevzuat oluşturma ve bu mevzuatı güçlendirme gibi unsurlar, bu alandaki literatürün temel odak noktalarını oluşturmaktadır.





2. TEORİK VE TARİHSEL ÇERÇEVEDE SİBER GÜVENLİK VE KÜRESEL YÖNETİŞİM KAVRAMLARI

2.1. Siber Güvenlik Kavramının Gelişimi ve Önemi

“Siber” kelimesi, kökenini Yunanca "kybernetes" kelimesinden almaktadır. Bu kelime, "dümen tutan" ya da "yönetici" anlamına gelmektedir. Modern dönemde ise, 1948 yılında Amerikalı matematikçi Norbert Wiener tarafından ortaya atılan "sibernetik" (cybernetics) terimiyle bağlantılı olarak kullanılmaya başlanmıştır (Wiener, 1948). Sibernetik, insan, makine ve organizasyonlar arasındaki kontrol ve iletişim süreçlerini inceleyen bir bilim dalı olarak bilinmektedir. Zamanla, bu terim dijital sistemlerin ve bilgisayarların denetim mekanizmalarını ifade eden bir anlam kazanmıştır. "Siber" ön eki, teknolojik ve dijital ortamlarla ilişkilendirilerek, bilgi güvenliği, dijital iletişim ve sanal dünyayla ilgili kavramları tanımlamak için kullanılmaya başlanmıştır.

Siber güvenlik kavramı, teknolojinin gelişmesiyle birlikte önem kazanan bir kavramdır. İlk olarak 1980'lerde, bilgisayarların ve ağ sistemlerinin yaygınlaşmaya başlamasıyla birlikte ortaya çıkmıştır. Bu dönemde, bilgisayar korsanlarının (hacker) sistemlere yetkisiz erişim sağlaması, virüslerin ve kötü amaçlı yazılımların (malware) yaygınlaşması, bilgi güvenliği konusunu gündeme getirmiştir (Kramer ve diğ., 2010). 1990'larda internetin küresel ölçekte yaygınlaşması, siber güvenlik tehditlerini daha da artırmıştır. Özellikle bankacılık, iletişim ve kamu hizmetlerinin dijitalleşmesi, siber saldırılara açık bir alan yaratmıştır. 2000'li yıllarda ise, devlet destekli siber saldırılar, kritik altyapılara yönelik tehditler ve kişisel verilerin korunması konuları ön plana çıkmıştır (Singer ve Friedman, 2014). Bu gelişmeler, siber güvenliği hem ulusal hem de uluslararası bir güvenlik meselesi haline getirmiştir. Siber güvenlik kavramı, 21. yüzyılda ise uluslararası ilişkiler literatürüne güçlü bir şekilde girmiştir. Özellikle 2007'de Estonya'ya yapılan siber saldırılar ve 2010'da İran'ın nükleer tesislerini hedef alan Stuxnet yazılımı gibi olaylar, devletlerin siber güvenliği bir ulusal güvenlik meselesi olarak ele almalarına neden olmuştur (Rid, 2013). Bu bağlamda, devletlerarası çatışmaların yeni bir boyutu olarak "siber savaş" kavramı ortaya çıkmıştır.

Uluslararası ilişkilerde siber güvenlik, sadece saldırı ve savunma mekanizmalarını değil, aynı zamanda siber uzayın yönetimi, uluslararası hukuk, etik, siber suçlarla mücadele ve iş birliği konularını da kapsamaktadır. NATO, Avrupa Birliği (AB), Birleşmiş Milletler gibi uluslararası örgütler, bu alanda politikalar geliştirmektedir. Ayrıca, büyük güçler arasında siber alandaki rekabet, uluslararası sistemin dinamiklerini şekillendiren önemli bir faktör haline gelmiştir.

(Healey, 2011). Siber güvenlik, dijital çağın kaçınılmaz bir gerekliliği olarak hem bireylerin hem de devletlerin gündeminde yer almaktadır. Etimolojik olarak "yönetim" ve "kontrol" kavramlarından türeyen "siber" terimi, bugün teknolojik ve dijital ortamların güvenliğini ifade eden bir kavram olarak karşımıza çıkmaktadır. Bu bağlamda, uluslararası ilişkilerde siber güvenliğin giderek artan önemi, dijital çağda barış ve güvenliğin sağlanması için uluslararası iş birliğinin ve düzenlemelerin hayati olduğunu göstermektedir.

Siber güvenlik, dijitalleşmenin hızla yayıldığı ve küresel ekonomilerin internet tabanlı bir altyapıya dayandığı günümüzde, sadece bireyler ve özel sektör için değil, aynı zamanda devletler için de kritik bir konu haline gelmektedir. Teknolojik gelişmeler, aynı zamanda yeni türde tehditleri de beraberinde getirmektedir. Siber saldırılar, veri ihlalleri, dijital suçlar gibi tehditler, ülkelerin güvenliğini tehdit etmektedir. Bu tehditlerin önlenmesi ve siber güvenliğin sağlanması, geleneksel güvenlik alanlarının ötesinde, dijital dünyada da etkin stratejiler geliştirilmesini gerektirmektedir. Bu bağlamda, siber güvenlik yalnızca hükümetler ve özel sektör arasındaki iş birliği ile sağlanmakla kalmayıp, kolluk kuvvetlerinin de rolünü giderek daha önemli hale getirmiştir (Zetter, 2020).

Kolluk kuvvetleri, siber güvenlik stratejilerinin uygulanmasında ve siber suçlarla mücadelenin ön saflarında yer almaktadır. Bu kuvvetler, siber suçları tespit etme, soruşturma, delil toplama ve suçlulara karşı hukuki işlemler başlatma gibi işlevleri yerine getirmektedirler. (Smith, 2021) Bununla birlikte, siber suçların sınırları aşan doğası, uluslararası iş birliğini ve kolluk kuvvetlerinin küresel yönetimdeki rolünü daha da önemli kılmaktadır. Küresel siber güvenlik yönetiminde, devletler arası iş birlikleri ve bilgi paylaşımı giderek daha fazla önem kazanmakta, kolluk kuvvetleri bu iş birliklerini destekleyerek küresel siber suçlarla mücadelede önemli bir aktör olarak konumlanmaktadır (Vermesan ve Friess, 2018).

Türkiye, Fransa ve ABD gibi ülkeler, siber güvenlikte kolluk kuvvetlerinin etkinliğini artırmak adına çeşitli stratejiler geliştirmektedir. Bu ülkelerin her biri, yerel ve küresel düzeydeki tehditlere karşı kendi kolluk kuvvetlerinin kapasitesini güçlendirme yolunda farklı yaklaşımlar benimsemektedir. Türkiye, 2013 yılında USGK'yı kurarak siber güvenliği devlet düzeyinde öncelikli bir mesele haline getirmiştir. Ayrıca, siber suçlarla mücadele için Siber Suçlarla Mücadele Daire Başkanlığı kurulmuş ve kolluk kuvvetlerinin siber suçlara karşı kapasitesi artırılmıştır (Öztürk, 2020). Fransa ise 2015'te kabul ettiği Siber Güvenlik Stratejisi ile kolluk kuvvetlerinin dijital suçlarla mücadelede etkinliğini artırmayı hedeflemiştir. Bu strateji, siber suçlara karşı kolluk kuvvetlerinin dijital forensik kapasitesini güçlendirmeyi ve uluslararası iş birliğini teşvik etmeyi amaçlamaktadır (Lemoine ve diğ., 2019). ABD, siber güvenlikte lider

konumda bulunan ülkelerden biridir ve kolluk kuvvetlerinin bu alandaki rolü oldukça belirgindir. FBI (Federal Soruşturma Bürosu) ve HSD (Homeland Security Department- İç Güvenlik Departmanı) gibi kolluk kuvvetleri hem siber suçları tespit etme hem de dijital suçlularla uluslararası düzeyde mücadele etme konusunda geniş bir ağ kurmuşlardır. ABD, aynı zamanda küresel siber suçlarla mücadelede uluslararası iş birliklerini güçlendirmek amacıyla Uluslararası Kriminal Polis Teşkilatı (INTERPOL) ve Avrupa Polis Teşkilatı (EUROPOL) gibi kuruluşlarla aktif olarak çalışmaktadır (Smith, 2021).

Bu tez, Türkiye, Fransa ve ABD'nin siber güvenlik stratejilerinde kolluk kuvvetlerinin rolünü ve bu ülkelerin küresel siber güvenlik yönetişimine nasıl katkı sağladığını incelemeyi amaçlamaktadır. Her bir ülkenin siber güvenlik politikaları, kolluk kuvvetlerinin bu politikalar içindeki yeri ve bu ülkelerin uluslararası düzeydeki iş birlikleri detaylı olarak ele alınmaktadır. Bu çalışma, kolluk kuvvetlerinin küresel siber güvenlik yönetişimindeki stratejik rolünü, yerel, bölgesel ve küresel iş birlikleri açısından değerlendirerek, bu aktörlerin siber suçlarla mücadeledeki etkinliğini ortaya koymaktadır.

Siber güvenlik, teknolojinin hızla evrildiği ve dijital dünyanın hayatın her alanında derinlemesine etkili olduğu günümüzde giderek daha fazla önem kazanan bir kavramdır. İnternetin, dijitalleşmenin ve bağlantılı sistemlerin yaygınlaşmasıyla birlikte, bu alanlarda ortaya çıkan tehditler de büyük bir hızla çeşitlenmekte ve karmaşıklaşmaktadır. 1990'lı yıllarda internetin yaygınlaşmaya başlamasıyla, bireyler ve kurumlar için dijital güvenlik, yalnızca bir tercihten ziyade bir gereklilik haline gelmektedir. Ancak, siber güvenlik kavramı, başlangıçta sadece bilgisayar sistemlerini ve ağlarını koruma amacı taşıyan bir uygulama alanıyken, günümüzde çok daha geniş bir anlam kazanmış, tüm dijital ekosistemlerin güvenliğini kapsayan bir disiplin haline gelmektedir (Denning, 2017). Siber güvenliğin evrimi, ilk olarak ağ güvenliği ve bilgi güvenliği gibi daha dar kapsamlı alanlarda başlamıştır. 1980'lerin sonlarına doğru, internetin ilk yıllarında, siber güvenlik daha çok temel bilgisayar virüsleri ve kötü amaçlı yazılımlar üzerine yoğunlaşmaktadır (Gordon ve d, 2020). Bununla birlikte, dijital dünyadaki hızlı değişim ve yayılma, siber güvenliğin yalnızca teknik bir sorun olmaktan çıkarmakta, sosyal, ekonomik ve hatta siyasi bir konu olarak da ele alınmasını gerektirmektedir. Bilgi ve iletişim teknolojilerinin hızla gelişmesiyle, siber saldırılar daha karmaşık hale gelmekte, hedefler daha çeşitli ve saldırı yöntemleri daha karmaşık bir boyut kazanmaktadır (Lemos ve diğ., 2020).

1990'ların sonlarından itibaren siber güvenlik kavramı, kritik altyapıların korunmasından bireysel veri güvenliğine kadar geniş bir alanı kapsar hale gelmektedir. Bu dönemde siber

güvenlik yalnızca hükümetler ve büyük şirketler için değil, günlük hayatı etkileyen bir tehdit olmaya başlamaktadır. Küresel anlamda, 2000'lerin başlarından itibaren siber güvenlikteki tehditler daha fazla dikkat çekmeye başlamakta, devletler, uluslararası örgütler ve özel sektör arasındaki iş birlikleri güçlenmektedir. Çeşitli siber saldırı türleri, sosyal mühendislik teknikleri, fidye yazılımları gibi yeni tehditler, güvenlik stratejilerinin çeşitlenmesini ve yeni teknolojik önlemlerin geliştirilmesini zorunlu kılmaktadır (NIST, 2018). Bugün siber güvenlik, sadece veri ve bilgi koruma değil, aynı zamanda devlet güvenliği, ulusal güvenlik, dijital ekonomik yapıların sürdürülebilirliği gibi daha geniş bir alanı kapsamaktadır. (Jøsang ve diğ., 2021).

Özellikle 2000'lerin başından itibaren siber güvenlik tehditleri sadece bireyler ve şirketler için değil, devletler için de büyük bir risk oluşturur hale gelmektedir. Devletlerin karşılaştığı tehditler, kritik altyapıların hedef alınmasından, devletin siber sistemlerinin manipülasyonuna kadar geniş bir yelpazeyi kapsamaktadır (Miller, 2020). Bu gelişmeler, siber güvenliğin küresel yönetim çerçevesinde ele alınmasını, çeşitli uluslararası iş birlikleri ve normların oluşturulmasını teşvik etmektedir. Uluslararası düzeyde siber güvenlik iş birlikleri, 2000'lerin ortalarından itibaren daha yoğun hale gelmekte, siber suçlarla mücadele, siber saldırılara karşı kolektif güvenlik anlayışı güçlendirmektedir (Mann ve Memon, 2021). Siber güvenliğin gelişimi, özellikle devletlerin bu konuda ciddi yasalar ve düzenlemeler getirmesiyle hız kazanmaktadır. Küresel siber güvenliğin yapılanması ve yönetimi için geliştirilen ilk uluslararası belgeler, özellikle siber suçlar, veri koruma ve güvenlik standartları konularında önemli adımlar atan belgelerdir. Bu belgeler arasında öne çıkanlar şunlardır:

Budapeşte Sözleşmesi 23 Kasım 2001 tarihinde Avrupa Konseyi tarafından kabul edilen ve siber suçlarla mücadelede uluslararası iş birliğini güçlendirmeyi amaçlayan ilk bağlayıcı uluslararası sözleşmedir. Sözleşme, bilgisayar sistemleri ve verileriyle ilgili suçların tanımlanması, soruşturulması ve kovuşturulması için ortak bir yasal çerçeve oluşturmayı hedeflemektedir. Avrupa dışındaki birçok ülke (ABD, Kanada, Japonya vb.) tarafından da kabul edilmiştir ve küresel siber güvenlik standartlarının temelini oluşturmaktadır (Avrupa Konseyi, 2001). Genel olarak temel hedeflerini sıralayacak olursak: Taraf devletlerin siber suçlarla ilgili yasal düzenlemelerini uyumlu hale getirerek, suçların tanımlanmasında ve cezalandırılmasında standart bir yaklaşım benimsemek; siber suçların etkin bir şekilde soruşturulması ve kovuşturulması için gerekli usul hukuku araçlarını sağlamak; siber suçlarla mücadelede devletler arasında hızlı ve etkili bir iş birliği mekanizması oluşturmaktır. Bu sözleşme kapsamında suç türlerinde ise: Bilgisayar Sistemlerine Yetkisiz Erişim (Hacking),

Veri Müdahalesi, Sistem Müdahalesi, Sahtecilik ve Dolandırıcılık, Çocuk Pornografisi sıralanmaktadır. Sözleşmeye ek olarak, 28 Ocak 2003 tarihinde kabul edilen bir Ek Protokol bulunmaktadır. Bu protokol, bilgisayar sistemleri aracılığıyla işlenen ırkçı ve yabancı düşmanlığı güden nitelikli eylemlerin cezalandırılmasını düzenlemektedir (Avrupa Konseyi Siber Suç Konseyi, 2003). Budapeşte Siber Suçlar Sözleşmesi, 23 Kasım 2001 tarihinde imzaya açılmış ve 1 Temmuz 2004 tarihinde yürürlüğe girmiştir. Amerika Birleşik Devletleri (ABD), Sözleşmeyi 23 Kasım 2001 tarihinde imzalamış ve 29 Eylül 2006 tarihinde onaylayarak taraf olmuştur. Fransa ise Sözleşmeyi 23 Kasım 2001 tarihinde imzalamış ve 10 Ocak 2006 tarihinde onaylayarak taraf olmuştur. Türkiye ise, Sözleşmeyi 10 Kasım 2010 tarihinde imzalamış ve 22 Nisan 2014 tarihinde onaylayarak 1 Ocak 2015'te yürürlüğe koymuştur. (Demirören, 2019)

OECD (Ekonomik İş birliği ve Kalkınma Örgütü), bilgi sistemlerinin güvenliği ve kişisel verilerin korunması alanında uluslararası standartlar oluşturmak amacıyla rehber ilkeler yayımlamaktadır. Bu ilkeler, siber güvenlik politikalarının geliştirilmesinde ve uygulanmasında önemli bir rol oynamaktadır. 1980'de Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Akışına İlişkin Rehber İlkeleri yayınlanmıştır. 23 Eylül 1980 tarihinde yayımlanan bu rehber ilkeler, kişisel verilerin korunması ve sınır ötesi veri akışının düzenlenmesi amacıyla oluşturulmuştur. Sekiz temel ilkedен oluşmaktadır.

- Veri Toplamanın Sınırlılığı İlkesi: Kişisel verilerin toplanması, belirli, meşru ve açık amaçlarla sınırlı olmalı ve ilgili kişinin rızasıyla veya yasal yetkiyle gerçekleştirilmelidir.
- Veri Kalitesi İlkesi: Toplanan veriler doğru, eksiksiz ve güncel olmalıdır.
- Belirli Amaç İlkesi: Veriler, toplama amacına uygun olarak kullanılmalı ve bu amaç dışında kullanılmamalıdır.
- Kullanımın Sınırlılığı İlkesi: Kişisel veriler, ilgili kişinin rızası olmadan veya yasal bir gereklilik bulunmadan üçüncü taraflarla paylaşılmamalıdır.
- Veri Güvenliği İlkesi: Kişisel verilerin yetkisiz erişim, ifşa, değiştirme veya imhaya karşı korunması için gerekli güvenlik önlemleri alınmalıdır.
- Açıklık İlkesi: Veri işleme politikaları ve uygulamaları şeffaf olmalı, bireyler kendi verileri hakkında bilgi sahibi olabilmelidir.
- Katılım İlkesi: Bireyler, kendileriyle ilgili verilerin varlığı hakkında bilgi edinme ve bu verilerin düzeltilmesini veya silinmesini talep etme hakkına sahip olmalıdır.
- Hesap Verebilirlik İlkesi: Veri denetleyicileri, yukarıdaki ilkelerin uygulanmasından sorumludur ve hesap verebilir olmalıdır. Bu ilkeler, uluslararası düzeyde kişisel verilerin korunması konusunda temel bir çerçeve sunmaktadır (OECD, 1980).

Bilgi teknolojilerindeki hızlı gelişmeler ve internetin yaygınlaşmasıyla birlikte, OECD 2002 yılında Bilgi Sistemlerinin Güvenliğine İlişkin Rehber İlkeleri yayımlamıştır. Bu rehber, bilgi sistemlerinin güvenliğini sağlamak için benimsenmesi gereken temel ilkeleri içermektedir. Bunlar;

- Farkındalık: Toplumun tüm kesimleri, bilgi sistemlerinin güvenliği konusunda bilinçlendirilmesidir.
- Sorumluluk: Bilgi sistemlerinin güvenliğinden sorumlu olan tüm taraflar, görev ve sorumluluklarını yerine getirilmesidir.
- Tepki Verme: Güvenlik ihlallerine karşı hızlı ve etkili bir şekilde yanıt verilmesidir.
- Etik Davranış: Bilgi sistemlerinin kullanımı sırasında etik kurallara uyulmasıdır.
- Demokrasinin Korunması: Bilgi sistemlerinin güvenliği, demokratik değerlerin korunmasına katkı sağlamasıdır.
- Risk Değerlendirmesi: Bilgi sistemlerine yönelik riskler düzenli olarak değerlendirilmelidir. Güvenlik Tasarımı ve Uygulaması: Güvenlik önlemleri, bilgi sistemlerinin tasarım ve uygulama aşamalarında dikkate alınmalıdır.
- Sürekli Gelişim: Güvenlik politikaları ve uygulamaları sürekli olarak gözden geçirilmeli ve iyileştirilmelidir. (OECD, 2002).

Bu ilkeler, bilgi sistemlerinin güvenliğine yönelik bir güvenlik kültürünün oluşturulmasını teşvik etmektedir (Ankara Üniversitesi Bilgi İşlem Daire Başkanlığı, 2018). OECD'nin bu rehber ilkeleri, üye ülkeler ve diğer devletler tarafından benimsenerek, siber güvenlik ve kişisel verilerin korunması alanında uluslararası standartların oluşturulmasına katkı sağlamaktadır. Bu ilkeler, günümüzde de siber güvenlik politikalarının temel taşlarını oluşturmaktadır.

Birleşmiş Milletler (BM) Genel Kurulu, siber güvenlik alanında uluslararası iş birliğini ve düzenlemeleri teşvik etmek amacıyla çeşitli kararlar almaktadır. Bu kararlar, üye devletlerin siber tehditlere karşı ortak bir yaklaşım benimsemelerini ve iletişim teknolojilerinin barışçıl kullanımını sağlamayı hedeflemektedir. BM Genel Kurulu, siber alana ilişkin ilk kararını 1998 yılında yayımlamıştır (A/RES/53/70 sayılı BM Kararı, 1998). Bu kararda, bilgi ve telekomünikasyon alanındaki gelişmelerin uluslararası güvenlik üzerindeki etkileri ele alınmakta ve üye devletlerin bu alandaki güvenlik tedbirlerini gözden geçirmeleri teşvik edilmektedir (Akdağ, 2020). 2002 yılında yayımlanan bir diğer kararda ise, siber güvenlik konusundaki uluslararası iş birliğinin artırılması amacıyla bir Ülke Uzmanları Grubu kurulması önerilmektedir (A/59/454 sayılı BM Kararı, 2004). Bu grup, siber tehditlerin değerlendirilmesi ve uygun önlemlerin belirlenmesi konularında çalışmalar yapmaktadır. BM Genel Kurulu,

2024 yılında siber suçlarla mücadelede uluslararası iş birliğini güçlendirmeyi ve toplumları dijital tehditlerden korumayı amaçlayan bir siber suç sözleşmesini kabul etmiştir. Sözleşmenin 2025 yılında yapılan toplantıdan sonra yürürlüğe gireceği duyurulmuştur. Bu sözleşme, üye devletlerin siber suçları önlemek ve bunlarla mücadele etmek için ortak bir çerçeve oluşturmasını sağlamaktadır (Sosyalup, 2024). Bu kararlar ve girişimler, BM'nin siber güvenlik alanında uluslararası normların ve iş birliğinin geliştirilmesine yönelik çabalarını yansıtmaktadır. Üye devletler arasında bilgi paylaşımı, kapasite geliştirme ve ortak standartların oluşturulması gibi konular, BM Genel Kurulu'nun siber güvenlik konusundaki çalışmalarının temel unsurlarını oluşturmaktadır.

Uluslararası Telekomünikasyon Birliği (ITU), 1865 yılında kurulan ve Birleşmiş Milletlere bağlı bir uzmanlık kuruluşu olan uluslararası bir organizasyondur. ITU, bilgi ve iletişim teknolojilerinin geliştirilmesini, dünya genelinde bu teknolojilere erişimin artırılmasını ve bu süreçte uluslararası iş birliğinin teşvik edilmesini hedeflemektedir (ITU, 2025). Siber güvenlik, ITU'nun stratejik öncelikleri arasında önemli bir yer tutmaktadır. ITU, ülkelerin ve kurumların dijital tehditlerle başa çıkabilmesi için çeşitli programlar ve girişimler yürütmektedir. Global Siber Güvenlik Gündemi (Global Cybersecurity Agenda- GCA) 2007 yılında başlatılmış olup, dünya genelinde siber güvenliğin geliştirilmesi için bir çerçeve sunmaktadır. GCA, politika oluşturma, yasal düzenlemeler, kapasite geliştirme, teknik önlemler ve uluslararası iş birliği gibi başlıklar altında çalışmaktadır (ITU GCA, 2025). Siber Güvenlik Endeksi (Global Cybersecurity Index- GCI) ITU tarafından yayımlanmakta olup, ülkelerin siber güvenlik kapasitelerini ölçmekte ve kıyaslamaktadır. Endeks, ülkelerin yasal düzenlemeleri, teknik kapasiteleri, iş birliği düzeyleri ve farkındalık yaratma çabalarını analiz ederek küresel bir veri sunmaktadır (ITU GCI, 2023). Kapalı Alan Testi ve Eğitim Programları ile ITU, gelişmekte olan ülkeler için siber güvenlik eğitimleri düzenlemekte ve çeşitli siber saldırı senaryolarına dayalı tatbikatlar yapmaktadır. Bu tür programlar, ulusal Bilgisayar Acil Müdahale Ekiplerinin (CERT- Computer Emergency Response Team) kapasitelerini artırmayı hedeflemektedir (ITU Trainings, 2024). ITU, siber güvenlik alanında çok taraflı iş birliğine büyük önem vermektedir. Bu bağlamda, diğer BM organları, ulusal hükümetler, akademik kurumlar ve özel sektörle ortak projeler yürütmektedir. Örneğin, ITU'nun INTERPOL ile ortak çalışmaları, sınır ötesi siber suçlarla mücadeleye odaklanmaktadır (ITU and INTERPOL Collaboration, 2025). ITU'nun siber güvenlik girişimleri, dijital dünyadaki güvenliği artırmak için kritik öneme sahiptir. Dijital altyapının korunması hem bireylerin hem de devletlerin ekonomik ve sosyal istikrarı için

vazgeçilmezdir. ITU'nün bu alandaki liderliği, uluslararası iş birliğinin ve yenilikçi çözümlerin hayata geçirilmesini kolaylaştırmaktadır.

Wassenaar Düzenlemesi (1996, Güncellenen Hükümler) ile çift kullanımlı teknolojiler (askeri ve sivil) için ihracat kontrollerini düzenlemektedir. Siber güvenlik araçları ve yazılımlar da kapsam dahiline alınmaktadır. Siber silahların ve teknolojilerin kötüye kullanılmasını önleme amacıyla siber güvenlik politikalarıyla ilişkilendirilmektedir. Talinn El Kitabı (2009 ve 2017 Güncellemeleri) NATO'nun sponsorluğunda hazırlanmış olup bu rehber, siber uzaydaki uluslararası hukukun uygulanabilirliğini inceleyen bir çalışmadır. Devletler arasında siber savaş, egemenlik ve müdahale gibi konuları ele almaktadır. APEC Gizlilik Çerçevesi (2004) ise Asya-Pasifik Ekonomik İş Birliği (APEC) tarafından oluşturulan, siber güvenlik ve veri gizliliğiyle ilgili bölgesel bir yaklaşımı temsil etmektedir. Bu belgeler, siber güvenlik alanında uluslararası iş birliğini teşvik eden ve ortak standartlar geliştiren önemli adımlardır. Siber güvenliğin dinamik yapısı nedeniyle bu çerçeveler zaman içinde revize edilmekte ve yeni girişimler eklenmektedir.

Birçok uluslararası girişimin yanı sıra ülkeler de ulusal siber güvenlik stratejileri de geliştirmek yolunda adımlar atılmaktadır. 2000'lerin sonlarına doğru, birçok ülke siber güvenlik stratejileri oluşturarak, kritik altyapılarını korumaya yönelik önlemler almaya başlamaktadır. 2013'te ABD, Ulusal Standartlar ve Teknoloji Enstitüsü (NIST-National Institute of Standards and Technology) Siber Güvenlik Çerçevesini sunmuş, bu çerçeve uluslararası düzeyde siber güvenlik politikalarının şekillenmesine katkı sağlamaktadır (NIST, 2018). Aynı dönemde AB, siber güvenlik alanında çeşitli direktifler yayımlamış, üye devletlerin siber güvenlik alanındaki iş birliğini teşvik etmektedir (European Commission, 2020). Türkiye de bu küresel trende ayak uydurarak, 2013 yılında Ulusal Siber Güvenlik Stratejisi'ni benimsemiş ve siber güvenlik politikalarını devletin stratejik öncelikleri arasına almaktadır (Başaran & Şahin, 2020).

Günümüzde, siber güvenlik yalnızca teknoloji odaklı bir mesele olmaktan çıkmış, bireylerin haklarının korunmasından, küresel ekonomik sistemin devamlılığına kadar pek çok alanı etkilemektedir. Bu nedenle siber güvenlik politikalarının oluşturulmasında devletler, özel sektör, uluslararası kuruluşlar ve kolluk kuvvetleri gibi farklı aktörler tarafından hazırlanarak kullanılan ortak politikalar, kararlar olması paydaşlar için oldukça önemli bir yer tutmaktadır.

2.2.Kopenhag Ekolü Çerçevesinde Siber Güvenlik

Kopenhag Ekolü, 1980'lerin sonlarında ve 1990'ların başlarında, Soğuk Savaş'ın sona ermesiyle birlikte uluslararası ilişkilerde güvenlik anlayışının değiştiği bir dönemde ortaya çıkmaktadır.

Bu ekol, Barry Buzan ve Ole Waever'in liderliğinde şekillenmektedir (Buzan ve diğ., 1998). İlk kez, Barry Buzan'ın İnsanlar, Devletler ve Korku (1983) adlı kitabında ortaya çıkardığı güvenliğin genişletilmesi fikri, 1990'larda daha olgunlaşmakta ve sistemli bir teori Analysis adlı çalışma, Kopenhag Ekolü' nü uluslararası güvenlik literatüründe önemli bir yere taşımaktadır (Buzan ve diğ., 1998).

Kopenhag Ekolü, geleneksel (gerçekçi) güvenlik anlayışına karşı bir eleştiri olarak doğmakta, temel unsurları devlet merkezilik, askeri odaklılık, anarşi ve güç dengesi olan realist yaklaşımı eleştirmektedir (Buzan, 1983). Kopenhag Ekolü, güvenliğin yalnızca askeri tehditlerden oluşmadığını, ekonomik, askeri, ekonomik, demokratik ve toplumsal boyutlarının olduğunu, bireylerden toplumlara kadar geniş bir yelpazede ele alınması gerektiğini savunmaktadır (Buzan ve diğ., 1998). Kopenhag Ekolü, geleneksel güvenlik anlayışını genişleterek güvenliği çok boyutlu bir kavram olarak ele almaktadır. Örneğin, küreselleşmenin ortaya çıkmasıyla ortaya çıkan ekonomik krizler, çevresel felaketler ve siber saldırılar gibi tehditler ile güvenlik anlayışının kapsamı genişletilmektedir (Collins, 2016). Güvenlik artık yalnızca devletlerin değil, toplumun ve uluslararası bileşenlerinde yapısında yer almaktadır.

Kopenhag Ekolü'nün bir diğer önemli katkısı, "güvenikleştirme" kavramıdır. Bu kavrama göre, bir konu, siyasi aktörlerin söylemleriyle bir güvenlik meselesi haline getirilebilmektedir. Örneğin, siber alan, göçmenlik veya iklim değişikliği gibi konular, belli bir söylemle ulusal güvenlik tehdidi olarak sunup ve buna karşı olağanüstü önlemlerle birlikte meşrulaştırılabilmektedir (Wæver, 1995). Kopenhag Ekolü, güvenliği çok boyutlu bir kavram olarak ele almaktadır. Bu boyutlar arasında askeri, ekonomik, toplumsal, siyasal ve çevresel güvenlik yer almaktadır.

- Askeri Güvenlik: Devletin sınırlarını ve kapsamını korumayı amaçlamaktadır. Bu geleneksel güvenlik anlayışının merkezinde yer almaktadır.
- Ekonomik Güvenlik: Yoksulluk, işsizlik, ekonomik krizler ve ticaret engelleri gibi toplumların refahını tehdit eden unsurları içermektedir.
- Çevresel Güvenlik: İklim değişiklikleri, doğal ürünlerin tükenmesi, çevre kirliliği ve ekolojik felaketler gibi küresel risklerle ilgili konularla ilgilenmektedir.
- Toplumsal Güvenlik: Etnik, dini, kültürel kimliklerin korunması ve sosyal istikrarın çalıştırılması konularını içermektedir.

- Siyasal Güvenlik: Devletin politik yapısı, anayasal düzeninin ve demokratik istikrarının korunması olarak tanımlanmaktadır (Collins, 2016).

Siber güvenlik ise Kopenhag Ekolü'nün genişleyen güvenlik çerçevesinde incelendiğinde siber güvenlik pek çok sektörle ilişkili bir konumda bulunmaktadır. Dijital altyapının önem kazanmasıyla birlikte, siber tehditler devletler, özel sektör ve bireyler için kritik bir mesele haline gelmiştir. Askeri güvenlik ve siber güvenlik ilişkisi irdelendiğinde siber güvenlik günümüz dünyasında askeri güvenliğin dijital bir uzantısı olarak değerlendirilebilmektedir. Siber saldırılar, fiziksel çatışmalar kadar yıkıcı etkiler yaratabilmektedir. Kritik altyapılara yönelik saldırılar (ör. enerji santralleri veya iletişim ağları), devletlerin savunma mekanizmalarını yeniden şekillendirmiştir. NATO'nun, siber saldırıları geleneksel bir askeri saldırı olarak kabul etmesi buna örnektir. (NATO Cyber Policy, 2023) Modern askeri stratejilerde, siber saldırılar hibrit savaşın bir parçası olarak kullanılmaktadır. Bu saldırılar hem devlet hem de devlet dışı aktörler tarafından ekonomik altyapılara, seçim sistemlerine ve kamu hizmetlerine zarar vermek amacıyla gerçekleştirilmektedir. Örneğin, 2007'de Estonya'ya yapılan büyük çaplı siber saldırılar, siber güvenliğin ulusal güvenlik politikalarındaki önemini göstermektedir (Rid, 2020). Bu sebeple birçok ülke, siber alanı askeri doktrinlerinin bir parçası haline getirmektedir. Örneğin, ABD Savunma Bakanlığı, siber alanı kara, deniz, hava ve uzayın yanında beşinci operasyonel alan olarak tanımlamaktadır (US Department of Defense, 2021). Siber güvenlik ve askeri güvenlik arasındaki ilişkinin karmaşıklığı, uluslararası hukukta da kendini göstermektedir. Siber savaş eylemlerinin, mevcut uluslararası hukuki çerçevelerle nasıl ele alınacağı hala tartışma konusu olarak karşımıza çıkmaktadır.

Siber güvenlik, siyasal güvenliğin sağlanmasında bir alt faktör olarak değerlendirilebilmektedir. Zira dijital tehditler, doğrudan siyasal sistemlerin işleyişine ve toplumların istikrarına zarar verebilmektedir. Siber güvenlik bağlamında dezenformasyon, bir toplumun siyasi algılarını şekillendirme ve toplumsal kutuplaşmayı artırma amacıyla kullanılan önemli bir araç olarak değerlendirilmektedir. Siyasal güvenliğin önemli bir göstergesi olan demokratik seçim süreçlerine yönelik tehditler siber güvenlik boyutuyla incelendiğinde, seçim sistemlerine yönelik siber saldırılar ve dezenformasyon kampanyaları, siyasal güvenliği baltalayabileceği görülmektedir. Örneğin, 2016 ABD başkanlık seçimleri sırasında yaşanan siber müdahaleler, küresel ölçekte siyasal güvenlik tartışmalarını derinleştirmiştir (Rid, 2020). Sosyal medya platformlarında yayılan yanlış bilgiler, toplumların demokratik süreçlere olan güvenini sarsabilmektedir (Hansen ve Nissenbaum, 2009).

Ekonomik güvenlik açısından ise siber güvenlik giderek kritik bir unsur haline gelmektedir. Dijitalleşen ekonomi, bilgi sistemlerine ve altyapılara olan bağımlılığı artırmış, bu da siber tehditlerin ekonomik güvenlik üzerindeki etkilerini artırmaktadır. Siber casusluk, ekonomik güvenlik açısından büyük bir tehdit oluşturmaktadır. Şirketlerin fikri mülkiyet haklarının çalınması, ekonomik rekabet gücünü azaltabilmektedir. Örneğin, Çin merkezli siber casusluk faaliyetleri, ABD ve Avrupa'daki teknoloji şirketlerini hedef almaktadır (Rid, 2020). Finansal sistemler, enerji şebekeleri ve tedarik zincirleri gibi kritik ekonomik altyapılar, siber saldırılar için hassas hedeflerdir. 2017'deki WannaCry saldırısı, küresel ekonomik sistemde milyarlarca dolarlık zarara yol açarak ekonomik güvenlik ve siber güvenlik arasındaki bağlantıyı açıkça ortaya koymaktadır (Hansen ve Nissenbaum, 2009). Kripto para birimlerinin yükselişi, ekonomik güvenlik ve siber güvenlik arasındaki ilişkiyi daha da karmaşık hale getirmektedir. Siber saldırılar, kripto para piyasalarında ciddi dalgalanmalara neden olabilmekte ve küresel ekonomiyi etkileyebilmektedir.

Toplumsal güvenliğin tesisi açısından bakıldığında siber güvenliğin, dijitalleşmenin toplumsal yapı üzerindeki etkisi nedeniyle, toplumsal güvenliğin de önemli bir bileşeni haline geldiği görülmektedir. Siber tehditler, toplumların kimlik algılarına, sosyal bütünlüğüne ve demokratik işleyişine zarar verebilmektedir. Toplumların kimlik algısı, ortak tarih, kültür, dil, din ve değerler etrafında şekillenmektedir. Siber tehditler, bu kimlik algısını doğrudan veya dolaylı yollarla zayıflatabilmektedir. Siber tehditlerin en önemli araçlarından biri dezenformasyondur. Sosyal medya platformlarında yayılan sahte haberler ve yanlış bilgiler, toplumun ortak değerlerine ve tarihine dair algıyı bozabilmektedir. Tarihi olayların çarpıtılarak sunulması, toplum içinde kutuplaşmayı artırabilmekte veya dini, etnik, kültürel farklı gruplara yönelik yanlış bilgilendirme, toplumsal çatışmaları tetikleyebilmektedir. Bazı siber tehditler ise daha ileri giderek bir toplumun kültürel kimliğini aşındırabilmektedir. Örneğin, dijital platformlar aracılığıyla belirli bir kültürel dilin veya yaşam tarzının baskın hale getirilmesi, azınlık gruplarının kültürel kimliğini tehdit edebilmektedir. Sosyal bütünlük, bir toplumun üyeleri arasındaki uyumu ve dayanışmayı ifade ederken, siber tehditler, sosyal medyanın yaygın kullanımı ve dijital iletişim araçları aracılığıyla bu uyumu zayıflatabilmektedir. Siber tehditler, toplum içindeki farklı gruplar arasında çatışma yaratabilmektedir. Bot hesaplar ve algoritmalar, toplumsal gruplar arasındaki karşıt görüşleri abartarak kutuplaşmayı artırabilmektedir. Dış müdahalelerin de etkisiyle belirli gruplar hedef alınarak, "biz ve onlar" ayrımı güçlendirilebilmektedir. Özellikle genç bireyler arasında yaygın olan siber zorbalık, bireylerin ruhsal sağlığını etkileyerek toplumsal bağları zayıflatabilmekte toplumun genel psikolojik

dayanıklılığın düşürebilmektedir. Sosyal medya platformları, toplumsal algıları şekillendiren ve toplumun birleşme veya ayrışma süreçlerini etkileyen güçlü araçlardır. Manipüle edilen trendler ve sahte haberler, toplumların gerçek bilgiye erişimini engellemektedir.

Çevresel güvenliğin siber boyutu, çevre teknolojilerine yönelik siber saldırılarla ilişkilendirilmektedir. Çevresel güvenliğin sağlanmasında büyük veri toplayan dijital altyapı sistemlerine yönelik saldırılar büyük riskler içermektedir. Örneğin; meteorolojik sistemler, iklim değişikliği verilerinin analizinde kritik öneme sahip olup, bu sistemlere yönelik siber saldırılar, yanlış bilgi yayılmasına veya kritik tahminlerin sabote edilmesine neden olmaktadır. Su kaynaklarının yönetiminde kullanılan sistemler, siber saldırılarla manipüle edilerek bölgesel krizlere yol açabilmektedir (Rid, 2020). Yenilenebilir enerji altyapıları (örn. Rüzgar türbinleri, güneş panelleri), çevresel güvenlikte önemli bir rol oynamaktadır. Ancak bu altyapılar da siber tehditlere açıktır. Sahte kampanyalar ve dezenformasyon, çevresel sorunların ciddiyetini azaltmak veya kamuoyunu yanlış yönlendirmek için kullanılabilir. Kopenhag Ekolü'nün literatüre sunduğu güvenliğin çeşitlenen yapısı çerçevesinde siber güvenlik kavramına baktığımızda devletlerin bu çok yönlü güvenlik anlayışı karşısında politikalarını, duruşlarını değiştirmesi gerektiği de çıkarılabilmektedir. Değişen güvenlik anlayışıyla birlikte nasıl tehditler, riskler, saldırılar farklılaşmışsa; çözüm önerilerinin, iş birliklerinin hem ulusal düzeyde hem de uluslararası düzeyde de değişmesi gerekmektedir.

Kopenhag Ekolü, siber tehditlerin güvenlikleştirme konusunda da önemli bir kavramsal çerçeve sunmaktadır. Siber saldırıların kritik altyapıları ve devletlerin egemenliğini tehdit etmesi, bu konunun genellikle siyasi liderler tarafından bir güvenlik meselesi olarak ele alınmasına yol açmaktadır. Güvenlikleştirme, bu alanda karar alıcıların halkı ve uluslararası toplumu tehdit algısı konusunda harekete geçirmesini sağlayan bir aracı olarak kullanılmaktadır (Buzan ve diğ., 1998). Kopenhag Ekolü'nün güvenlik algısına göre, siber tehditlerin siyasileşmesi, ulusal güvenlik politikalarının şekillendirilmesinde önemli bir etkiye sahiptir. Siber saldırıların ulusal egemenliği tehdit etme potansiyeli, devletlerin bu alandaki stratejik önceliklerini yeniden değerlendirmelerine yol açmaktadır (Hansen ve Nissenbaum, 2009; Nye, 2011). Örneğin, 2007 yılında Estonya'ya yönelik siber saldırılar, NATO'nun siber güvenlik politikalarını yeniden yapılandırmasına zemin hazırlamıştır (Clarke ve Knake, 2010) Kopenhag Ekolü, siber güvenlik gibi yeni ve karmaşık tehditleri anlamak için çok boyutlu bir çerçeve sunmaktadır. Siber tehditlerin askeri, siyasi, ekonomik, toplumsal ve çevresel boyutları, bu ekolün genelleyici güvenlik anlayışı içinde yer bulmaktadır. Bu nedenle, siber güvenlik politikalarını geliştirirken Kopenhag Ekolü'nün sunduğu çok boyutlu yaklaşımdan yararlanmak, tehditlerin daha etkili bir

şekilde ele alınmasını sağlayabilmektedir. Bu çok boyutlu siber güvenlik tehditleri için ise bireylerden devletlere uluslararası aktörlerin iş birliği yapması önem arz etmektedir. Kolluk kuvvetleri de siber güvenliğin sağlanmasında önemli bir aktör olarak değerlendirilmektedir.

Kopenhag Okulu'na göre, bir mesele tehdit olarak tanımlandığında, bu tehditle mücadele eden aktörler belirginleşmektedir. Siber tehditlerin suç unsuru olarak tanımlandığı noktalarda, kolluk kuvvetleri (polis, jandarma, adli bilişim birimleri) doğrudan müdahil olmaktadır. Örneğin, fidye yazılım saldırıları, kimlik hırsızlığı, çevrimiçi dolandırıcılık gibi suçlarda, kolluk kuvvetleri siber suçların tespit edilmesi, soruşturulması ve önlenmesinde anahtar bir rol oynamaktadır. Bazı ülkelerde ise siber tehditler doğrudan ulusal güvenlik sorunu olarak ele alındığında, kolluk kuvvetleri ulusal siber savunma mekanizmalarının bir parçası hâline gelmektedir. Örneğin, FBI'ın Siber Suçlar Birimi veya Türkiye'deki Siber Suçlarla Mücadele Daire Başkanlığı gibi birimler bu alanda faaliyet göstermektedir (Buzan ve diğ., 1998). Kolluk kuvvetleri, yasadışı dijital faaliyetlere karşı hem ulusal hem de uluslararası mevzuatın uygulanmasını sağlamaktadır. Örneğin, siber suçlara karşı operasyonlar düzenlemekte, uluslararası iş birliğine katkı sunmakta ve suçluları adalet önüne çıkarmaktadırlar. Kopenhag Okulu'na göre, güvenlikleştirme, bazı durumlarda olağanüstü önlemleri meşrulaştırmaktadır. Kolluk kuvvetleri, siber güvenlikte bireylerin özgürlükleri ve devlet güvenliği arasındaki dengeyi sağlama sorumluluğu taşımaktadır. Bu da onların rolünün siyasi ve toplumsal açıdan kritik olduğunu göstermektedir. (Taddeo ve Floridi, 2018)

2.3. Küresel Yönetişim Kavramı ve Siber Güvenlik

Küresel yönetim, günümüz dünyasında giderek daha fazla dikkat çeken ve tartışılan bir kavramdır. 21. yüzyılda, ulusal sınırların giderek daha fazla aşınmasına ve küreselleşmenin derinleşmesine paralel olarak, küresel meselelerin çözülmesinde devletler arasındaki iş birliğinin yanı sıra, uluslararası kuruluşlar, özel sektör ve sivil toplum gibi çoklu aktörlerin de rol aldığı bir yönetim yapısı önem kazanmaktadır. Küresel yönetim, başta ekonomik, çevresel ve sosyal sorunlar olmak üzere, devletlerin ortak paydada buluşması gereken küresel çapta var olan karmaşık ve birbirine bağlı sorunları ele almak için kullanılan bir çerçevedir. (Rosenau, 2000). Küresel yönetim kavramı, 1990'ların başlarında, Soğuk Savaşın sona ermesinin ardından ortaya çıkmaya başlamaktadır. Bu dönemde, uluslararası ilişkilerde devletlerin egemenlikleri ön plana çıkarken, aynı zamanda devlet dışı aktörlerin de küresel düzeyde artan bir şekilde etkili olmaya başladığı gözlemlenmektedir. (Held ve McGrew, 2002) Küresel yönetim, sadece devletlerin yönettiği bir süreç değil, aynı zamanda çok sayıda farklı aktörün yer aldığı, daha karmaşık bir yönetim biçimi olarak tanımlanabilmektedir. Bu kavram,

esasen uluslararası ilişkilerin sadece diplomatik ya da askeri anlamda değil, ekonomik, çevresel, kültürel ve teknolojik boyutlarda da şekillendiğini göstermektedir (Karns ve Mingst, 2010). Küresel yönetişimin bu çok aktörlü doğası, devletlerin geleneksel yönetim araçlarının yanında, uluslararası iş birliklerini ve çok taraflı mekanizmaları da içermektedir.

Küresel yönetişim, uluslararası kuruluşlar ve devletler arasındaki etkileşimin yanı sıra, özel sektör ve sivil toplum gibi aktörlerin de dahil olduğu bir süreç olarak çalışmaktadır. Bu süreçte, devletler çoğunlukla uluslararası düzeyde politika oluşturma ve uygulama süreçlerinde birincil rolü oynarken, özel sektör ve sivil toplum örgütleri gibi aktörler de küresel sorunların çözülmesinde önemli katkılarda bulunmaktadır (Biermann ve diğ., 2009). Örneğin, çevre koruma ve iklim değişikliği gibi alanlarda BM gibi küresel aktörler, dünya çapında yönetişim politikalarını belirlerken, aynı zamanda özel sektörün teknolojik yenilikleri ve sivil toplumun farkındalık yaratma faaliyetlerinde de önemli roller üstlenmektedir. Küresel yönetişimde, çok taraflı iş birliği ve uluslararası normların geliştirilmesi gerekliliği, özellikle küresel tehditler karşısında belirgin hale gelmektedir. Bu tehditler, siber güvenlik gibi dijital tehditlerden, iklim değişikliği gibi çevresel sorunlara kadar geniş bir yelpazeye yayılmaktadır. Küresel yönetişimin bu tehditleri etkili bir şekilde ele alabilmesi için, devletler arasında daha fazla iş birliği ve koordinasyon gerekmektedir. Ayrıca, uluslararası hukuk, normlar ve çok taraflı anlaşmalar gibi unsurlar da küresel yönetişimin yapı taşları olarak sıralanmaktadır. (Keohane, 2002).

Küresel yönetişimin temel amaçlarından biri, küresel düzeyde karşılaşılan ortak sorunların çözülmesine yönelik kolektif bir eylem geliştirmektir. Bu, yalnızca uluslararası iş birliğini değil, aynı zamanda her bir aktörün kendi düzeyinde sorumluluk taşımasını da gerektiren bir yaklaşımdır. Bu çerçevede, devletlerin egemenlik hakları ile küresel iş birliği gereksinimleri arasında denge sağlanması önemlidir. Küresel yönetişimde, çeşitli aktörlerin birbirleriyle iş birliği yaparak çözüm üretmesi gerektiği vurgulanmaktadır. (Rosenau & Czempiel, 1992).

Küresel yönetişim kavramı, genellikle uluslararası sorunların çözülmesinde geleneksel egemen devlet anlayışını aşan bir yönetim biçimini ifade etmektedir. Özellikle 21. yüzyılda, siber güvenlik, çevresel krizler ve ekonomik eşitsizlik gibi küresel tehditler, devletlerin ve diğer aktörlerin koordineli bir şekilde hareket etmelerini gerektirmektedir. Bu tehditler karşısında, devletlerin iş birliği yaparak kolektif bir güvenlik ortamı oluşturmaları, küresel yönetişimin gerekliliklerinden biri olarak karşımıza çıkmaktadır. Bu tezde, küresel yönetişim kavramı, siber güvenlik gibi günümüzdeki önemli sorunların çözülmesinde nasıl bir rol oynadığı ve devletlerin, özel sektörün ve diğer aktörlerin bu süreçteki iş birliği potansiyeli incelenmektedir.

Küresel yönetişimin, yalnızca uluslararası ilişkilerdeki aktörler arasında değil, aynı zamanda devlet içindeki çeşitli aktörler arasında da dinamik bir etkileşim gerektirdiği vurgulanmaktadır.

Siber güvenlik, küresel bir yönetim çerçevesi gerektiren önemli bir alandır. (Clarke ve Knake, 2010). Dijital bağılıkların artması ve siber tehditlerin sınır tanımaması, bu alanda uluslararası iş birliğini zorunlu kılmaktadır (Castells, 2010). Ancak dünya genelinde farklı teknik kapasite seviyeleri, yasal düzenlemelerdeki çeşitlilik ve ülkeler arasındaki politik çıkar farklılıkları, siber güvenlikte küresel yönetişimin uygulanmasını zorlaştıran temel faktörlerdir (Kurbalija, 2016). Bununla birlikte, küresel normlar, standartlar ve protokoller oluşturularak bu zorlukların ötesine geçmek için çalışmaların yapılması gerekmektedir. Siber Güvenliğin Küresel Yönetişimdeki aktörleri:

1. Hükümetler ve Ulusal Yönetimler: Ulusal düzenlemelerin uyumlaştırılması ve uluslararası iş birliği mekanizmalarını desteklemeleri beklenmektedir.
2. Uluslararası Örgütler: Birleşmiş Milletler (BM), NATO ve AB gibi örgütler, siber güvenlikteki uluslararası politikaları belirlemede kritik rol oynamaktadırlar.
3. Özel Sektör: Teknoloji şirketleri ve altyapı sağlayıcıları, siber tehditlere karşı savunma mekanizmaları geliştirerek bu alanda liderlik etmektedirler.
4. Sivil Toplum ve Akademik Kuruluşlar: Bilgi paylaşımı, farkındalık artırma ve politika önerileri sağlama konularında önemlidir.
5. Teknik Standart Kuruluşlar: ITU ve İnternet Tahsisli Sayılar ve İsimler Kurumu (ICANN-Internet Corporation for Assigned Names and Numbers) gibi kuruluşlar, teknik altyapının düzenlenmesinde temel aktörlerdir.

Siber tehditlerin sınır tanımaması sebebiyle bir ülkedeki siber saldırı, başka bir ülkenin altyapısını etkileyebilmekte, koordinasyon ve bilgi paylaşımı bu saldırının en kısa sürede bertaraf edilmesinde kritik önem taşımaktadır. Her ülkenin kendi siber güvenlik düzenlemeleri bulunmakla birlikte, bunların uyumlaştırılması uluslararası ticaret ve veri akışı açısından önemli bir faktör olarak değerlendirilmektedir. Siber suçlar, coğrafi sınırları aştığı ve farklı ülkelerdeki bireyler, kurumlar ve altyapılara zarar verdiği için uluslararası iş birliğini zorunlu kılmaktadır. Bu kapsamda, ortak adli mekanizmalar ve teknik önlemler geliştirilmesi, siber suçların önlenmesi ve suçluların adalet önüne çıkarılması açısından kritik öneme sahiptir. Uluslararası hukukun güçlendirilmesi, bilgi paylaşım ağlarının oluşturulması ve ortak operasyonların yürütülmesi gibi adımlar, siber suçlarla etkin mücadelede temel unsurları oluşturmaktadır. Küresel yönetim, teknik kapasitesi düşük ülkelerin desteklenmesini ve siber

güvenlik düzeyinin yükseltilmesini sağlayabilmektedir. Siber güvenlikte küresel yönetim, artan dijital bağımlılıklar ve siber tehditlerle başa çıkabilmek için çağımızın zorunlu bir ihtiyacıdır. Bu alanda etkili bir yönetim sistemi kurmak için hükümetlerin, özel sektörün, uluslararası örgütlerin ve sivil toplumun bir araya gelerek ortak standartlar ve politikalar oluşturması kritik önem taşımaktadır. Küresel yönetim yaklaşımlarının, sadece mevcut tehditlerle mücadelede değil, aynı zamanda daha güvenli bir dijital gelecek inşa etmede de temel rol oynamakta olduğunun unutulmaması gerekmektedir.

Siber güvenlik, küresel yönetimde asimetrik güç dengesizliklerinin öne çıktığı bir alan olarak dikkat çekmektedir. Özellikle teknolojik altyapı ve bilgi birikimi bakımından güçlü olan devletler ve şirketler, daha zayıf aktörlere karşı ekonomik, siyasi ve stratejik üstünlük kurma yolunda bu dengesizlikleri kendi lehine kullanabilmektedir. Bu durum, dijital sömürgecilik olarak adlandırılan yeni bir kavramı ortaya çıkarmıştır (Smith & Jones, 2020). Siber alandaki asimetrik ilişkiler, zayıf tarafların ulusal güvenliklerini riske atarken, güçlü tarafların politikalarını empoze etmesine olanak tanımaktadır. Bu bağlamda, teknolojik üstünlüğe sahip aktörler, yazılım altyapıları, veri toplama araçları ve uluslararası platformlar üzerinden daha az gelişmiş ülkeleri hem ekonomik hem de politik olarak etkisi altına alabilmektedir. Bu durum, küresel yönetimde güç dengelerinin yeniden tanımlanmasını gerektirmektedir. Özellikle, uluslararası hukuk ve normlar yoluyla daha adil bir sistemin oluşturulması, bu sömürgeci eğilimlerin önüne geçilmesinde kilit rol oynamaktadır (Brown, 2021). Dijital sömürgecilik, yalnızca devletler arasında değil, aynı zamanda büyük teknoloji şirketleri ile kullanıcılar arasında da asimetrik bir ilişki doğurmaktadır. Kullanıcı verilerinin kontrolsüz bir şekilde işlenmesi ve bu veriler üzerinden ekonomik kazanç elde edilmesi, küresel ölçekte büyük bir etik ve güvenlik sorunu oluşturmaktadır (Miller & Thompson, 2019). Bu nedenle, siber güvenliğin küresel yönetimde etkin bir şekilde düzenlenmesi, asimetrik tarafların birbirini sömürge haline getirmesinin önlenmesi için kritik bir ihtiyaçtır.

3. SİBER GÜVENLİK ve KOLLUK İLİŞKİSİ

Siber güvenlik, günümüzde yalnızca devletlerin değil, aynı zamanda küresel toplumun her bireyinin, kurumunun ve devlet dışı aktörlerinin karşı karşıya kaldığı karmaşık bir tehdit olarak karşımıza çıkmaktadır. İnternetin, dijitalleşmenin ve küreselleşmenin etkisiyle, siber tehditler giderek daha sofistike hale gelmekte, buna bağlı olarak devletler ve uluslararası kuruluşlar, küresel güvenliği sağlamak adına siber güvenlik stratejilerini güçlendirme gereksinimi duymaktadır. Küresel yönetişimde bu tehditlere karşı etkin bir mücadele, yalnızca devletlerin değil aynı zamanda çoklu aktörlerin de iş birliği ve koordinasyonunu gerektirmektedir. Bu noktada, kolluk kuvvetleri (polis teşkilatları ve diğer güvenlik birimleri), devletlerin siber güvenlik politikalarının uygulanmasında ve siber suçlarla mücadelede kritik bir rol üstlenmektedir (Bojadžijev ve Fidler, 2018).

Kolluk kuvvetlerinin siber güvenlik alanındaki rolleri, yerel güvenliği sağlamaktan çok daha öte bir boyuta ulaşmaktadır. 21. yüzyılda, internet ve dijital ağların yaygınlaşmasıyla birlikte siber suçlar, yalnızca ulusal sınırlar içinde değil, küresel düzeyde de sorunlar yaratmaya başlamaktadır. Bu tehditler, siber saldırılar, fidye yazılımları, kimlik hırsızlığı, dijital casusluk ve terörizme kadar geniş bir yelpazeye yayılmaktadır (Nissenbaum, 2019). Kolluk kuvvetlerinin bu tehditlere karşı etkili olabilmesi sadece ulusal düzeyde değil, uluslararası iş birliği çerçevesinde de bir koordinasyon gerektirmektedir. Bu bağlamda, kolluk kuvvetlerinin, siber güvenlik alanındaki faaliyetleri, siber suçların takibi, dijital delillerin toplanması ve siber suçluların yargıya sevk edilmesi gibi operasyonel görevlerle sınırlı olmayıp, bu tür suçlarla mücadelede uluslararası iş birliği ağlarının kurulmasında da kritik bir rol oynamaktadırlar (Finklea, 2018).

Siber suçlarla mücadelede kolluk kuvvetleri, devletin iç hukuk sisteminin etkinliğini arttırmak ve iş birlikleri aracılığıyla küresel düzeydeki tehditlere karşı güvenliği sağlamak için gerekmektedir. Ancak, küresel siber tehditler, ulusal sınırların ötesine geçerken, ülkeler arasında farklı yasal, kültürel ve siyasi yapılar olması, bu iş birliklerini karmaşık hale getirebilmektedir. Bu noktada, uluslararası organizasyonlar ve çok taraflı iş birlikleri, siber güvenlik alanında etkin bir yönetim için gerekmektedir (Biermann ve diğ., 2009). INTERPOL, EUROPOL gibi kuruluşlar, siber suçlarla mücadelede devletler arası iş birliğini teşvik eden platformlar sunarak kolluk kuvvetlerinin küresel bir ağ içinde daha etkili olmasını sağlamaktadır. Ayrıca bu tür organizasyonlar, kolluk kuvvetlerinin siber suçlar konusunda bilgi ve becerilerini geliştirebilmeleri için eğitim ve strateji geliştirme olanakları da sunmaktadır (McGuire, 2020). Kolluk kuvvetlerinin siber güvenlikteki rolü, yalnızca suçların tespiti ve

cezalandırılmasından ibaret değildir. Aynı zamanda, siber güvenlik politikalarının şekillendirilmesinde, tehditlerin önceden tespit edilmesinde ve erken uyarı sistemlerinin kurulmasında da önemli işlevleri bulunmaktadır. Kolluk kuvvetleri, siber tehditler ve suçlarla ilgili verileri toplayarak, kamu güvenliği konusunda istihbarat sağlamada önemli bir aktör haline gelmektedir (Lemos, 2019). Bunun yanı sıra, kolluk kuvvetleri aracılığıyla devletler arasında koordinasyon artmakta olup, siber suçlarla mücadeledeki önemi giderek daha fazla anlaşılmaktadır. Özellikle siber suçlar ve dijital suçlar sınır aşan niteliklere sahip olduğu için ulusal sınırlar içinde yapılan operasyonların yanı sıra uluslararası iş birliği ve ortak operasyonlar da büyük önem taşımaktadır (Finklea, 2018).

Siber güvenlikteki iş birliğini artıran bir diğer faktör de devletlerin siber güvenlik stratejilerinin küresel düzeyde uyumlu hale gelmesi gerektiğidir. Bu stratejiler, siber suçları tespit etme, önleme, engelleme ve cezalandırma süreçlerinde ortak standartların geliştirilmesini sağlamaktadır. Örneğin Birleşmiş Milletler, AB ve NATO gibi uluslararası organizasyonlar, siber güvenlik alanında standartların belirlenmesi ve bu standartlara uyum sağlanması noktasında kolluk kuvvetlerine rehberlik etmektedir (Miller, 2019). Böylece kolluk kuvvetleri ulusal düzeyde ve uluslararası iş birlikleri çerçevesinde etkili bir şekilde siber güvenliği sağlamak adına gerekli mekanizmaları kurmakta önemli bir rol oynamaktadır. Bu tezde kolluk kuvvetlerinin siber güvenlik alanındaki rollerini ve bu aktörlerin küresel yönetimdeki etkileri analiz edilmektedir. Siber güvenlikteki tehditler ve siber suçların uluslararası boyutta nasıl daha etkin bir şekilde yönetilebileceği üzerine değerlendirmelerde bulunmakta, kolluk kuvvetlerinin bu bağlamdaki stratejik işlevlerine odaklanılmaktadır.

3.1. Siber Suç Nedir?

Siber güvenlik ve kolluk kuvvetleri arasındaki ilişki, günümüzün dijitalleşmiş dünyasında giderek daha önemli bir hal almaktadır. Dijital teknolojilerin gelişmesi, küresel bağlamda birçok fırsat yaratırken, aynı zamanda siber suçlar gibi yeni tehditleri de beraberinde getirmiştir. Siber suçlar, geleneksel suç türlerinden farklı olarak, sanal ortamda işlenmesi ve sınır tanımaması nedeniyle, geleneksel kolluk kuvvetlerinin müdahale etmesini zorlaştıran dinamiklere sahip olmaktadır. Bu sebeple siber suçlarla mücadele sadece yerel düzeyde değil küresel düzeyde de iş birliğini gerektiren, çok aktörlü bir çaba haline gelmektedir (Finklea, 2018). Siber suçlar bireylerin, kurumların ve devletlerin dijital sistemlerine zarar vermek, bilgi çalmak veya sistemleri bozmak amacıyla yapılan yasa dışı faaliyetleri kapsamaktadır. Siber saldırılar, kimlik hırsızlığı, finansal dolandırıcılık, siber zorbalık, veri ihlalleri ve dijital casusluk gibi birçok alt kategoriye ayrılabilir (McGuire, 2020). Bu tür suçların

yaygınlaşması, siber güvenlik önlemlerinin artırılmasına ve bu suçlarla mücadele eden kolluk kuvvetlerinin rolünün yeniden şekillendirilmesine yol açmaktadır. Kolluk kuvvetleri, bu tür suçlarla mücadelede sadece suçları tespit etmekle kalmaz, aynı zamanda dijital delilleri toplamak, suçluları yargıya sevk etmek ve suç öncesi ve sonrası operasyonel stratejiler geliştirmek gibi kritik görevler üstlenmektedir (Bojadžijev ve Fidler, 2018).

Siber suçlar, geleneksel suçlarla kıyaslandığında tek bir ulusal sınır içinde kalmayabilmektedir. Özellikle siber suçlar, dijital ağların ve internetin küresel doğası nedeniyle, sınır aşan niteliklere sahip olmaktadır. Birçok siber suç, uluslararası düzeyde iş birliğini gerektirmektedir. Bunun yanı sıra, kolluk kuvvetlerinin siber suçlarla mücadelede başarılı olabilmesi için, dijital teknolojilere olan hâkimiyetinin artırılması, ulusal ve uluslararası yasal düzenlemelerin uyumlu hale getirilmesi gerekmektedir. Bu süreçte, farklı ülkeler arasındaki yasal farklılıklar, siber suçların uluslararası alanda takibinin zorlaştırılmasına neden olabilmektedir. Ancak, küresel düzeydeki siber suçlarla mücadele için INTERPOL, EUROPOL gibi uluslararası kolluk kuruluşları da önemli bir iş birliği platformu sağlamaktadır (Biermann ve diğ., 2009). Siber güvenlik ve kolluk kuvvetlerinin ilişkisini anlamak aynı zamanda siber suçların önlenmesi ve bu suçlarla mücadeleye yönelik stratejilerin geliştirilmesi açısından da önemli olmaktadır. Kolluk kuvvetleri siber güvenlik stratejilerinin uygulanmasında kritik bir aktör olarak hem devletlerin siber güvenliğine katkı sağlamakla hem de bireyleri dijital tehditlere karşı korumakla sorumlu olmaktadır. Bu sorumluluk yalnızca suçların soruşturulması ve suçluların tespiti ile sınırlı değil, kolluk kuvvetlerinin aynı zamanda halkı bilinçlendirme, siber güvenlik politikalarını destekleme ve siber suçlarla mücadelede toplumla iş birliği yapma gibi sosyal sorumlulukları da bulunmaktadır (Lemos, 2019). Bununla birlikte kolluk kuvvetlerinin etkili bir şekilde çalışabilmesi için siber suçlarla ilgili ulusal ve uluslararası iş birliklerinin güçlendirilmesi büyük önem taşımaktadır. Siber güvenlik ve kolluk kuvvetleri arasındaki ilişkinin özellikle siber suçlar bağlamında nasıl şekillenmeye devam etmektedir. Siber suçların küresel ölçekteki etkisi ve kolluk kuvvetlerinin bu suçlarla mücadeledeki rolü artmakta uluslararası iş birliklerinin önemine de giderek belirginleşmektedir.

3.2. Siber Suçlarla Mücadelede Kolluk Kuvvetlerinin Rolü ve Karşılaştıkları Sorunlar

Siber suçlar, teknolojinin hızla yaygınlaşmasıyla birlikte küresel düzeyde önemli bir tehdit haline gelmiştir. Bu tehditlere karşı koymada kolluk kuvvetlerinin üstlendiği rol, yalnızca yerel düzeyde değil uluslararası arenada da stratejik bir öneme sahip olduğu değerlendirilmektedir (Wall, 2007). Kolluk kuvvetlerinin siber suçlarla mücadelede hem teknik uzmanlık hem de hukuki düzenlemelerle donatılması gerekmektedir (Holt ve Bossler, 2015). Tarihte kolluk

kuvvetlerinin siber suçlarla mücadelesine dair önemli olaylar bulunmaktadır. Örneğin, 2000 yılında gerçekleşen "I Love You" virüsü saldırısı, dünya çapında milyonlarca bilgisayara zarar vermiş olup, bu olay siber tehditlerin sınır tanımadığını ve uluslararası iş birliğinin önemini göstermektedir. Filipinler kolluk kuvvetleri saldırının sorumlusunu yakalamakta zorluk çekmiş olup, olay siber suçlarla mücadelede ulusal yasaların güncellenmesi gerekliliğini ortaya koymaktadır. (Goodman, 2016). Bir diğer örnek, 2017 yılında gerçekleşen "WannaCry" fidye yazılımı saldırısı olarak karşımıza çıkmaktadır. Bu saldırıda, dünya genelinde binlerce kurumun sistemleri etkilenmiş, kolluk kuvvetlerinin siber tehditlere hızlı yanıt verebilmesi ve uluslararası iş birliğini güçlendirmesi gerektiğini vurgulamaktadır. (Hutchings, 2018).

Kolluk kuvvetleri, siber suçlarla mücadelede çeşitli sorunlarla karşılaşmaktadır. Bu sorunların başında teknolojik altyapının yetersizliği gelmektedir. Birçok ülkenin kolluk birimleri, siber tehditlere yanıt verecek yeterli teknik donanım ve eğitime sahip değildir (Jaishankar, 2011). Ayrıca, siber suçların doğası gereği sınır ötesi nitelikte olması, uluslararası iş birliğini zorunlu kılmaktadır. Ancak farklı ülkelerin hukuki ve teknik altyapılarındaki uyumsuzluk, bu iş birliğini zorlaştırmaktadır (Carr, 2016). Bir diğer sorun, siber suçların hızlı bir şekilde değişen ve karmaşık yapısıdır. Kolluk kuvvetlerinin bu dinamik tehdide uyum sağlayabilmesi için sürekli bir eğitim ve kapasite geliştirme programlarına ihtiyaç duyulmaktadır (Lavorgna, 2014). Ayrıca kişisel veri gizliliği ve ifade özgürlüğü gibi etik konular, siber suçlarla mücadelede kolluk kuvvetlerinin hareket alanını sınırlayabilmektedir (Taylor ve diğ., 2019). Siber suçlarla mücadelede kolluk kuvvetlerinin rolü; teknolojik, hukuki ve uluslararası iş birliği boyutlarını içeren çok yönlü bir yaklaşımı gerektirmektedir. Tarihteki örnekler ve mevcut zorluklar bu alanın daha fazla geliştirilmesi gerektiğini açıkça göstermektedir. Siber güvenlik, günümüzün dijital dünyasında devletlerin güvenliğini sağlamada ve siber suçlarla mücadelede kritik bir rol oynamaktadır. Küresel çapta artan siber suçlar ve tehditler, devletlerin yalnızca ulusal düzeyde değil, aynı zamanda uluslararası iş birliği ve koordinasyon içinde hareket etmelerini gerektirmektedir. Siber güvenlik stratejileri bu bağlamda kolluk kuvvetlerinin iş birliği ile şekillenmekte ve ülkeler arasındaki bilgi paylaşımını ve ortak çalışma mekanizmalarını güçlendirmektedir.

Küresel siber güvenlik yönetişimi, uluslararası düzeyde siber suçlarla mücadele etmek ve dijital dünyada güvenliği sağlamak amacıyla devletler ve uluslararası organizasyonlar arasında iş birliğini teşvik eden bir çerçeve olarak çizilmiştir. Bu yönetim, ülkelerin siber güvenlik standartlarını belirlemeleri, siber suçlarla mücadele etmeleri ve bu suçların cezalandırılmasına yönelik uluslararası iş birliklerini güçlendirmelerine olanak tanımaktadır (Schjolberg, 2017).

Kolluk kuvvetlerinin siber güvenlik alanındaki rolü, yalnızca suçları soruşturmakla kalmayıp aynı zamanda uluslararası siber suç ağlarını izlemek, analiz etmek ve bu suçlarla mücadelede koordinasyon sağlamak olarak da tanımlanabilmektedir. (Wall, 2017). Kolluk kuvvetlerinin küresel siber güvenlik stratejilerine katılımı, dünya genelinde siber suçların daha etkili bir şekilde önlenmesi ve cezalandırılmasına olanak tanımaktadır. Bunun yanı sıra, siber güvenlik tehditlerinin çeşitliliği ve karmaşıklığı göz önünde bulundurulduğunda, uluslararası iş birliğinin önemi giderek artmaktadır. Bu bağlamda Türkiye, Fransa ve ABD gibi ülkelerin siber kolluk teşkilatları, küresel yönetişime önemli katkılarda bulunmaktadır.

3.3. Küresel Siber Güvenlik Endeksi ve Kolluk Kuvvetlerinin Rolü

Küresel Siber Güvenlik Endeksi (Global Cybersecurity Index- GCI), ülkelerin siber güvenlik kapasitesini ölçmek ve karşılaştırmak amacıyla ITU tarafından geliştirilen bir endekstir. Bu endeks, siber güvenlik konusunda ülkelerin yeteneklerini beş ana boyutta değerlendirmektedir: yasal önlemler, teknik kapasiteler, organizasyonel önlemler, kapasite geliştirme ve iş birliği (ITU, 2021). Endeks, ülkelerin siber güvenlik politikalarının etkinliğini değerlendirmede ve küresel standartlara uygunluğunu belirlemede önemli bir araç olarak literatürde geniş bir şekilde ele alınmaktadır (Kshetri, 2016). Endeksin oluşturulmasında kullanılan yöntemler hem nicel hem de nitel verilerin bir araya getirilmesiyle şekillenmektedir. GCI, ülkelerin ulusal siber güvenlik stratejilerinden teknik müdahale ekiplerinin varlığına kadar geniş bir veri yelpazesini kapsamaktadır. Literatürde, bu tür indekslerin, siber tehditlere karşı uluslararası iş birliği ve kapasite geliştirme girişimlerini teşvik ettiği vurgulanmaktadır (Schia ve Gjesvik, 2020). GCI’da üst sıralarda yer alan ülkeler, genellikle güçlü bir siber güvenlik altyapısına ve gelişmiş düzenleyici mekanizmalara sahip olmalarıyla dikkat çekmektedir. Örneğin ABD, Birleşik Krallık ve Güney Kore gibi ülkeler, yüksek teknik kapasiteye ve gelişmiş yasal düzenlemelere sahip olmaları nedeniyle endekste yüksek puanlar almıştır (ITU, 2021; Carr, 2016). Buna karşın, gelişmekte olan ülkeler, siber güvenlik kapasitelerini artırma konusunda çeşitli zorluklarla karşılaşmaktadır (Tanczer ve diğ., 2018). GCI’nın bir diğer önemli yönü, siber güvenlikte bölgesel ve küresel farkları görünür kılmasıdır. Endeks sonuçları, bölgesel farklılıkların giderilmesi için hedef odaklı politikaların geliştirilmesi gerektiğini ortaya koymaktadır. Bu bağlamda, GCI’nın özellikle kapasite geliştirme ve iş birliği alanlarındaki verileri politika yapıcılar için yol gösterici bir kaynak niteliğinde olduğu değerlendirilmektedir (Hathaway ve diğ., 2012).

GCI, siber güvenlik kapasitesinin ölçülmesi ve karşılaştırılması için önemli bir araç olarak, literatürde, endeksin uluslararası iş birliğini teşvik etme ve siber güvenlik politikalarının

geliştirilmesine katkıda bulunma potansiyeli sıkça vurgulanmaktadır. GCI'nın bu çok boyutlu yaklaşımı, siber güvenlik alanında daha etkin stratejilerin geliştirilmesine olanak sağlamaktadır. GCI'siber güvenliğin küresel yönetişime olumlu yönde katkıları bulunmaktadır. GCI siber güvenliği ulusal sınırları aşan bir mesele olarak ele almakta ve ülkeler arasında karşılaştırmalar yaparak bu konuyu küresel yönetim alanında daha görünür hâle getirmektedir. Siber güvenliğin ölçülmesi ve değerlendirilmesi uluslararası toplumu bu alandaki eksiklikleri daha somut bir şekilde görmeye teşvik etmektedir. Örneğin, düşük puan alan ülkeler endeks sonuçlarına dayanarak politika reformlarına gitmektedir (ITU, 2021). Endeks, ülkeler arasında standartlaştırılmış bir değerlendirme sistemi sunarak politika yapıcılarını, uluslararası normlara uyum sağlamaya yönlendirmektedir. Özellikle Budapeşte Siber Suçlar Sözleşmesi gibi uluslararası çerçevelerin benimsenmesi ülkelerin GCI puanlarını artıran bir unsurdur (Singh ve Chakraborty, 2020). Bu, ülkeler arasında daha fazla iş birliğini ve uyumlu politika yaklaşımlarını teşvik eder. Endeksin sonuçları, ülkelerin yalnızca ulusal kapasitelerini artırmakla kalmayıp aynı zamanda bölgesel ve uluslararası iş birliği mekanizmalarını geliştirmesi gerektiğini vurgulamaktadır. Özellikle gelişmekte olan ülkelerin siber güvenlik kapasitelerini artırmak için kalkınmış ülkelerle ortak projeler geliştirmesi, küresel yönetişimi güçlendiren bir unsur olarak karşımıza çıkmaktadır (Kshetri, 2021). GCI, bu iş birliği ihtiyacını açık bir şekilde ortaya koymaktadır. GCI, ülkelerin siber güvenlik alanındaki eksikliklerini belirleyerek kapasitelerini geliştirmeleri için rehberlik sağlamaktadır. Örneğin birçok ülke, yasal düzenlemelerini ve siber suçlarla mücadele mekanizmalarını GCI'nın sunduğu değerlendirme kriterlerine göre yeniden yapılandırmıştır. Bu durum, küresel yönetişimin temel ilkelerinden biri olan kapasitelerin eşitlenmesine doğrudan katkı sunmaktadır (Abdulrauf ve Basu, 2022). GCI, siber güvenlik konularını ortak bir tehdit algısı çerçevesinde sunarak, uluslararası toplumu topyekûn eyleme yönlendirmektedir. Endeksin sonuçları, özellikle kritik altyapıların korunması ve siber suçların önlenmesi konularında küresel bir dayanışma kültürü oluşturmayı hedeflemektedir (Choucri, 2012).

Tablo 3. 1. Küresel Siber Güvenlik Endeksinde Rol Model Ülkeler

Küresel Siber Güvenlik Endeksi Küresel Katman Performansı			
Avusturalya	Gana	Fas	Slovenya
Bahreyn	Yunanistan	Hollanda	İspanya
Bangladeş	İzlanda	Norveç	İspanya
Belçika	Hindistan	Umman	İsveç
Brezilya	Endonezya	Pakistan	Tanzanya
Birleşik Krallık	İtalya	Portekiz	Tayland
Danimarka	Japonya	Katar	Türkiye
Mısır	Ürdün	Kore	BAE
Estonya	Kenya	Ruanda	Kıbrıs
Finlandiya	Lüksemburg	Suudi Arabistan	ABD
Fransa	Malezya	Sırbistan	Vietnam
Almanya	Mauritius	Singapur	

*GCI, 2024 (<https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx>)

Kolluk kuvvetleri, siber suçlarla ilgili yasaların etkin bir şekilde uygulanmasından sorumludur. Siber saldırılar, veri ihlalleri ve diğer dijital suçlarla mücadelede kanunların uygulanması kolluk kuvvetlerinin başarılı operasyonlar yürütmesini gerektirmektedir (INTERPOL, 2021). Siber tehditleri belirlemek ve bunlara karşı harekete geçmek için kolluk kuvvetleri, güncel teknolojiler ve uzman ekipler kullanmaktadır. Bu kapsamda siber olaylara hızlı yanıt verebilmek için gelişmiş analiz ve tespit sistemleri kritik bir rol oynamaktadır (ITU, 2021). Kolluk kuvvetleri, ulusal siber güvenlik stratejilerinin uygulanmasında çok önemli bir destek mekanizması sağlamaktadır. Kritik altyapıların korunması, acil durum planlarının uygulanması ve farkındalık kampanyalarının yaygınlaştırılması gibi alanlarda önemli katkı sağlamaktadır (Ulaştırma ve Altyapı Bakanlığı, 2013). Siber tehditlerin sınır ötesi doğası nedeniyle kolluk kuvvetleri, INTERPOL gibi uluslararası örgütlerle iş birliği yaparak bilgi paylaşımı ve koordinasyon sağlamaktadır. Bu ortak çalışmalar, organize siber suç gruplarını hedef alır ve küresel düzeyde caydırıcı etki yaratmaktadır (INTERPOL, 2021). Kolluk kuvvetlerinin etkinliği, GCI’da ülkelerin skorlarını doğrudan etkilemesi sebebiyle kolluk kuvvetlerinin uluslararası iş birlikleri, GCI değerlendirmelerinde iş birliği kategorisini güçlendiren önemli bir etken olduğu söylenebilmektedir. FBI ve DHS gibi ABD kurumları, INTERPOL ve EUROPOL gibi uluslararası kuruluşlarla ortak çalışarak siber suçlarla mücadelede küresel bir ağ oluşturmaktadır. Örneğin, INTERPOL’ün siber suçların yönetimi girişimlerinde ABD’nin aktif rol oynaması, uluslararası iş birliklerinin güçlenmesini sağlamaktadır (INTERPOL, 2021). Yasal önlemler, ulusal stratejiler ve teknik kapasite gibi değerlendirme kriterleri, kolluk kuvvetlerinin performansı ile yakından ilişkilidir ve bu ilişkiler ülkelerin GCI’daki konumlarında etkili olmaktadır.

3.4.Kamu Kurumlarının Kurumsal Siber Güvenliđi

Kamu kurumlarının kurumsal siber güvenliđi, günümüzün dijitalleşmiş dünyasında devletin, vatandaşlarının ve kurumlarının güvenliđini sağlamak amacıyla kritik bir öneme sahiptir. Dijital teknolojilerin hızla yayılması, kamu sektörü hizmetlerinin internet ve dijital altyapılar üzerinden sunulmasına olanak sağlamış olsa da bu durum aynı zamanda siber saldırılar ve dijital tehditler karşısında savunmasız hale gelmelerine de yol açmaktadır. Bu tehditler, kişisel verilerin çalınması, kritik altyapıların hedef alınması, devletin bilgilerine sızılması gibi birçok ciddi sonucu beraberinde getirebilmektedir (Bojadžijev ve Fidler, 2018). Kamu kurumlarının siber güvenliđi, yalnızca teknolojik önlemlerle değil, aynı zamanda yasal, organizasyonel ve eğitimsel stratejilerle de şekillenmektedir. Kamu kurumları, devletin çeşitli hizmetlerini dijital ortamda sunan, veri depolayan ve kritik altyapı sağlayan kurumlar olduğundan, bu kurumların siber güvenliđi tüm devletin güvenliđini doğrudan etkilemektedir. Özellikle sağlık, eğitim, enerji, ulaşım ve finans gibi alanlarda faaliyet gösteren kamu kurumlarının altyapıları, siber saldırılar ve veri ihlalleri gibi tehditlere karşı savunmasızdır. Kamu kurumlarının siber güvenliđini sağlamak hem iç hizmetlerin sürekliliđini hem de vatandaşların güvenliđini korumak açısından hayati bir önem taşımaktadır (McGuire, 2020). Bununla birlikte, siber güvenlik, yalnızca teknolojik önlemlerle sağlanamayacak kadar geniş bir kapsamı içermektedir. Kamu kurumlarının siber güvenliđini sağlamak için, devletlerin ve kurumların doğru bir siber güvenlik kültürü geliştirmeleri, personel eğitimi sağlamaları ve siber güvenlik stratejilerini sürekli olarak güncellemeleri gerekmektedir (Finklea, 2018).

Kamu kurumlarının siber güvenlik stratejilerinin başarılı olabilmesi için, genellikle bir dizi önlem alınması gerekmektedir. Bu önlemler, kurumların dijital altyapılarının güvenliđini sağlamanın yanı sıra, kamu hizmetlerinin her aşamasında siber güvenlik risklerinin minimize edilmesini hedeflemektedir. Bu bağlamda, siber güvenlik politikalarının oluşturulması, tehditlerin erken tespiti, siber saldırıların engellenmesi ve siber krizlere müdahale gibi başlıca faaliyetler önemli yer tutmaktadır. Bu tür stratejilerde yer alan "siber güvenlik çerçeveleri", ulusal ve uluslararası normlar ile uyumlu olmalı, aynı zamanda sektörel ihtiyaçlar göz önünde bulundurularak özelleştirilmesi gerekmektedir (Biermann ve diğ., 2009). Kamu kurumlarının siber güvenliđini sağlamak için uygulanabilecek en önemli stratejilerden biri, devletin siber güvenlik konusundaki düzenlemelerini güçlendirmektir. Devletler, kamu kurumlarının siber güvenliđi için belirli düzenlemeler ve yasalar oluşturmakta, aynı zamanda bu yasaların uygulanmasını denetlemektedir. AB'nin Genel Veri Koruma Yönetmeliđi (GDPR) gibi siber güvenlik düzenlemeleri, yalnızca verilerin korunmasını değil, aynı zamanda kurumların siber

güvenlik altyapılarının güçlendirilmesini de sağlamaktadır. Benzer şekilde, ABD’de Federal Bilgi Güvenliği Modernizasyonu Yasası (FISMA), federal kurumların siber güvenlik önlemlerini yasal bir çerçeveye oturtarak, devletin tüm kurumlarında güvenliğin sağlanmasına yönelik standartlar getirmektedir (Biermann ve diğ., 2009).

Siber güvenlik alanındaki düzenlemelerin yanı sıra, kamu kurumlarında siber güvenlik kültürünün oluşturulması ve bu kültürün kurum çapında benimsenmesi de oldukça önemlidir. Kurumların personeline yönelik düzenlenen eğitim programları, çalışanların siber güvenlik tehditlerine karşı bilinçlenmesini sağlayarak, güvenlik ihlallerinin önlenmesine katkı sağlamaktadır. Ayrıca, siber güvenlik uzmanlarının yer aldığı özel birimlerin oluşturulması, kurumların siber saldırılara karşı daha hızlı ve etkili bir şekilde yanıt vermelerini sağlamaktadır (McGuire, 2020). Kamu kurumlarının siber güvenliğinde yalnızca iç hizmetlerle sınırlı kalmayıp, aynı zamanda dış paydaşlarla olan etkileşimde de güvenliğin sağlanması önemli görülmektedir. Bu bağlamda, kamu kurumlarının, özel sektör ve diğer kamu kurumları ile iş birliği yaparak siber güvenlik önlemlerini entegre etmeleri gerekmektedir. Küresel düzeyde, siber güvenlik tehditleri sınır tanımadığından, uluslararası iş birlikleri de bu süreçte kritik rol oynamaktadır. Bu sebeple, devletler ve kamu kurumları, uluslararası siber güvenlik çerçeveleri ile uyumlu hale gelmek için çaba göstermeli ve diğer ülkelerle iş birliği yaparak daha güçlü bir siber güvenlik altyapısı oluşturmalıdır (Lemos, 2019). Kolluk teşkilatları, kamu kurumlarının siber güvenliğini sağlarken kamu kurumlarının siber güvenlik politikalarının geliştirilmesi ve uygulanmasındaki zorlukları, fırsatları ve en iyi uygulamaları incelenmekte, bu esnada çeşitli tehditlerle karşı karşıya gelmekte, bu tehditlere karşı önlemler almakta ve gelecekteki güvenlik stratejileri üzerine düzenlemelere katkı sağlamaktadır.



4. TÜRKİYE’DE KOLLUĞUN SİBER GÜVENLİK YÖNETİŞİMİ

Küreselleşme ve dijitalleşme çağında, siber güvenlik, ulusal güvenlik politikalarının ayrılmaz bir parçası haline gelmektedir. Günümüzde artan siber tehditler, sadece bireyleri ve kurumları değil, aynı zamanda devletlerin kritik altyapılarını ve kamu güvenliğini de tehdit etmektedir. Türkiye, coğrafi ve stratejik konumu nedeniyle siber saldırıların hedefinde olan ülkelerden biri haline gelmektedir (Ünal, 2021). Bu bağlamda, siber güvenliğin etkin bir şekilde sağlanması, yalnızca teknik altyapının geliştirilmesiyle değil, kapsamlı bir yönetim yaklaşımıyla mümkün görünmektedir. Siber güvenlik yönetimi, teknik müdahalelerin yanı sıra yasal çerçeve, insan kaynağı kapasitesi ve uluslararası iş birliği gibi unsurları içeren çok boyutlu bir yapıya sahiptir. Türkiye, 2013 yılında yürürlüğe giren Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ile siber güvenlik politikalarını daha sistematik bir çerçevede ele almaya başlamıştır (Bilgi Teknolojileri ve İletişim Kurumu-BTK, 2013). Ancak bu stratejik planların etkinliği, uygulamadaki koordinasyon ve iş birliği düzeyine bağlıdır. Kolluk kuvvetlerinin, siber güvenlik yönetiminde diğer kamu kurumları, özel sektör ve uluslararası kuruluşlarla etkin bir şekilde iş birliği yapması gerekmektedir (Erdoğan, 2022). Tezin bu bölümünde, Türkiye'deki kolluk kuvvetlerinin teşkilat yapılanmalarını, siber güvenlik yönetimindeki rollerini, uluslararası iş birlikleri ile mevcut yönetim yapısının etkinliğini incelenmesi amaçlanmaktadır.

4.1. Türkiye’de Kolluk Yapılanması

Türkiye’de kolluk kuvvetleri, kamu düzeninin korunması, suçun önlenmesi ve soruşturulması, vatandaşların can ve mal güvenliğinin sağlanması gibi görevlerle yükümlenmiştir. Türk kolluk yapılanması, merkezi bir yapıya sahip olup, başlıca dört ana teşkilat tarafından yürütülmektedir; Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı, Sahil Güvenlik Komutanlığı ve Gümrük Muhafaza Genel Müdürlüğü’dür. Bu teşkilatlar, Türkiye Cumhuriyeti Anayasası, ilgili kanunlar ve yönetmeliklere dayanarak görevlerini yerine getirmektedir. Bu tezde ağırlıklı olarak Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı’nın siber güvenlik alanında katkıları anlatılmaktadır. Emniyet Genel Müdürlüğü, İçişleri Bakanlığı’na bağlı olarak faaliyet gösteren bir teşkilattır. EGM, şehir merkezlerinde asayişin sağlanmasından, suç soruşturmalarının yürütülmesinden ve trafik düzeninin korunmasından sorumlu bulunmaktadır. Özellikle büyük şehirlerdeki suçlarla mücadelede ön safta yer almaktadır (İçişleri Bakanlığı, 2022). Teşkilat, merkezi bir yapılanma ile yönetilmekte ve illerde İl Emniyet Müdürlükleri, ilçelerde ise İlçe Emniyet Müdürlükleri aracılığıyla görev yapmaktadır. Ayrıca, siber suçlarla mücadele, organize suçlar, terörle mücadele ve narkotik suçlarla ilgili özel birimlere sahiptir

(Emniyet Genel Müdürlüğü, 2021). Jandarma Genel Komutanlığı, İçişleri Bakanlığı'na bağlı bir teşkilattır. Türkiye'nin kırsal kesimlerinde kamu düzeninin sağlanması ve suçun önlenmesi ile görevli bulunmaktadır. Jandarma, adli kolluk ve askeri görevleri bir arada yürütmektedir (Jandarma Genel Komutanlığı, 2021). Jandarma'nın kırsal bölgelerdeki sorumluluk alanı, genellikle Emniyet Genel Müdürlüğü'nün yetki sınırlarının dışında kalan yerleşim yerlerini kapsamaktadır. Ayrıca, terörle mücadelede etkin bir rol üstlenmekte ve özel operasyon birimleri aracılığıyla kritik görevler yürütmektedir. Sahil Güvenlik Komutanlığı, denizlerde kamu düzeninin korunması, kaçakçılığın önlenmesi ve deniz güvenliğinin sağlanması görevlerini üstlenmiştir. (Sahil Güvenlik Komutanlığı, 2022). Teşkilat, denizlerde yasa dışı göç, kaçakçılık ve çevre kirliliğiyle mücadele gibi görevlerde önemli bir role sahiptir. Ayrıca, arama kurtarma operasyonlarında aktif bir şekilde yer almaktadır. Gümrük Muhafaza Genel Müdürlüğü, Ticaret Bakanlığı'na bağlı olarak sınır kapılarında ve gümrük bölgelerinde kaçakçılıkla mücadele etmekle görevli olup, yasadışı ticaretin önlenmesi, uyuşturucu ve kaçak malların yakalanması gibi görevler üstlenmektedir (Ticaret Bakanlığı, 2022).

Tablo 4. 1. Türkiye'de Kolluk Kuvvetlerinin Yapısı

Kolluk Türü	Bağlı Olduğu Kurum	Görev Alanı	Temel Görevleri	Yasal Dayanaklar
Polis Teşkilatı	T.C. İçişleri Bakanlığı	Kentsel alanlar	Asayişin sağlamak, trafik düzenini denetlemek, suçları önlemek ve soruşturmak.	1934 tarihli Polis Vazife ve Salahiyet Kanunu
Jandarma	T.C. İçişleri Bakanlığı	Kırsal alanlar ve küçük yerleşim yerleri	Asayişin sağlamak, terörle mücadele, trafik denetimi, suç soruşturması yapmak.	1983 tarihli Jandarma Teşkilat, Görev ve Yetkileri Kanunu
Sahil Güvenlik	T.C. İçişleri Bakanlığı	Deniz sınırları ve sahil şeridi	Deniz asayişini sağlamak, kaçakçılıkla mücadele, arama ve kurtarma operasyonları.	1982 tarihli Sahil Güvenlik Komutanlığı Kanunu
Belediye Zabıtası	Yerel Yönetimler	İl ve ilçe belediye sınırları	Kamu düzeni ve çevrenin korunması, ruhsatsız faaliyetlerin denetimi.	5393 sayılı Belediye Kanunu
Gümrük Muhafaza	T.C. Ticaret Bakanlığı	Sınır kapıları, limanlar ve havalimanları	Kaçakçılıkla mücadele, ithalat ve ihracat güvenliğini sağlamak.	2004 tarihli Gümrük Kanunu

Bu tablo açık kaynak verileri kullanılarak yazar tarafından oluşturulmuş olup, Türkiye'deki kolluk teşkilatlarının yasal dayanakları, görev alanları ve sorumlulukları hakkında genel bir çerçeve sunmaktadır.

Türkiye'deki kolluk yapılanması, merkezi bir yönetim altında farklı alanlarda uzmanlaşmış teşkilatlardan oluşmaktadır. Her bir teşkilat, kendi görev alanında kamu düzenini sağlama, suçla mücadele ve vatandaşların güvenliğini sağlama sorumluluğunu üstlenmiştir. Bu yapı gerek kırsal gerekse kentsel alanlarda etkin bir kolluk hizmeti sunmaktadır.

4.2. Türkiye'nin Kolluk Teşkilatlarında Siber Güvenliğin Yeri ve Geliştirilen Stratejiler

Türkiye'de internet ilk kez 12 Nisan 1993'te TÜBİTAK (Türkiye Bilimsel ve Teknolojik Araştırma Kurumu) tarafından lisanslanmıştır. Orta Doğu Teknik Üniversitesi'nde (ODTÜ) ilk internet bağlantısı sağlanmıştır. İlk bağlantı ABD'deki Ulusal Bilim Vakfı (National Science Foundation Network-NFSNET) ağına yapılmış ve bu, Türkiye'nin dijital çağ girişinin başlangıcı olarak kabul edilmiştir. 1990'ların sonları ve 2000'li yılların başında, internet hızla genişlemiş ve bireysel olarak da satışa sunulmuştur. Sosyal medya, e-ticaret ve kamunun dijitalleşmesi, e-devlet uygulamaları gibi yenilikler hayatımıza girmiş, günlük yaşantımızı, kamu kurum ve kuruluşlarının işleyişini kolaylaştırmıştır. Ancak bu genişleme, güvenlik zayıflıklarını ve siber suçların artışı beraberinde getirmiştir. Siber suç kavramının kendini göstermesi sonrasında ulusal mevzuata da suçlarla mücadele kapsamında eklentiler yenilikler yapılmaya başlanılmıştır.

Türkiye'de, siber suç türlerinin ulusal mevzuata girişi 1991 yılında 765 sayılı Türk Ceza Kanunu'na (TCK) kayıtlı "Bilişim Alanında Suçlar" başlıklı kanunun 525/a, b, c ve d maddeleri ile çok kısıtlı bir şekilde olmuştur. Ancak bu düzenleme, bilgisayar sistemlerine yetkisiz giriş, veri tahribi ve bilişim dolandırıcılığı gibi suçlara yönelik ilk hukuki çerçeveyi oluşturmuştur (Türk Ceza Kanunu, 1991). İlerleyen yıllarda dijital teknolojilerin hızla gelişiyor olması sebebiyle mevzuatın güncelleştirilmesi zorunluluk göstermiştir. 2004 yılında 5237 sayılı Türk Ceza Kanun'unda yapılan düzenleme ile bilişim suçlarına yönelik daha kapsamlı bir yaklaşım benimsemiştir. Bu yeni düzenleme "Bilişim Sistemine Girme" (Madde 243), "Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme" (Madde 244) ve "Bilişim Sistemleri Aracılığıyla Dolandırıcılık" (Madde 245) gibi suçlar açıkça tanımlanmış ve cezai yaptırımlar netleştirilmiştir. (5237 Sayılı Türk Ceza Kanunu, 2004). Siber suçlarla mücadeleye ilişkin önemli bir diğer düzenleme, 2007 yılında 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanundur. Bu kanunda, internet ortamında işlenen suçlarla mücadele için içerik sağlayıcılar, yer sağlayıcılar ve erişim sağlayıcılar gibi aktörlere yönelik yaptırımlar bulunmaktadır. Aynı zamanda kanun, çocuk istismarı, yasa dışı kumar, müstehcenlik gibi içeriklerin engellenmesine yönelik yasal mekanizmaları da sunmaktadır (5651 Sayılı Kanun, 2007).

Türkiye'de siber güvenlik alanındaki resmî kurumlar, üç temel hedef çerçevesinde organize edilmektedir. İlk grup, siber suçlarla mücadele etmek ve istihbarat faaliyetleri yürütmek amacıyla çalışmaktadır. İkinci grupta ise kritik altyapıların ve kamu şirketlerinin siber dağıtım hizmetine odaklanılmakta, ayrıca ülkenin siber saldırılara karşı savunma hizmetlerini geliştirmeyi amaçlayan kuruluşlarına yer verilmektedir. Üçüncü grup ise devlet destekli özel girişimlerden oluşmaktadır. Tüm bu bilgilerin oluşturulması planlanması ve Türkiye'nin siber güvenlik politikalarının belirlenmesinde ise üst kurul olarak SGK (Siber Güvenlik Kurulu) sorumlu kuruluştur. (Darıcılı, 2019) Resmî kurumlar siber güvenliğin çok katmanlı, bütüncül yapısı sebebiyle sürekli koordinasyon kurarak iş birliği yapmaktadır.

Türkiye, dijital teknolojilerin hızla gelişmesi ve siber suçların sınır tanımayan doğası nedeniyle, siber güvenlik alanında önemli adımlar atmıştır. Son yıllarda, ülke çapında siber suçlarla mücadele eden kolluk teşkilatlarının yapılandırılması ve güçlendirilmesi hem ulusal güvenliği sağlamak hem de küresel siber suçlarla mücadelede etkin bir aktör olmak amacıyla büyük önem kazanmaktadır. Türkiye, bu bağlamda, siber güvenlik konusunda ulusal stratejiler geliştirirken aynı zamanda uluslararası iş birlikleriyle de siber güvenliği sağlamaya yönelik katkı sunmaktadır. Türkiye'nin temel kolluk birimlerinden olan Emniyet Genel Müdürlüğü bünyesinde Siber Suçlarla Mücadele Daire Başkanlığı (SSMDB) 2013 yılında kurulmuştur (Emniyet Genel Müdürlüğü, 2013). Başkanlık, öncelikle bilişim sistemleri üzerinden işlenen suçların önlenmesi ve bu suçların faillerinin yakalanması amacıyla faaliyet göstermektedir. Kuruluşundan bu yana SSMDB hem ulusal hem de uluslararası düzeyde önemli operasyonlara imza atmaktadır. SSMDB, merkez ve taşra teşkilatından oluşan bir yapıya sahiptir. Merkez teşkilatı Ankara'da bulunmakta olup; strateji geliştirme, uluslararası iş birliklerini yönetme ve üst düzey operasyonların koordinasyonundan sorumludur. Taşra teşkilatları ise her ilde kurulu Siber Suçlarla Mücadele Şube Müdürlükleri üzerinden faaliyet göstermektedir. Bu yapılar, yerel düzeyde siber suçlara müdahale ederken aynı zamanda merkeze bağlı olarak koordinasyon içerisinde çalışmaktadır (Resmî Gazete, 2013). Başkanlık, internet kullanıcılarının karşılaşılabileceği tehditleri önlemek amacıyla farkındalık kampanyaları düzenlemektedir. "Siber Güvenlik Bilinçlendirme Projesi" kapsamında yürütülen çalışmalarda okullarda ve kamu kurumlarında eğitimler verilmekte, internet üzerinden bilgi kirliliğinin önlenmesi hedeflenmektedir (Emniyet Genel Müdürlüğü, 2021). SSMDB, çevrim içi dolandırıcılık, yasa dışı bahis, veri ihlalleri, çocuk istismarı ve terör örgütlerinin dijital propaganda faaliyetlerine karşı etkin operasyonlar yürütmektedir. Siber suçların delillendirilmesi sürecinde adli bilişim çalışmaları kritik bir öneme sahiptir. Başkanlık, suç

unsuru barındıran dijital materyallerin incelenmesi, veri kurtarma ve delil niteliği taşıyan materyallerin mahkemelerde kullanılabilir hale getirilmesi için yoğun mesai harcamaktadır (Emniyet Genel Müdürlüğü, 2020)

Türkiye'de siber suçlarla mücadelede önemli bir rol üstlenen diğer bir yapılanma olan Jandarma Genel Komutanlığıdır. Siber Suçlarla Mücadele Daire Başkanlığı, Jandarma Genel Komutanlığı bünyesinde faaliyet gösteren bir birim olarak kurulmuş, dijital ortamda işlenen suçların önlenmesi, tespiti ve soruşturulmasından sorumludur (Jandarma Genel Komutanlığı, 2024). İl Jandarma Komutanlıkları altında da Siber Suçlarla Mücadele Şube Müdürlükleri bulunmaktadır. Örneğin, Sakarya İl Jandarma Komutanlığı bünyesinde 2021 yılında faaliyete geçen Siber Suçlarla Mücadele Şube Müdürlüğü, dijital dünyada işlenen suçları önlemek, tespit etmek ve soruşturmak amacıyla çalışmalar yürütmektedir. (Sakarya İl J.K.lığı, 2025) Siber Suçlarla Mücadele Daire Başkanlığı'nın temel görevleri aşağıda sıralanmıştır:

- Dijital ortamda işlenen suçların erken tespiti ve önlenmesi amacıyla sürekli izleme ve analiz faaliyetleri yürütmek.
- Siber suçlarla ilgili operasyonlar düzenlemek, suçluların tespitine yönelik çalışmalar yapmak ve diğer kurumlarla iş birliği sağlamak.
- Suçlarla ilgili dijital delillerin toplanması, muhafaza edilmesi ve incelenmesini sağlamak.
- Toplumun siber suçlar konusunda bilinçlendirilmesi amacıyla eğitim ve bilgilendirme faaliyetleri gerçekleştirmek. (JGK, 2024)

Siber suçlarla mücadele, dijitalleşen dünyada güvenlik ve kamu düzeninin süreklilik açısından hayati önem taşımaktadır. Karşılıklı bağımlılık kavramının yaygın olduğu siber güvenlik tehditlerinde ülkelerin kendi yerli teknolojilerini geliştirmeleri de büyük önem arz etmektedir. Türkiye'deki kolluk kuvvetleri, siber suçlarla mücadelede gelişmiş araç ve yazılımla kullanarak etkin bir rol üstlenmektedir. Bu araçların büyük bir kısmı, yerli ve milli üretim anlayışıyla Türk kamu kurumları tarafından geliştirilmiş ve siber tehditlerle mücadelede önemli roller üstlenmiştir. Siberay yapılanması Emniyet Genel Müdürlüğü SSMDDB tarafından 2020 yılında geliştirilmiştir. Siberay, hem dijital kampanyalarını destekleyen hem de dijital tehditlerin genişletilmesi ve analiz edilmesi amacıyla kullanılan bir platform olup, siber suçlara ilişkin veri toplama, olay analizi ve kamuya yönelik eğitim programları bu sistem üzerinden yürütülmektedir. AVCI, AZAD ve KASIRGA yazılımları ise TÜBİTAK BİLGEM (Türkiye Bilimsel ve Teknik Araştırma Kurumu-Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi) tarafından 2018 yılında geliştirilmeye başlanmış olup, AVCI saldırı tespit ve önleme

sistemi olarak geliştirilmiştir. AZAD, ağlarda tehdit algılama ve anormallik tespitinde kullanılan bir yazılımdır. KASIRGA, güvenlik açıklarını önceden belirlemek için kullanılan bir güvenlik test aracıdır. Kolluk kuvvetleri bu araçlarla, özellikle siber saldırıların önlenmesi ve ağ güvenliğinin sürdürülmesinde aktif olarak bulunmaktadır. Türkiye kolluk kuvvetleri için araçları, 2010'lu yıllardan itibaren artan siber tehditlerle mücadele kapsamında geliştirilmeye başlamaktadır. TÜBİTAK, Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve yerel teknoloji firmalarının iş birliğiyle hem adli bilişim hem de siber güvenlik alanlarında yüksek kapasite araçları geliştirmektedir. Bu araçlar, ulusal güvenlikten kamu düzenine kadar geniş bir alanda kullanım ve etkin sonuçlar sağlamaktadır. Türkiye'nin siber suçlarla mücadelede kullandığı araçlar, yerli ve milli teknolojilere sahip portföy, daha güvenilir bir altyapı sunmaktadır. Kolluk güçlerinin bu araçlarla siber suçlarla mücadele etmesi Türkiye'yi daha güçlü bir şekilde konuma getirmektedir.

Siber güvenlik, dijitalleşmenin hız kazandığı günümüzde, ülkelerin ulusal güvenlik politikalarının kritik bir parçası haline gelmiştir. Türkiye, bu kapsamda 2013 yılında Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nı hayata geçirmiştir. Bu strateji, siber tehditlere karşı ulusal düzeyde koordinasyon sağlamayı, altyapıyı güçlendirmeyi ve farkındalık yaratmayı amaçlamaktadır (BTK, 2013). Bu strateji kapsamında siber güvenlik stratejilerinin güçlendirilmesi hedeflenmiş 2013 yılında kurulan Ulusal Siber Olaylara Müdahale Merkezi (USOM), siber tehditlerin önlenmesi ve müdahalesinde kritik bir yapı hâline gelmektedir. USOM'un temel görevi, Türkiye'nin dijital altyapısını tehdit eden siber olaylara karşı hızlı ve etkili müdahalelerde bulunmak, ulusal ve uluslararası düzeyde koordinasyonu sağlamaktır (BTK, 2020). Bu süreçte, kolluk kuvvetleri USOM'un önemli bir paydaşı olarak rol oynamaktadır. Kolluk kuvvetleri, USOM tarafından tespit edilen siber olayların adli boyutunu ele almakta ve suçluların tespiti için gerekli teknik incelemeleri yürütmektedir. Özellikle, Emniyet Genel Müdürlüğü SSMDDB ve Jandarma Genel Komutanlığı SSMDDB, USOM ile iş birliği yaparak yasa dışı çevrimiçi faaliyetlerin izlenmesi ve suçluların adalete teslim edilmesi süreçlerinde etkin bir rol üstlenmektedir (TÜBİTAK, 2019). Kolluk kuvvetleri, USOM'un düzenlediği ulusal tatbikatlara ve eğitim programlarına katılarak siber güvenlik alanındaki kapasitelerini artırmaktadır. Bu, yalnızca teknik bilgi paylaşımını değil, aynı zamanda ulusal güvenlik stratejilerinin siber boyutunun geliştirilmesini de sağlamaktadır. Kolluk kuvvetleri, USOM'un rehberliğinde hareket ederek kritik altyapıların korunmasında da sorumluluk almaktadır (Ulaştırma ve Altyapı Bakanlığı, 2021). Kolluk kuvvetlerinin USOM ile entegrasyonu, geleneksel güvenlik anlayışından uzaklaşarak genişleyen bir güvenlik

perspektifine işaret etmektedir. Klasik güvenlik anlayışında askerî tehditler öncelikli iken, siber güvenlik bağlamında ekonomik, toplumsal ve politik tehditler de güvenlik yelpazesine eklenmektedir. Bu, kolluk kuvvetlerinin yalnızca suçla mücadele eden bir birim olmanın ötesine geçerek ulusal güvenlik aktörü hâline gelmesini gerektirmektedir (Buzan ve diğ., 1998). USOM ve kolluk kuvvetlerinin iş birliği, karşılıklı bağımlılık ilişkisi içinde de değerlendirilmektedir. Siber saldırıların karmaşık yapısı ve çok boyutlu etkileri, farklı kurumlar arasındaki koordinasyonu zorunlu kılmaktadır. Kolluk kuvvetlerinin USOM ile iş birliği, yalnızca saldırıların önlenmesi ve suçluların yakalanması için değil, aynı zamanda uluslararası siber güvenlik normlarının uygulanması için de kritik bir rol oynamaktadır (ITU, 2021). USOM, Türkiye'nin siber güvenlik ekosisteminin temel taşlarından biri olup, kolluk kuvvetlerinin katkısıyla daha etkin bir yapıya kavuşmaktadır. Bu iş birliği, hem siber suçların etkili bir şekilde soruşturulmasını hem de ulusal güvenlik stratejilerinin dijital çağın gereksinimlerine uygun şekilde geliştirilmesini sağlamaktadır. Bu bağlamda, USOM çatısı altında kolluk kuvvetlerinin çalışmaları, Türkiye'nin siber tehditlere karşı direncini artıran önemli bir unsur haline gelmektedir.

2013 yılında yayımlanan planın devamı niteliğinde, 2016 yılında yayımlanan 2016-2019 yıllarını kapsayan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, Türkiye'nin siber suçlarla mücadele çerçevesinde önemli bir dönüm noktası olmaktadır. Bu belgede, kritik altyapıların korunması, siber tehditlere karşı ulusal kapasitenin geliştirilmesi ve yerli teknolojilerin geliştirilmesine yönelik hedefler belirlenmektedir (Ulusal Siber Güvenlik Stratejisi, 2016). Ayrıca, Kişisel Verilerin Korunması Kanunu (KVKK), veri ihlallerine karşı koruma sağlamakta, bilişim alanındaki düzenlemelerin kapsamını genişletmektedir (6698 Sayılı Kişisel Verilerin Korunması Kanunu, 2016). Türkiye'de siber suçlarla mücadeleye yönelik mevzuat, teknolojik gelişmelere paralel olarak sürekli güncellenmektedir. 2020-2023 dönemi Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ve sonrasında 7 Eylül 2024 tarihinde ise 2024-2028 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı yayınlanmıştır. Kolluk teşkilatları da, bu planın uygulanmasında önemli bir role sahiptir. 2024 -2028 Eylem Planı ile bir önceki plan genişletilmiş ve güncelleştirilmiştir. 2024-2028 planı, "insan", "savunma", "caydırıcılık" ve "iş birliği" temaları üzerine inşa edilmiştir. Bu temalar, siber güvenlik stratejisinin somut kazanımlara dönüştürülmesine yönelik bir yapı sunmaktadır. Yeni planda, 18 spesifik hedef belirlenmiştir. Bu hedefler, siber güvenlik ekosisteminin güçlendirilmesi, yerli ve milli teknolojilerin geliştirilmesi, insan kaynağının artırılması ve uluslararası iş birliğinin derinleştirilmesi gibi alanları kapsamaktadır. 2024-2028 planı, önceki plandan farklı olarak,

uygulama sürecinde daha geniş bir paydaş katılımını hedeflemektedir. Kamu kurumları, özel sektör, sivil toplum kuruluşları ve üniversitelerin iş birliği içinde çalışması öngörülmektedir. (Ulusal Siber Güvenlik Stratejisi, 2024) Türkiye'nin 2024-2028 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, önceki planın üzerine inşa edilerek, yeni tehditlere karşı daha kapsamlı ve iş birliğine dayalı bir yaklaşım sunmaktadır. İş birliklerinde ise çok aktörlü çok yönlü bir plan çizilmiştir. Bu plan ile, Türkiye'nin siber güvenlik alanındaki kapasitesini artırmayı ve uluslararası alanda daha etkin bir rol oynamayı amaçladığı görülmektedir. Kolluk kuvvetleri siber bilincin artması amacıyla eğitim faaliyetleri düzenlemekte, geliştirilen yerli yazılımlar ile siber suçlar ortaya çıkmadan önlemekte, siber suçların ortaya çıkmasından sonra ise suçluların yakalanması ve yargıya çıkarılması sürecinde etkin bir rol üstlenerek, planın “savunma” ve “caydırıcılık” temalarında aktif olmaktadır. (CyberArts,2024)

Ulusal Strateji Belgelerinin yanı sıra Türkiye, dijital dönüşüm sürecinde ülke genelinde kamu, özel sektör ve akademik kurumların katılımıyla siber güvenlik alanında bir kümelenme modeli oluşturulmuştur. Siber Güvenlik Kümelenmesi, 2017 yılında T.C. Cumhurbaşkanlığına bağlı Savunma Sanayii Başkanlığı'nın (SSB) liderliğinde kurulmuş olup, ulusal siber güvenlik ekosistemini güçlendirmeyi amaçlamaktadır (Savunma Sanayii Başkanlığı, 2017). Kümelenmenin temel amaçları arasında, yerli ve milli siber güvenlik çözümlerinin geliştirilmesi, sektör oyuncuları arasındaki iş birliğinin artırılması ve nitelikli insan kaynağının yetiştirilmesi yer almaktadır. Bunun yanında, ülke çapında siber tehditlere karşı dayanıklılık oluşturulması ve uluslararası arenada rekabetçi bir siber güvenlik sektörü yaratılması hedeflenmektedir (Siber Güvenlik Kümelenmesi, 2023). Kolluk kuvvetleri, siber güvenlik kümelenmesinin bir parçası olarak konumlanmaktadır. Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve diğer kolluk birimleri, siber tehditlere karşı ilk savunma hattını oluşturmaktadır. Bu bağlamda, SSMDB gibi birimler hem operasyonel hem de stratejik düzeyde kümelenme faaliyetlerine katkı sağlamaktadır. Kolluk kuvvetleri, kümelenme çerçevesinde yürütülen iş birlikleri, bilgi paylaşımı ve eğitim faaliyetlerine aktif olarak katılmakta ve yerli teknolojilerin uygulanmasında öncü rol üstlenmektedir. Siber Olaylara Müdahale Ekipleri (SOME), Türkiye'nin siber güvenlik altyapısında önemli bir yere sahip olup, SOME'ler, kamu ve özel sektör kurumlarında ortaya çıkan siber olaylara hızlı ve etkili bir şekilde müdahale etmeyi amaçlamaktadır. Siber Güvenlik Kümelenmesi, SOME'lerin koordinasyonunu desteklemekte ve bu ekiplerin teknolojiye erişimini kolaylaştırmaktadır. Kolluk kuvvetlerinin SOME ekipleri ile kümelenme içerisindeki paydaşlarla iş birliği yapması, ulusal siber savunma mekanizmalarının daha etkili bir şekilde işlemlerini sağlamaktadır

(USOM, 2023). Siber Güvenlik Kümelenmesi, 2023 yılı itibarıyla 200'den fazla firma ve kurumun katılımıyla faaliyetlerini sürdürmektedir. Bunlar arasında, yerli siber güvenlik firmalarının ulusal ve uluslararası projelerde elde ettiği başarılarla dikkat çekilmektedir. Ayrıca, kümelenme çatısı altında organize edilen Siber Yüz Yüze Günleri, eğitim programları ve fuarlar sektörün gelişimine katkı sunmaktadır. Türkiye'nin siber güvenlik kümelenmesi, yalnızca ulusal seviyede değil, aynı zamanda uluslararası alanda da aktif rol almaktadır. AB'nin Horizon projeleri gibi uluslararası araştırma ve geliştirme programlarına katılım sağlanmakta ve yabancı ortaklıklarla iş birlikleri geliştirilmektedir (European Commission, 2022). Gelecekte, kümelenmenin daha fazla yenilikçi proje ve teknoloji geliştirmesi öngörülmektedir. Türkiye'nin Siber Güvenlik Kümelenmesi, ulusal güvenlik ve ekonomik kalkınma için kritik bir rol üstlenmektedir. Kolluk kuvvetlerinin ve SOME'lerin bu yapıya olan katkısı, ulusal siber savunma sisteminin daha güçlü ve entegre bir şekilde çalışmasını sağlamaktadır. Bu yapının, yenilikçi yaklaşımlarla ülkenin dijital altyapısını daha da güçlendirmesi beklenmektedir.

4.3. Uluslararası İş birliği Örnekleri ve Küresel Yönetişime Katkısı

Siber suçlar, ulusal sınırları aşarak küresel bir tehdit haline gelmiştir. Bu durum, ülkeler arası iş birliğini zorunlu kılmaktadır. Türk kolluk teşkilatları, özellikle Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı, siber suçlarla mücadelede uluslararası kuruluşlar ve diğer ülkelerin güvenlik birimleriyle iş birliği içinde çalışmaktadır. İş birliklerinin temel taşlarını INTERPOL, EUROPOL, BM ve NATO gibi platformlar oluşturmaktadır. Türkiye, 1930 yılında INTERPOL'e üye olmuş ve o tarihten bu yana uluslararası güvenlik iş birliklerinde aktif bir rol üstlenmiştir. (INTERPOL Türkiye, 2023). INTERPOL'ün Küresel Siber Suç Merkezi ve diğer operasyonel birimleriyle güçlü bir iş birliği yürütmektedir. INTERPOL'ün 2022 yılında düzenlediği "Cyber Surge Operation- Siber Dalgalanma Operasyonu" kapsamında Türk Emniyet Teşkilatı, çevrim içi dolandırıcılık ve sahte e-ticaret sitelerine yönelik operasyonlara katılmıştır. Bu operasyon sonucunda 100'den fazla suçlu yakalanmış ve milyonlarca dolar değerinde yasa dışı işlem engellenmiştir (INTERPOL, 2022). Türk yetkililer, INTERPOL'ün Siber Suç Veri Tabanı'nı kullanarak fidye yazılım saldırılarına karşı önemli bilgi paylaşımında bulunmuş ve bu saldırıların arkasındaki uluslararası şebekelere ulaşılmasına katkı sağlamıştır (INTERPOL Türkiye, 2023).

Avrupa'da sınır ötesi siber suçlarla mücadelede EUROPOL kilit bir role sahiptir. Türkiye, 2004 yılında AB ile Geri Kabul Anlaşması kapsamında EUROPOL ile iş birliğini başlatmıştır. 2010 yılında Türkiye ile EUROPOL arasında Operasyonel İş birliği Anlaşması imzalanmış, bu anlaşma siber suçlarla mücadelede daha kapsamlı bir iş birliği yapılmasının önünü açmıştır

(EUROPOL, 2010). 2022 yılında düzenlenen bir operasyonda, EUROPOL iş birliğiyle Türk Emniyet Teşkilatı, uluslararası bir fidye yazılım ağını çökertmiştir. Operasyon kapsamında Türkiye üzerinden saldırı düzenleyen bir grup, kripto para cüzdanlarının izlenmesi yoluyla yakalanmıştır (EUROPOL, 2022). EUROPOL'ün "Operation Dark HunTOR" kapsamında, Türk kolluk kuvvetleri, yasa dışı ürünlerin Darknet üzerinden satışıyla ilgili yerel ve uluslararası bağlantılara ulaşarak 15 şüphelinin yakalanmasına yardımcı olmuştur (EUROPOL, 2021).

Birleşmiş Milletler (BM) ile iş birliğinde ise BM'nin Uyuşturucu ve Suç Ofisi (UNODC) ile Türk kolluk teşkilatları, özellikle siber suçlarla mücadele eğitimleri ve kapasite geliştirme projeleri üzerine yoğunlaşmıştır. 2021 yılında UNODC tarafından düzenlenen bir programda, Türk Emniyet Teşkilatı uzmanları adli bilişim ve dijital delil toplama konularında bölgesel bir eğitim vermiştir. Bu eğitimler, Balkanlar ve Orta Asya ülkelerini de kapsamaktadır (UNODC, 2021). Türk kolluk kuvvetleri, BM ile iş birliği yaparak çevrim içi terör propagandası yapan platformlara karşı düzenlenen bir projede aktif rol oynamaktadır (BM Türkiye, 2022). NATO, siber güvenlik ve savunma alanında uluslararası iş birliğinin geliştirilmesinde önemli bir platformdur. Türk kolluk kuvvetleri, NATO'nun Siber Savunma Mükemmeliyet Merkezi ile koordinasyon halinde çalışmaktadır. 2021 ve 2022 yıllarında Türk Emniyet Teşkilatı, NATO tarafından düzenlenen Locked Shields tatbikatlarına katılarak siber saldırılara karşı savunma ve müdahale yeteneklerini geliştirmiştir (NATO Türkiye, 2021). NATO koordinasyonu, Türk kolluk kuvvetleri siber tehdit istihbaratı paylaşımı yaparak uluslararası saldırılara karşı erken uyarı mekanizmalarının geliştirilmesine katkı sağlamaktadır. Türkiye, 2001 yılında Budapeşte Siber Suçlar Sözleşmesi'ni imzalayarak uluslararası siber suçlarla mücadelede önemli bir adım atmıştır. Bu sözleşme çerçevesinde Türkiye, uluslararası siber suç soruşturmalarında dijital delil paylaşımı yaparak global operasyonlara destek sağlamaktadır. Bu sözleşme kapsamında, diğer ülkelerin talepleri doğrultusunda veri ve suç unsurlarının izlenmesinde Türk kolluk teşkilatları önemli bir rol oynamaktadır (Council of Europe, 2001).

Türk kolluk teşkilatları, uluslararası iş birlikleri sayesinde siber suçlarla mücadelede etkin bir aktör haline gelmiştir. INTERPOL, EUROPOL, BM ve NATO ile ortak yürütülen Türkiye'nin bu alandaki yetkinliğini artırmaktadır. Bu iş birlikleri, Türk kolluk kuvvetlerinin sadece ulusal değil, küresel güvenliğe de katkıda bulunmasını sağlamaktadır. Özellikle, Türkiye'nin imzaladığı Siber Suçlarla Mücadele Kapsamında Uluslararası Anlaşmaları çerçevesinde, diğer ülkelerle bilgi paylaşımı ve teknik destek sağlanması, küresel siber suçlarla mücadeleye önemli bir katkı sunmaktadır. Bu iş birlikleri, Türkiye'nin küresel siber güvenlik politikalarının

etkinliğini artırmakta ve uluslararası alanda daha güçlü bir oyuncu olmasına yardımcı olmaktadır (Finklea, 2018). Türkiye'nin kolluk teşkilatları, siber suçlarla mücadele konusunda ulusal ve uluslararası düzeyde önemli bir sorumluluğa haiz olmaktadır. Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı gibi kurumlar, siber suçlarla mücadelede önemli birer aktör olarak çalışmaktadır.

Türkiye, bölgesel iş birliklerinden olan EUROPOL üyeliğinin yanı sıra, 1998 yılında Avrupa ve Akdeniz Jandarmaları ve Askeri Statülü Kolluk Kuvvetleri Birliği (FIEP) üyesi olmaktadır. Bu üyelik, Türkiye'nin jandarma teşkilatının uluslararası iş birliği ve bilgi paylaşımına katkıda bulunmasını sağlamıştır (FIEP, 2023). FIEP üyeliği, Türkiye'nin kolluk kuvvetlerinin uluslararası standartlara uyumunu artırırken, siber güvenlik gibi yeni tehdit alanlarında da deneyim ve teknoloji paylaşımına olanak tanımaktadır. FIEP, üye ülkeler arasında siber güvenlik alanında iş birliğini güçlendirmek için çeşitli girişimlerde bulunmaktadır. Bu girişimler, küresel yönetişime önemli katkılar sağlamaktadır. FIEP, üye ülkeler arasında siber tehditlerle mücadelede kullanılan en iyi uygulamaların ve teknolojilerin paylaşılmasını teşvik etmektedir. Türkiye, FIEP çatısı altında diğer ülkelerle bilgi ve deneyim paylaşarak, siber tehditlere karşı uluslararası düzeyde koordinasyon sağlamaktadır (FIEP, 2023). FIEP, siber güvenlik eğitimi ve uzmanlık geliştirme programları düzenleyerek üye ülkelerin siber tehditlere karşı daha etkin müdahalede bulunmasını amaçlamaktadır. Türkiye, bu programlara aktif katılım göstererek ulusal kapasitesini artırmakta ve bu deneyimlerini diğer üyelerle paylaşmaktadır (Jandarma Genel Komutanlığı, 2023). FIEP, siber suçlarla mücadelede uluslararası bir ağ oluşturarak sınır ötesi tehditlerin önlenmesinde önemli bir rol oynamaktadır. FIEP'in siber güvenlik çalışmaları, küresel yönetişime önemli katkılar sağlamaktadır. Bu katkılar arasında uluslararası iş birliğinin güçlendirilmesi, sınır ötesi suçların önlenmesi ve küresel güvenlik politikalarının geliştirilmesi yer almaktadır. Türkiye'nin FIEP üyeliği, bu süreçlerde aktif bir rol üstlenerek bölgesel ve küresel güvenliğe katkı sunmaktadır.

Tüm bu veriler ışığında, Türkiye'nin siber güvenlik stratejileri hem iç güvenliği sağlamak hem de küresel siber güvenliğe katkı sağlamak amacıyla geliştirmektedir. Bu doğrultuda yerli ve milli teknolojilerin geliştirilmesi, siber güvenlik uzmanlarının yetiştirilmesi ve uluslararası düzeyde uygun politikaların benimsenmesi, çok paydaşlı organizasyonlarda yer almak operasyonel hedefler arasında yer almaktadır.

Ayrıca, toplumun her kesimine siber bilinci oluşturmak için eğitim programları ve bilinçlendirme kampanyaları düzenlenmekte, siber saldırılara karşı erken uyarı sistemleri ve güçlü müdahale kapasitesi geliştirilmesi hedeflenmektedir. Bütün bu çabalar, Türkiye'nin hem kendi dijital varlığını korumasını hem de küresel siber güvenlik ekosisteminde güvenilir bir ortak olarak yer sağlamasına olanak sağlayacağını değerlendirilmektedir.

4.4. Küresel Siber Güvenlik Endeksinde Türkiye'nin Yeri ve Kolluk Kuvvetlerinin Etkisi

GCI'da Türkiye, yıllar içinde gösterdiği ilerlemeyle dikkat çekmiştir. Kolluk kuvvetleri, siber suçlarla mücadelede önleyici güç olması sebebiyle Türkiye'nin siber güvenlik politikalarının uygulanmasında ve uluslararası standartlara uyum sağlamasında aktif bir rol oynamaktadır. Türkiye, GCI sıralamalarında ilk kez 2014 yılında değerlendirilmiştir. 2017 yılı raporunda, Türkiye 28. sırada yer alması, siber güvenlikte uluslararası bir oyuncu olmaya başladığını göstermektedir (ITU, 2017). Bu dönemde, Emniyet Genel Müdürlüğü (EGM) ve Jandarma Genel Komutanlığı gibi kolluk birimlerinin siber suçlarla mücadelede kapasitesini artırmaya yönelik adımlar atılmıştır. 2020 yılında yayımlanan raporda, Türkiye 193 ülke arasında 20. sıraya yükselmiştir (ITU, 2020). Bu yükseliş, özellikle Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nın yürürlüğe girmesi, etkin bir siber kümelenmesinin sağlanması ve kolluk kuvvetlerinin bu alandaki önleyici etkinliğinin artmasıyla sağlanmaktadır.

2024 yılında rapor sıralama sisteminden değerlendirme sistemine geçiş yapmıştır. Yayımlanan rapora göre, Türkiye, değerlendirilen 194 ülke arasında tüm kriterlerden tam puan alarak "rol model" ülkeler arasında en üst seviyede yer almıştır. (Anadolu Ajansı, 2024). Türkiye'nin dijital teknolojilerde yaşanan trendi yakalayarak siber güvenlik alanındaki literatüre katkıları ve operasyonel faaliyetleri, genişleyen güvenlik anlayışı ve yönetim kavramı çerçevesinde değerlendirildiğinde, klasik yönetim yaklaşımlarının ötesine geçerek, çok paydaşlı ve esnek stratejilerin benimsenmesinin önemini ortaya koymaktadır. Bu alınan puan, Türkiye'nin sadece bölgesel bir güç değil, aynı zamanda küresel düzeyde etkin bir aktör olduğunu göstermektedir. Özellikle bilgi teknolojilerindeki ilerlemeler ve bu alandaki düzenleyici çerçevelerin güçlendirilmesi, Türkiye'yi bu alanda lider ülkelerden biri haline getirmiştir (ITU, 2024). Yumuşak güç kavramı, bir ülkenin kültürü, değerleri ve politikaları aracılığıyla diğer ülkeler üzerinde etki yaratma kapasitesini ifade etmektedir (Nye, 2004). Türkiye'nin siber güvenlik alanında elde ettiği başarı, uluslararası alanda yumuşak güç unsurlarından biri olarak değerlendirilebilmektedir. Siber güvenlikte rol model ülke statüsü, Türkiye'nin uluslararası itibarını artırırken diğer ülkelerle iş birliği fırsatlarını da güçlendirmektedir. Örneğin,

Türkiye'nin siber güvenlik eğitimleri, teknolojik inovasyonları ve uluslararası normlara uyumu, diğer ülkeler tarafından örnek alınan bir model oluşturmıştır. Türkiye'nin siber güvenlik alanındaki bu başarısı hem bölgesel hem de küresel düzeyde stratejik önem taşımaktadır. Bölgesel anlamda, Türkiye'nin liderliği, komşu ülkelerde siber güvenlik kapasitelerinin geliştirilmesine katkı sağlarken; küresel düzeyde, uluslararası organizasyonlar ve iş birlikleriyle teknolojik standartların belirlenmesinde daha etkili bir rol üstlenmesine olanak tanımaktadır. Ayrıca, Türkiye'nin bu başarısı, ekonomik kalkınma ve uluslararası ilişkilerde de önemli bir güç çarpanı olarak değerlendirilebilmektedir (ITU, 2024).

Sonuç olarak, Türkiye'nin GCI'da elde ettiği rol model ülke statüsü, yumuşak güç unsurları çerçevesinde önemli bir başarıdır. Kopenhag Ekolü'nün genişletilmiş güvenlik teorisi çerçevesinde düşünüldüğünde, Türkiye'nin siber güvenliği kapsamlı bir çerçevede yorumlanmakta, devlet kurumlarının rolleri derinleşmekte ve iş birlikleri hem ulusal hem de uluslararası seviyede artmaktadır. İnsani güvenlikten askeri güvenliğe kadar pek çok alanı içinde barındıran siber güvenlik devlet bazında yapılan planlamalarda bu geniş çerçevesiyle ele alınmaktadır. Türkiye'nin, teknolojik altyapısını ve insan kaynağını geliştirme yönündeki kararlılığıyla, siber kümelenme, milli siber teknolojilerin geliştirilmesi, siber suçların kolluk marifetiyle önlenmesi, işlenen suçlarda gerek ulusal düzeyde gerekse uluslararası iş birlikleriyle suçluların adalet önüne çıkarılmasıyla gelecekte siber güvenlik alanında daha da güçlü bir aktör olarak karşımıza çıkacağı değerlendirilmektedir.



5. FRANSA'DA KOLLUĞUN SİBER GÜVENLİK YÖNETİŞİMİ

Fransa, dijital teknolojilerin gelişmesi açısından tarih boyunca önemli bir rol oynamakta ve internetin benimsenmesi açısından küreselleşmenin öncü ülkelerinden biri konumunda bulunmaktadır. İnternet öncesi dönemde, Fransa 1980'lerde geliştirilen Minitel sistemi ile dikkat çekmektedir. Minitel, modern dijital iletişim teknolojilerinin bir habercisi olarak kabul edilmektedir. Fransa Telekom tarafından tasarlanan bu sistem, çevirmeli ağ bağlantısı kullanarak ev kullanıcılarına çeşitli hizmetler sunmayı hedeflemiştir. Minitel, telefon hattı üzerinden çalışarak bilgi erişimi, elektronik posta, çevrimiçi alışveriş ve hatta banka işlemleri gibi işlevler sağlayan bir terminal olarak tasarlanmıştır (Mailland ve Driscoll, 2017).

İnternet, 1990'ların başında Fransa'da yaygınlaşmaya başlamıştır. İlk başlarda üniversiteler ve araştırma merkezleri tarafından kullanılan internet, 1994 yılında Fransa'da ticari internet servis sağlayıcılarının kurulmasıyla kamuya açılmaktadır (Durand, 2019). Bu dönemde Fransız hükümeti, internet altyapısının yayılmasını ve yeni teknolojilerin benimsenmesini teşvik etmek amacıyla çeşitli politikalar uygulamaktadır. 2000'li yıllara gelindiğinde, geniş bant internet erişimi hızla yayılmaktadır. Özellikle 2003 yılında geniş bant seferberliği ile Fransa'da yüksek hızlı internet önemli ölçüde artırılmaktadır. 2007 yılında fiber optik internet için yapılan büyük yatırımlar Fransa'yı Avrupa'nın önde gelen ülkelere biri haline getirmektedir (ANFR, 2021). Son yıllarda, Fransa'daki dijital teknolojilerin sosyal ve ekonomik boyutlarını geliştirmek amacıyla çeşitli girişimlerde bulunmaktadır. Özellikle, AB'nin Dijital Tek Pazar stratejisiyle uyumlu politikalar benimseyerek internet erişimini daha demokratik ve kapsayıcı hale getirme hedefinin uygulanması bu kapsamda sayılabilmektedir (Avrupa Komisyonu, 2022). Fransa'nın dijital teknolojilerin ortaya çıkış sürecini diğer ülkelere kıyasla daha erken tecrübe etmiş olması ve sonrasında yaşadığı siber tehditler sebebiyle siber güvenlik alanında gelişmiş bir altyapıya sahip olmasına neden olmaktadır. Siber alandaki tecrübelerini uluslararası iş birliklerinde aktarmaya önem veren bir ülke olarak karşımıza çıkmaktadır.

Fransa'nın Ulusal Siber Güvenlik Ajansı (National Cybersecurity Agency-ANSSI), ülke genelinde siber güvenlik politikalarının koordinasyonundan sorumlu olan kurumdur ve aynı zamanda Avrupa çapında da çeşitli siber güvenlik projelerine liderlik etmektedir. Fransa, EUROPOL ve INTERPOL ile sıkı bir iş birliği içerisinde çalışarak, küresel siber suçlarla mücadelede aktif bir rol oynamaktadır. Özellikle Fransa'nın ulusal güvenlik alanındaki stratejileri, AB ve NATO düzeyindeki siber güvenlik politikalarına büyük katkı sağlamaktadır (Perrin ve Courtois, 2018). Bu sebeple hem ulusal hem de uluslararası alanda küresel yönetim konusunda rol model ülkelere biri olarak karşımıza çıkmaktadır.

5.1. Fransa’da Kolluk Yapılanması

Güvenlik, modern devletlerin temel önceliklerinden biri olarak karşımıza çıkmaktadır. Toplumların düzenini ve bireylerin güvenliğini sağlama sorumluluğu, devletin en temel görevlerinden biri olarak kabul edilmektedir. Bu bağlamda Fransa, gelişmiş ve disiplinli bir kolluk yapılanmasına sahip olan ülkelerden biri olarak konumlanmaktadır. Fransa, tarihsel ve kurumsal olarak merkezi bir devlet yapısına sahip olması nedeniyle, kolluk kuvvetlerinin organizasyonunda da merkezi bir yaklaşım sergilemektedir. Fransa’da kolluk kuvvetleri, halkın güvenliğini sağlamak, kamu düzenini korumak ve suçla mücadele etmek amacıyla, polis ve jandarma kuvvetlerinden oluşan iki ana kolluk birimini kapsamaktadır. Bu tezde ana olarak bu iki kolluk birimi üzerinden değerlendirmeler yapılmaktadır.

Tablo 5. 1. Fransa'da Kolluk Yapılanması

Kolluk Birimi	Görev Alanı	Alt Birimler
Ulusal Jandarma	Kırsal alanlar ve küçük yerleşim yerlerinde güvenlik ve asayiş	- Siber Suçlarla Mücadele Birimi (C3N)- Terörle Mücadele Birimleri- Kaçakçılıkla Mücadele Birimleri
Ulusal Polis	Şehir merkezleri ve büyük yerleşim yerlerinde asayiş ve güvenlik	- Siber Suçlarla Mücadele Birimi (DCPJ)- Çevik Kuvvet- Organize Suçlarla Mücadele Birimi
Sınır Polisi	Sınır bölgelerinde güvenlik ve yasa dışı geçişlerin önlenmesi	- Havalimanı Güvenlik Birimleri- Deniz Sınır Güvenliği Birimleri
Sivil Savunma ve Acil Durumlar	Afet ve acil durumlarda müdahale ve koordinasyon	- İtfaiye Birimleri- Arama ve Kurtarma Birimleri
Uluslararası İş Birliği	INTERPOL ve EUROPOL ile koordinasyon	- AB Siber Güvenlik Ajansı (ENISA) ile ortak projeler

Bu tablo, açık kaynak verileri kullanılarak tezin yazarı oluşturulmuştur. Fransa'da Kolluk Yapılanması hakkında genel bir çerçeve sunmaktadır.

Ulusal Polis, Fransa’nın kentsel alanlarında görev yapmakta ve İçişleri Bakanlığı’na bağlı olarak çalışmaktadır. Bu kurum, şehirlerde kamu güvenliğini sağlama, trafik kontrolü, asayiş ve suçla mücadele gibi görevleri yerine getirmektedir. Aynı zamanda organize suçlar, terörle mücadele ve siber güvenlik gibi daha karmaşık konuları ele almak için uzmanlaşmış birimlere sahip bulunmaktadır. Ulusal Jandarma ise kırsal alanlarda ve küçük yerleşimlerde görev yapan, Fransa Savunma Bakanlığı’na bağlı kolluk teşkilatıdır. Bu kurum hem askeri hem de sivil bir

kolluk kuvveti olarak çift yönlü bir rol üstlenmektedir. Jandarma, sınır güvenliği ve acil durum müdahalelerinde önemli bir rol oynamaktadır. Ayrıca, kırsal kesimde adli polis görevlerini yerine getirmektedir. Fransa'daki kolluk kuvvetleri merkezi bir yapıya sahip olsa da yerel yönetimlerle iş birliği yapmaktadır. Belediye polisleri (Police Municipale), belediyelere bağlı olarak çalışmaktadır ve yerel seviyede kamu düzeninin sağlanmasına yönelik görevler üstlenmekte olup, bu polisler, silahlı müdahale yetkisi olmayan sınırlı bir yargı yetkisine sahip olmaktadır.

Fransa'nın kolluk sistemi, göç, şehirleşme ve toplumsal olaylar gibi modern zorluklarla başa çıkmak için sürekli olarak reformlara tabi tutulmaktadır. Teknolojik yatırımlar, şeffaflık politikaları ve halkla iş birliğine dayalı yaklaşımlar, kolluk kuvvetlerinin etkinliğini artırmayı amaçlamaktadır. Sonuç olarak, Fransa'nın kolluk yapılanması, merkeziyetçi ve disiplinli bir yaklaşımla şekillenmiş olup hem şehirde hem de kırsal alanlarda kamu düzenini ve güvenliği sağlamaya yönelik hareket etmektedir. Bu yapı, modern toplumun dinamiklerine uyum sağlamak için evrilmeye devam etmektedir.

5.2. Fransa'nın Kolluk Teşkilatlarında Siber Güvenliğin Yeri ve Geliştirilen Stratejiler

Teknolojinin hızla gelişimiyle birlikte, siber suçlar modern toplumlar için ciddi bir tehdit haline gelmektedir. Bu bağlamda Fransa, siber suçlara karşı etkin bir hukuki çerçeve oluşturmak amacıyla çeşitli yasal düzenlemeler yapmaktadır. Fransa'nın siber suçlarla mücadelesinin tarihçesi, dijitalleşmenin ilk yıllarına dayanmaktadır. Fransa'nın siber suçlarla ilgili ilk düzenlemeleri, 1988 tarihli Godfrain Yasası ile başlamıştır (Godfrain Yasası, 1988). Bu yasa, izinsiz bilgisayar erişimi ve veri bozulması gibi eylemleri suç kapsamına alan ilk düzenlemelerden biri olarak bilinmektedir. Bu yasa, özellikle dijital çağın başlangıcında Fransa'nın bu konuda öncü adımlar atmasını sağlamaktadır. 2000'li yıllara gelindiğinde, dijital teknolojilerin daha yaygın hale gelmesiyle birlikte Fransa, 2004 yılında yürürlüğe giren Dijital Ekonomide Güven Yasası (Loi pour la Confiance dans l'Économie Numérique-LCEN) ile dijital işlemleri ve çevrimiçi platformları düzenlemeye başlamaktadır (LCEN, 2004). Bu yasa, çevrimiçi içeriklerin sorumluluğu, veri güvenliği ve elektronik ticaretin hukuki çerçevesini belirlemektedir. 2013 yılında kurulan ANSSI, siber güvenlik alanında stratejik bir rol üstlenmektedir (ANSSI, 2013). ANSSI'nin kurulması, kritik altyapıların korunması ve siber tehditlere karşı ulusal düzeyde bir güvenlik stratejisi oluşturulması açısından önemli bir dönüm noktası olarak görülmektedir.

Fransa'nın siber suçlarla mücadeleye yönelik mevzuatı, temel olarak Ceza Kanunu (Code pénal) ve LCEN yasalarına dayanmaktadır. Fransa Ceza Kanunu'nun 323. maddesi, izinsiz erişim, veri bozma, yasa dışı veri kopyalama gibi siber suçları kapsamlı bir şekilde düzenlemektedir. Bu kapsamda, izinsiz bir sisteme erişim, verilerin kasıtlı olarak değiştirilmesi veya imha edilmesi ağır cezalarla yaptırıma bağlanmaktadır (Code pénal, 323. madde, 2023). LCEN ise dijital ekonomiyi düzenlemeyi amaçlamakta, çevrimiçi içerik sağlayıcılarının sorumluluklarını belirlemekte ve elektronik iletişimle ilgili hükümlere yer vermektedir (LCEN, 2004). AB Genel Veri Koruma Tüzüğü (RGPD), kişisel verilerin korunmasına yönelik sıkı düzenlemeler öngörmektedir. Fransa, bu tüzüğü ulusal hukuku kapsamında doğrudan uygulamaktadır (RGPD, 2018). Fransa, Avrupa Siber Suç Sözleşmesi'ne (Budapeşte Sözleşmesi) taraf ülkelerden biridir ve sınır ötesi siber suçlarla mücadelede uluslararası iş birliğini desteklemektedir (Budapeşte Sözleşmesi, 2001). Fransa, AB'nin Ağ ve Bilgi Güvenliği Direktifi'ni (NIS Direktifi) ulusal mevzuatına dahil etmekte, bu direktif kritik altyapı operatörlerinin ve dijital hizmet sağlayıcıların siber güvenlik standartlarına uyumlu olmalarını zorunlu kılmaktadır. Fransa'nın siber suçlarla mücadeleye yönelik yasal düzenlemeleri, teknolojiye dayalı tehditlere karşı etkili bir hukuki altyapı sunmaktadır. Ancak dijital suçların dinamik yapısı, düzenlemelerin sürekli güncellenmesini ve yeni teknolojilere uygun stratejiler geliştirilmesini zorunlu kılmaktadır.

Siber güvenlik, modern devletlerin ulusal güvenlik stratejilerinde kritik bir unsur haline gelmektedir. Fransa, bu alanda ulusal ve uluslararası iş birliğine dayalı kapsamlı politikalar geliştirmiştir. Özellikle, kolluk teşkilatlarının siber tehditlere karşı etkin mücadele edebilmesi için güçlü bir altyapı ve organizasyon oluşturulmaktadır (OECD, 2020). Fransa'nın siber güvenlik strateji alanındaki çalışmaları, 2000'lerin başlarında kritik altyapıların korunması ihtiyacıyla şekillenmeye başlamaktadır. 2008 yılında yayımlanan Beyaz Kitap (Livre Blanc sur la Défense et la Sécurité Nationale) siber tehditleri ulusal güvenlik politikasının öncelikli unsurlarından biri olarak tanımlamaktadır. Kritik altyapıların korunması ve siber sıkıyönetim kavramı bu belgede ilk kez vurgulanmaktadır. 2013 Ulusal Siber Güvenlik Stratejisi (Stratégie Nationale pour la Sécurité du Numérique), ANSSI tarafından geliştirilmiş olup, kritik altyapıları koruma, siber sıkıyönetim ve ulusal kapasite geliştirme gibi hedefler belirlemektedir. Bu strateji aynı zamanda siber olaylara müdahale ve zorunlu raporlama gerekliliklerini de kapsamaktadır. Askeri Planlama Yasası (Loi de Programmation Militaire) 2015 yılında kabul edilmekte, kritik altyapı operatörlerinin siber olaylara karşı zorunlu raporlama yapmasını şart koşmakta ve kolluk kuvvetleri ile ANSSI arasındaki koordinasyonu güçlendirmektedir. 2018-

2020 Siber Güvenlik Stratejisi, dijital dönüşüm sürecinde bireylerin ve kurumların korunmasına odaklanmaktadır. Aynı zamanda, teknoloji geliştirme ve şirketlerin farkındalığını artıracak programlar hayata geçirilmektedir. 2021 yılında başlatılan 2021-2025 Ulusal Siber Güvenlik Planı teknoloji geliştirme, kamu-özel sektör iş birliği ve uluslararası düzenlemelere uyum gibi öncelikleri kapsamakta ve siber tehditlere karşı ulusal kapasiteyi daha da arttırmayı hedeflemektedir.

Fransa'da kolluk kuvvetleri, siber güvenlik stratejilerinde önemli bir yere sahiptir. Ulusal Jandarma'nın Siber Suçlarla Mücadele Birimi (C3N), organize siber suçlara karşı operasyonlar düzenlerken, Bilgi ve İletişim Teknolojilerine Bağlı Suçlarla Mücadele Merkez Ofisi (OCLCTIC-Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communications), siber suçlarla mücadele etmek için Ulusal Polis bünyesinde faaliyet gösteren önemli bir birim olarak karşımıza çıkmaktadır (Direction Générale de la Police Nationale, 2023). Ayrıca, ANSSI ile iş birliği içinde çalışan kolluk kuvvetleri hem şahıs hem de kurumlara yönelik siber tehditleri azaltmaya yönelik çalışmalar yürütmektedir. Bu kapsamda, siber olaylara müdahale ekipleri oluşturulmuş ve uzmanlık alanlarına ayrılarak şüpheli şahısların, organizasyonların, kurumların izlenmesine yoğunlaşmıştır. ANSSI ile iş birliği içinde çalışan polis birimleri ve jandarma, bireylerin ve kurumların siber tehditlerden korunmasını sağlamaktadır. Bu süreçte, siber olaylara müdahale ekipleri kurulmakta ve uzmanlık alanlarına göre potansiyel tehditleri izleme çalışmaları yoğunlaşmaktadır. Bu ekipler, şüpheli hareketleri hızlı bir şekilde tespit edip yanıt vererek, kurumların ve bireylerin zarar görmesini önlemeye çalışmaktadır. Özellikle siber suçların karmaşıklığı arttıkça, bu ekiplerin uzmanlığı kritik hale gelmektedir. Uzmanlık, özellikle yeni nesil tehditlerin (örneğin fidye yazılımları veya siber casusluk girişimleri) tespiti ve engellenmesi için hayati önem taşımaktadır.

Kolluk kuvvetlerinin görevleri arasında, sadece olay anında müdahale değil, aynı zamanda tehditlerin önlenmesi amacıyla önleyici tedbirler almak da yer almaktadır ANSSI ile yapılan iş birliği, kamu ve özel sektörün bilgi paylaşımıyla koordinasyonunu arttırmaktadır. Böylece, ulusal düzeyde bir bütünlük sağlanarak etkili müdahale mekanizmaları oluşturulabilmektedir. 2017 yılında dünya genelinde büyük hasara yol açan WannaCry saldırıları sırasında, Fransa'da ANSSI ve C3N hızlı bir koordinasyon sağlayarak etkilenen kritik altyapıları korumuş ve saldırıların etkisini minimuma indirmiştir (ANSSI, 2017).

ANSSI, Fransa'nın ulusal siber güvenlik otoritesi olarak 2009 yılında kurulmaktadır. ANSSI, kritik altyapıların korunması, dijital güvenliğin sağlanması ve siber tehditlere karşı ulusal

direnç oluşturulması amacıyla faaliyet göstermektedir. Fransa Başbakanlığına bağlı olan ANSSI hem ulusal hem de uluslararası düzeyde siber güvenlik stratejilerinin uygulanmasından sorumludur (ANSSI, 2021) Bu bağlamda siber tehditlerin ulusal güvenlik üzerindeki etkisini fark ederek, 2015 yılında ilk Ulusal Siber Güvenlik Strateji Belgesini yayımlamıştır. Bu strateji, dijitalleşmenin getirdiği fırsatları değerlendirmek ve siber saldırılara karşı ulusal direnç oluşturmak amacıyla hazırlanmıştır. Strateji, kritik altyapıların korunmasından bireylerin dijital farkındalığının artırılmasına kadar geniş bir çerçeve sunmaktadır (ANSSI, 2015). Fransa, bu Strateji Belgesi aracılığıyla kolluk kuvvetlerinin kapasitelerini artırmaya yönelik önemli adımlar atmaktadır. Bu strateji çerçevesinde, siber tehditlere karşı erken uyarı sistemleri, dijital suç analizi ve kamu-özel sektör iş birliğini güçlendirme hedeflenmiştir (ANSSI, 2016). Ayrıca, NATO ve EUROPOL gibi uluslararası kuruluşlarla yapılan iş birlikleri sayesinde, Fransa kolluk kuvvetleri uluslararası siber suçlarla mücadelede etkili bir aktör haline gelmiştir (NATO, 2020). 2021-2025 Ulusal Siber Güvenlik Stratejisi ise ANSSI tarafından Şubat 2021 tarihinde yayımlanmıştır. Bu strateji belgesiyle önceki strateji belgelerinde yer alan dijital güvenlik politikalarının güçlendirilmesi ve Fransa'nın siber alanda lider bir ülke konumuna gelmesi amacıyla hazırlanmıştır (ANSSI, 2021).

Fransa, siber güvenlik stratejilerini geliştirirken hem ulusal hem de uluslararası düzeyde önemli adımlar atmış ve bu süreçte kolluk kuvvetlerini de etkin bir biçimde entegre etmiştir. Uluslararası iş birlikleri ve yasal düzenlemeler, Fransa'nın bu alandaki etkinliğini artırmaya devam etmektedir. Siber tehditlerin karmaşıklaşan yapısı, gelecekte daha fazla inovasyon ve iş birliği ihtiyacını gündeme getirecektir. Fransa'nın kolluk teşkilatlarında siber güvenliğin yeri, hem Ulusal Jandarma hem de Ulusal Polis bünyesinde oluşturulan özel birimlerle belirginleşmektedir. C3N, Fransa'nın dijital suçlarla mücadele birimi olarak 2010 yılında faaliyete geçmiştir. C3N, Fransa Ulusal Jandarması bünyesinde faaliyet göstermekte ve özellikle siber suçlarla mücadele, dijital delil analizi ve çevrim içi suç ağlarının çökertilmesi konusunda uzmanlaşmıştır. (Ministère de l'Intérieur, 2022) AB Siber Güvenlik Ajansı (ENISA) ile ortak projelerde yer almaktadır. (ENISA, 2021). C3N'nin temel görevleri aşağıda sıralanmıştır:

- Çevrim içi dolandırıcılık, çocuk istismarı, yasa dışı içerik yayılımı ve fidye yazılım saldırılarına karşı operasyonel faaliyetler yürütmek,
- Dijital delillerin toplanması, analizi ve adli süreçlerde kullanılabilir hale getirilmesini sağlamak,

- EUROPOL, INTERPOL ve diğer uluslararası kuruluşlarla iş birliği yaparak sınır ötesi siber suç operasyonlarına katılmaktadır (Gendarmerie Nationale, 2022).

C3N, yüksek uzmanlık gerektiren bir yapılanmaya sahiptir. Operasyonel Mücadele Departmanı siber suçları tespit ve analiz eden ve gerektiğinde operasyon düzenleyen birimken, Teknoloji Geliştirme Departmanı, Adli bilişim araçlarını geliştiren ve siber güvenlik teknolojilerini araştıran ekiplerden oluşmaktadır. Eğitim ve Farkındalık Departmanı ise kolluk kuvvetlerine ve kamuoyuna yönelik siber güvenlik eğitimleri düzenleyen birim olarak karşımıza çıkmaktadır (Gendarmerie Nationale, 2022). C3N hem ulusal hem de uluslararası düzeyde operasyonel etkinliğini artırmak için sürekli olarak teknolojiye yatırım yapmakta ve siber suçlarla mücadelede yenilikçi yöntemler geliştirmektedir (Ministère de l'Intérieur, 2022). C3N, Fransa'nın siber suçlarla mücadele kapasitesinin temel taşı olup hem ulusal hem de uluslararası düzeyde yürüttüğü operasyonlar, yenilikçi teknolojilere yaptığı yatırımlar ve iş birliği çalışmaları ile siber suçlarla mücadelede örnek teşkil eden bir kurum olması sebebiyle Fransa'nın dijital suçlarla mücadele politikasının başarısında C3N'nin rolü büyüktür. DCPJ (Direction Centrale de la Police Judiciaire- Adli Polis Merkez Müdürlüğü) Fransa'nın organize suçlar, uyuşturucu kaçakçılığı, ekonomik suçlar, terörizm ve siber suçlarla mücadele konularında uzmanlaşmış ulusal adli polis teşkilatıdır. 1907 yılında kurulan DCPJ, Fransa İçişleri Bakanlığı'na bağlı olarak faaliyet göstermektedir ve ülke genelinde adli soruşturmalarda anahtar bir rol üstlenmektedir (Ministère de l'Intérieur, 2022). DCPJ, merkezi bir yapıya sahip olmakla birlikte bölgesel düzeyde örgütlenmiştir. Bu yapı, çeşitli birimlerin uzmanlık alanlarına göre görevlerini yerine getirmesine olanak tanımaktadır. Siber Suçlarla Mücadele Birimi (BL2C) çevrim içi dolandırıcılık, veri ihlalleri ve çocuk istismarı gibi suçlara karşı faaliyet göstermektedir (DCPJ, 2022). 2021 yılında DCPJ, EUROPOL ile iş birliği içinde yürütülen bir operasyonda uluslararası bir fidye yazılım çetesinin çökertilmesine katkıda bulunmuş ve Fransa'daki siber güvenlik kapasitelerini uluslararası düzeyde göstermiştir (EUROPOL, 2021). DCPJ, Fransa'nın adli polis teşkilatı olarak suçla mücadelede etkili bir yapı sunmaktadır. Hem ulusal hem de uluslararası düzeyde operasyonel etkinliği, yenilikçi teknolojilere yatırımı ve güçlü iş birlikleri ile DCPJ, suçla mücadelede örnek bir kurumdur. Teknolojik gelişmelere uyum sağlayarak ve uluslararası ortaklıklarını genişleterek, suçla mücadeledeki liderliğini sürdürmektedir. Siber güvenliğin kolluk teşkilatlarındaki yeri sadece teknik altyapı ile sınırlı kalmamaktadır. Eğitim ve kapasite geliştirme programları, bu teşkilatların insan kaynağını güçlendirme açısından büyük önem taşımaktadır. Fransa'nın siber güvenlik stratejileri arasında kamu bilincini artırmaya yönelik kampanyalar da bulunmaktadır. Siber tehditlere karşı

bireylerin ve kurumların dayanıklılığını artırmak için düzenlenen farkındalık programları, kolluk kuvvetlerinin faaliyetlerini desteklemektedir (ENISA, 2021).

5.3. Uluslararası İş birliği Örnekleri ve Küresel Yönetişime Katkısı

Fransa, siber güvenlik alanında uluslararası iş birliği ve küresel yönetişimde önemli bir aktör olarak öne çıkmaktadır. AB, EUROPOL ve INTERPOL gibi organizasyonlarla güçlü ilişkiler kurarak, sınır ötesi suçlarla mücadelede etkin bir rol oynamaktadır (EUROPOL, 2022). Yediler Grubu (Group of Seven-G7) ve Birleşmiş Milletler gibi uluslararası platformlarda da etkin bir rol oynayan Fransa, küresel düzenlemeler ve normlar üzerinde etkili olma çabalarına devam etmektedir. 2021'de Paris'te gerçekleştirilen Uluslararası Siber Barış Forumu, bu alandaki liderliğini pekiştirmektedir (International Cybersecurity Forum, 2021). Özellikle, AB'nin Siber Güvenlik Ajansı (ENISA) ile yapılan iş birlikleri, Fransa'nın hem teknik hem de stratejik kapasitesini artırmaktadır (ENISA, 2021). EUROPOL çatısı altında, Fransa'nın aktif olarak yer aldığı Avrupa Siber Suç Merkezi (European Cybercrime Centre-EC3), Avrupa genelinde organize siber suçlarla mücadelede kritik bir platform olarak faaliyet göstermektedir. Fransa, bu merkeze uzman personel ve bilgi paylaşımı açısından önemli katkılar sağlamaktadır (EUROPOL, 2020). Ayrıca, INTERPOL ile yürütülen operasyonlar, küresel düzeyde siber suçların önlenmesine yönelik etkili bir mekanizma sunmaktadır. Örneğin, Fransa, INTERPOL'ün "Operation Falcon" adlı uluslararası siber suç operasyonunda lider ülkelerden biri olmaktadır (INTERPOL, 2019).

Fransa'nın AB içerisindeki iş birlikleri sadece operasyonel düzeyde kalmamaktadır. AB Siber Güvenlik Yönetişim Çerçevesi'nde (Cybersecurity Act), Fransa'nın öncü rolü, siber güvenlik standartlarının belirlenmesi ve uygulanmasında kritik öneme sahiptir (European Commission, 2019). Ayrıca, Fransa, NATO ile de siber güvenlik konusunda yakın iş birliği yürütmekte ve ortak tatbikatlarda yer almaktadır (NATO, 2020).

Fransa'nın siber güvenlik eğitim programları ANSSI tarafından koordine edilmektedir. Bu programların temel amacı, kolluk kuvvetlerine dijital tehditler ve güvenlik önlemleri konusunda kapsamlı bilgi ve uygulamalı deneyim sağlamaktır (ANSSI, 2020). Kolluk kuvvetlerine, siber suçların tanımı, türleri ve izleme yöntemleri gibi konularda temel bilgiler verilmektedir. Eğitimler arasında dijital izleme, veri analizi ve siber olay müdahale süreçleri yer almaktadır. Kolluk kuvvetlerinin yanı sıra kamu kurumları ve özel sektör temsilcileri için düzenlenen atölyeler, siber suçlarla mücadelede iş birliği kapasitesini artırmayı hedeflemektedir (ENISA, 2019). ANSSI, düzenli aralıklarla "siber tatbikatlar" düzenleyerek, olası tehdit senaryolarında

kolluk kuvvetlerinin tepkisini test etmektedir (ANSSI, 2021). Fransa, INTERPOL ve EUROPOL gibi uluslararası kuruluşlarla iş birliği yaparak, kolluk kuvvetlerinin uluslararası siber suçlarla mücadele kapasitelerini artırmayı amaçlamaktadır (INTERPOL, 2020). Siber güvenlik farkındalığı, yalnızca teknik bilgileri içermekle kalmayıp, aynı zamanda kolluk kuvvetlerinin iş birliği ve koordinasyon becerilerini de geliştirmektedir. Fransa, AB'nin genel siber güvenlik politikalarına uyum sağlamakla birlikte, siber güvenlik eğitiminde lider konumunu korumaktadır. Avrupa Siber Güvenlik Eğitim ve Farkındalık Çerçevesi (European Cybersecurity Skills Framework) ile uyumlu bir yaklaşım benimseyen Fransa, ulusal düzeyde kazandığı deneyimleri Avrupa çapında yaygınlaştırmaktadır. (ENISA, 2019).

Fransa, Afrika başta olmak üzere gelişmemiş ve gelişmekte olan ülkelerde geniş çaplı operasyonlar düzenleyerek, eğitim hizmetleri vererek ve dijital altyapı desteği sağlayarak bu ülkelerin dijital kapasitelerini artırmayı hedeflemektedir. Ancak bu girişimlerin, dijital sömürgecilik endişelerinin arttığı da görülmektedir. Özellikle dijital altyapıların Fransa merkezli şirketler tarafından inşa edilmesi ve kritik veri oluşumlarının Fransa'nın etkisi altında olması, bu ülkelerin ulusal egemenliklerini bağımlı hale getirerek zedeleyebilmektedir. (Taylor, 2021). Dijital sömürgecilik, ulusal egemenlik rejimi eriten bir güç dinamiği olarak öne çıkmaktadır. Gelişmemiş ülkeler, teknoloji transferi ve siber güvenlik eğitimleri gibi yardımlardan yararlanırken, aynı zamanda bu yardımlara bağımlı hale getirilebilmektedir. Bu durum, bu ülkelerin kendi dijital politikalarını oluşturma kapasitelerini sınırlamakta ve karar almada dış etkilerinin artmasına yol açmaktadır (Smith & Lambert, 2020). Örneğin, Fransa'nın geliştirdiği siber güvenlik programlarının içerikleri, genellikle uluslararası güvenlik perspektifine uygun olsa da yerel özellikler göz ardı edilebilir ve bu da uzun süreli ulusal egemenlik algısını zedeleyebilmektedir. Bu tür politikaların etkili ve etik bir şekilde uygulanabilmesi için şeffaflık ve yerel çalışmaların ulusal düzeyde devam etmesi gerekmektedir. Aksi takdirde, bu girişimler sadece kalkınma ve güvenlik hedeflerini değil, aynı zamanda dijital sömürgecilik kaygılarını da beraberinde getirebileceği değerlendirilmektedir.

5.4. Küresel Siber Güvenlik Endeksinde Fransa'nın Yeri ve Kolluk Kuvvetlerinin Etkisi

Fransa, GCI sıralamalarında genellikle üst sıralarda yer almıştır. Özellikle 2018 yılında Fransa, endekste üçüncü sırada bulunarak siber güvenlik alanındaki güçlü performansını göstermiştir. Fransa'nın GCI'daki yüksek sıralaması, çeşitli stratejik adımlar ve politikaların sonucu olarak değerlendirilmektedir. Fransa, siber güvenlik alanında kapsamlı yasal düzenlemeler ve politikalar oluşturmuştur. ANSSI, ülkenin siber güvenlik stratejilerinin uygulanmasında merkezi bir rol oynamaktadır. Fransa, siber güvenlik altyapısını güçlendirmek için önemli

yatırımlar yapmaktadır. Teknik önlemler ve kapasite geliştirme çalışmaları, ülkenin siber tehditlere karşı dayanıklılığını artırmaktadır. Fransa, uluslararası platformlarda aktif rol alarak siber güvenlik alanında iş birliğini teşvik etmektedir. Bu yaklaşım, ülkenin küresel siber güvenlik politikalarında etkin bir aktör olmasını sağlamaktadır. (Altıntaş, 2022)

2024 yılı GCI raporunda, ITU sıralama yapısından seviyelendirme yapısına geçmiştir. Bu yeni değerlendirme sistemine göre, ülkeler yasal düzenlemeler, hukuki düzenleme, teknik altyapı, organizasyonel yapılanma, kapasite geliştirme ve kurumlar arası iş birliği alanlarına göre seviyelendirilmiştir. Fransa, tüm alanlarda çok yüksek puanlar alarak hem küreselde hem de Avrupa ülkeleri arasında "örnek alınan ülkeler" arasında en üst seviyede yer almıştır. Fransa'nın GCI konumu, ülkedeki bu alandaki adımların oluşturulması ve politikalarının uluslararası düzeyde olduğunun bir göstergesidir. Fransa, siber güvenlik politikaları ve altyapı gelişiminde önem veren bir ülke olarak, küresel iş birliği çözümlerine de büyük önem vermektedir (ITU, 2021) Bu başarı, teknolojik altyapının gelişmişliği, stratejik politikalar ve uluslararası iş birliğinin yanı sıra, kolluk kuvvetlerinin etkin yapılanması ve bu alandaki uzmanlaşmasıyla doğrudan ilişkilendirilebilmektedir. Fransa'nın kolluk kuvvetleri, geleneksel güvenlik tehditlerine karşı mücadele etmekle kalmayıp, aynı zamanda modern çağın siber suçlarına yönelik kapsamlı ve organize bir yaklaşım geliştirmiştir. Ulusal Polis ve Jandarma'nın uzman birimleri, siber tehditlere karşı güçlü bir savunma mekanizması oluşturmuş ve uluslararası düzeyde iş birliklerini geliştirerek Fransa'nın dijital güvenlikteki lider konumunu pekiştirmiştir. Bu model, diğer ülkeler için de bir örnek teşkil etmekte ve siber suçlarla mücadelede güçlü bir yaklaşım olarak değerlendirilmektedir (Ministère de l'Intérieur, 2023).

6.ABD'DE KOLLUĞUN SİBER GÜVENLİK YÖNETİŞİMİ

ABD, internet ve dijital teknolojilerin doğuşu ve gelişiminde öncü bir rol oynamıştır. İnternetin temelleri, 1960'larda ABD Savunma Bakanlığı'nın İleri Araştırma Projeleri Ajansı (ARPA) tarafından başlatılan ARPANET projesine dayanmaktadır. ARPANET, bilgisayarlar arasında veri paylaşımını mümkün kılarak, günümüz internetinin temelini oluşturmuştur (Leiner ve diğ., 2009). 1980'ler ve 1990'lar, internetin akademik çevrelerden çıkarak ticari ve kamusal alanda genişlediği bir dönem olmuştur. Özellikle 1991 yılında Dünya Çapında Ağ' ın (World Wide Web-www) halka açılması, internetin yaygınlaşmasında dönüm noktası olmuştur (Berners-Lee, 2000). ABD, bu süreçte hem altyapı yatırımları hem de teknoloji şirketlerinin inovasyonları sayesinde küresel liderlik pozisyonunu korumuştur. Microsoft, Apple, Google ve Amazon gibi şirketler, internetin gelişiminde önemli bir rol oynamış ve dijital ekonominin temel taşlarını oluşturmuştur. Dijital teknolojilerdeki gelişim, yalnızca internet erişiminin artmasıyla sınırlı kalmamış, aynı zamanda yapay zeka büyük veri analitiği ve bulut bilişim gibi yeni teknolojilerin gelişimini de kapsayacak şekilde genişlemiştir. 2010'lu yıllarda ABD hükümeti, geniş bant internet erişimini artırmak ve dijital uçurumu kapatmak için çeşitli girişimlerde bulunmuştur. Örneğin, Ulusal Geniş Bant Planı (National Broadband Plan), ekonomik büyümeyi hızlandırmak ve tüm vatandaşların dijital teknolojilerden faydalanmasını sağlamak için hazırlanmıştır (FCC, 2010). ABD'de dijital teknolojilerin gelişimi, toplumsal ve ekonomik alanlarda büyük dönüşümler yaratmıştır. E-ticaret, uzaktan eğitim ve tele-tıp gibi uygulamalar, bu teknolojilerin bireylerin günlük yaşamında nasıl bir devrim yarattığını göstermektedir. Bununla birlikte, mahremiyet, siber güvenlik ve dijital eşitsizlik gibi sorunlar, dijital teknolojilerin yaygınlaşmasıyla birlikte çözüm bekleyen önemli meseleler olarak öne çıkmaktadır. ABD internet ve dijital teknolojilerdeki liderliğini, yenilikçi politikalar, kamu-özel sektör iş birliği ve araştırma-geliştirme yatırımları sayesinde bugüne kadar sürdürmüş ve küresel dijital dönüşüme yön vermeye devam etmektedir.

ABD'de hızla gelişen dijital sektör beraberinde siber suçlar ve siber tehditleri getirmiş ABD de bu siber suçlarla mücadelede kapsamlı bir mevzuat ağı geliştirmiş ve bu alanda ulusal güvenlik ile bireysel hakları korumayı hedefleyen bir yasal çerçeve oluşturulmuştur. Siber suçlar, bilgisayar ve internet kullanımıyla işlenen yasa dışı faaliyetleri içermektedir. Bu suçlar arasında kimlik hırsızlığı, dolandırıcılık, veri ihlalleri, fidye yazılımları ve kritik altyapılara yönelik saldırılar yer almaktadır (Goodman, 2016). ABD'de siber suçlarla ilgili ilk kapsamlı yasa, 1986 yılında çıkarılan Bilgisayar Dolandırıcılığı ve Kötüye Kullanımı Yasası (Computer Fraud and Abuse Act-CFAA) olmuştur. CFAA, bilgisayar sistemlerine yetkisiz erişimi ve bu sistemlerin

kötüye kullanılmasını suç olarak tanımlamıştır. Yasa hem bireylerin hem de kurumların siber tehditlere karşı korunmasını amaçlayan temel bir araçtır. (DOJ, 2020). 1996 yılında kabul edilen Ekonomik Casusluk Yasası (Economic Espionage Act), ticari sırların çalınması ve siber casusluk gibi suçlara odaklanmıştır. Bu yasa, özellikle yabancı devletlerin desteklediği ekonomik casusluk faaliyetlerine karşı koymayı hedeflemiştir. Bunun yanı sıra, 2001 yılında yürürlüğe giren ABD Vatanseverlik Yasası (USA PATRIOT Act), terörizmle mücadele kapsamında siber alanda dijital veri izleme yetkilerini genişletmiştir (Givens, 2011). ABD’de siber suç mevzuatı, sürekli gelişen teknolojilere ve tehditlere uyum sağlamak için güncellenmeye devam etmektedir. Örneğin, 2015 yılında çıkarılan Siber Güvenlik Bilgi Paylaşım Yasası (Cybersecurity Information Sharing Act), kamu ve özel sektör arasında siber verilerin paylaşımını teşvik etmektedir. Bu yasa hem bireysel hem de ulusal düzeyde siber saldırılara karşı savunmayı güçlendirmeyi amaçlamaktadır (Congress.gov, 2015).

Dijital teknolojilerde öncü olmasının yanı sıra ABD siber güvenliğin sağlanması hususunda da öncü ülkelerden biri olup, siber suçlarla mücadele ve küresel siber güvenlik yönetiminde lider bir rol oynamaktadır. ABD’de kolluk kuvvetlerinin siber güvenlik yönetimi ise dijital çağda giderek önem kazanan bir konu haline gelmiştir. Gelişen teknolojiler ve artan siber tehditler, ulusal ve federal düzeydeki kolluk kuvvetlerinin bu alanda daha etkin bir şekilde faaliyet göstermesini gerektirmiştir. ABD’de, siber güvenlik yönetimi genellikle Ulusal Güvenlik Bakanlığı, FBI ve yerel kolluk kuvvetleri arasında iş birliği ile yürütülmektedir (DHS, 2018). Kolluk kuvvetleri, özellikle kritik altyapıların korunması, siber suçların soruşturulması ve siber tehditlerin önlenmesi konularında önemli bir rol oynamaktadır. FBI’ın 2002 yılında kurulan Siber Birimi (Cyber Division), bu alanda federal düzeydeki çabaların bir örneğidir. Birim, fidye yazılımları, kimlik hırsızlığı ve ulus devlet destekli siber saldırılar gibi sorunlarla mücadele etmektedir (FBI, 2021). Aynı zamanda, FBI’ın InfraGard programı, kamu ve özel sektör arasındaki bilgi paylaşımını artırarak siber tehditlere karşı daha güçlü bir savunma oluşturmayı amaçlamaktadır. Yerel kolluk kuvvetleri ise, siber suçlarla mücadelede genellikle sınırlı kaynaklara sahip olmalarına rağmen, eğitim ve iş birliği programlarıyla desteklenmektedir. DHS’in geliştirdiği Siber Güvenlik ve Altyapı Güvenliği Ajansı (Cybersecurity and Infrastructure Security Agency-CISA), yerel kolluk kuvvetlerine eğitim ve teknik destek sağlamaktadır (DHS, 2020). Ayrıca, eyalet bazında geliştirilen Birleşim Merkezleri (Fusion Centers), federal ve yerel düzeydeki siber güvenlik girişimlerini koordine eden önemli araçlar olarak işlev görmektedir. Dünyada olduğu gibi ABD’de de kolluk kuvvetlerinin siber güvenlik yönetimindeki en büyük zorluklardan biri, hızla gelişen teknolojilere ve artan siber tehditlere

ayak uydurabilmektir. Bu nedenle, kamu-özel sektör iş birliğinin güçlendirilmesi ve daha geniş çaplı bir koordinasyon mekanizması oluşturulması gerekmektedir. Siber güvenlik yönetişiminde etkinliğin artırılması, sadece ulusal güvenlik için değil, aynı zamanda bireylerin ve organizasyonların güvenliği için de kritik bir gerekliliktir. ABD'nin kolluk kuvvetleri, FBI ve CISA gibi önemli kuruluşlar aracılığıyla siber suçlarla mücadelede etkin bir strateji izlemektedir.

6.1. ABD’de Kolluk Yapılanması

ABD, kolluk kuvvetleri yapılanmasında federal, eyalet ve yerel düzeyde çok katmanlı bir sisteme sahiptir. Bu yapılanma, siber güvenlik de dahil olmak üzere geniş bir suç yelpazesıyla mücadele etmek için farklı kurumların iş birliğini gerektirmektedir (FBI, 2021). ABD’nin federal düzeydeki kolluk birimleri arasında en dikkat çeken FBI olarak karşımıza çıkmaktadır. FBI, 26 Temmuz 1908’de ABD Adalet Bakanlığı tarafından kurulmuştur. İlk olarak BOI "Bureau of Investigation-Soruşturma Bürosu" adıyla biliniyordu. FBI’ın kuruluş amacı, federal bölgelerdeki istihbari faaliyetlerden sorumlu bir kurum oluşturmaktır. Yıllar boyunca, özellikle beyaz yakalı suçlar, kara para aklama ve dolandırıcılık gibi konulara odaklanılmıştır. 1924 yılında J. Edgar Hoover BOI’da yönetici konumu gelmiştir. Hoover, BOI’nin profesyonel bir soruşturma kurumu haline gelmesinde kritik bir rol oynamıştır. Hoover döneminde, ajanların seçiminde, eğitim ve görevlerde reformlar gerçekleştirmiş, BOI ajanlarının etik ve disiplin standartları yükseltilmiştir. 1930’larda FBI, organize suçlarla, özellikle de Büyük Buhran sırasında artan kaçakçılık faaliyetleriyle mücadelede etkili olmuştur. John Dillinger, Bonnie ve Clyde gibi ünlü suçluların yakalanmasında önemli roller oynamıştır. FBI, bu dönemde parmak izi analizi ve adli tıp gibi modern suç araştırma tekniklerini uygulamaya başlamıştır. 1935 yılında FBI olarak yeniden adlandırılmış ve kapsamı genişletilmiştir. İkinci Dünya Savaşı sırasında ajanlar casusluk ve sabotaj faaliyetlerini engellemek için görev yapmıştır (FBI, 2024).

Soğuk Savaş Dönemi (1947-1991), FBI için casusluk ve iç güvenlik tehditlerinin ön planında olduğu bir dönemdir. 1990’lardan itibaren FBI, organizasyonu güncel tutarak yeni tehditlere uyum sağlamaya çalışmaktadır. Eylül 2001 saldırılarından sonra FBI’nın görünürlüğü büyük ölçüde değiştiği görülmektedir. Terörle mücadele, FBI’nın temel misyonu haline gelmiş olup, kurum, terörizm ve uluslararası terörle mücadele operasyonlarını genişletmektedir. 21. yüzyılın ilerleyen yıllarında FBI, siber suçlar, dijital dolandırıcılık, radikal radikalleşme ve yabancı tehditlere karşı önemli bir rol üstlenmektedir. Bugün FBI, Adalet Bakanlığı’na bağlı bir kurum olarak hem iç güvenlik hem de suç soruşturması aşamalarında görev yapmaktadır. Ana sorumluluk alanları içerisinde terörizmle mücadele, siber suçlar, beyaz yakalı suçlar, insan

ticareti ve çocuk istismarı yer almaktadır. FBI, dünya çapında 50'den fazla ofisle faaliyet gösteren uluslararası bir kurum haline gelmiştir. Yaklaşık 36.000 çalışan ile ABD'nin en büyük ve en etkili federal kolluk kuvvetlerinden birini teşkil etmektedir. FBI'ın tarihi, ABD'nin tehdit algılarına ve ulusal güvenlik özelliklerine paralel olarak sürekli olarak geliştirilmektedir. Kurum, modern suçlarla mücadelede ön saflarda yerini korumaya devam etmektedir. FBI, özellikle siber suçlarla mücadele konusunda yetkili olup, İnternet Suçları Şikâyet Merkezi (IC3) aracılığıyla birey ve kurumların bildirimlerini toplamaktadır. (DOJ, 2020). Bunun yanı sıra, DHS'ye bağlı CISA da, kritik altyapıların korunması için siber tehditlere karşı çalışmalar yürütmektedir. (CISA, 2022)

Tablo 6. 1.ABD'de Kolluk Kuvvetlerinin Yapısı

Kolluk Birimi	Görev Alanı	Alt Birimler
Federal Soruşturma Bürosu (FBI)	Ulusal güvenlik, terörle mücadele ve federal suçlar	- Siber Suçlarla Mücadele- Terörle Mücadele Birimi- Organize Suçlar Birimi
Uyuşturucuyla Mücadele Dairesi (DEA)	Uyuşturucu kaçakçılığı ve ilgili suçlarla mücadele	- Operasyonel Taktik Birimler- İstihbarat ve Analiz Birimleri
Gizli Servis (USSS)	Başkanlık koruması, sahtecilikle mücadele ve siber suçlar	- Siber Güvenlik Operasyon Birimi- Başkanlık Koruma Birimi
Gümrük ve Sınır Koruma (CBP)	Sınır güvenliği, göç kontrolü ve gümrük denetimleri	- Sınır Devriye Birimleri- Deniz Operasyon Birimleri
Federal Acil Durum Yönetimi Ajansı (FEMA)	Doğal afetler ve acil durumlara müdahale	- Afet Müdahale Birimleri- Eğitim ve Hazırlık Programları

Bu tablo, tezin yazarı tarafından açık kaynak kullanılarak, ABD'nin genel kolluk yapılanması hakkında bir çerçeve sunmak amacıyla hazırlanmıştır.

Eyalet düzeyinde ise, her bir eyaletin kendi polis gücü ve soruşturma birimi bulunmaktadır. Bu birimler, federal kurumlarla koordinasyon içerisinde çalışarak eyalet sınırları içindeki suçlarla mücadele etmektedir. Özellikle Kaliforniya ve New York gibi eyaletlerde, siber güvenlik konusunda özel birimlerin oluşturulduğu görülmektedir (National Governors Association, 2021). Yerel düzeyde ise şehir ve kasaba polis departmanları, topluluk güvenliğini sağlama ve yerel suçları önleme konusunda görev yapmaktadır. Büyük şehirlerdeki polis departmanlarının çoğu, siber suçlarla mücadele için teknoloji destekli birimlere sahiptir. Örneğin, New York

Polis Departmanı (NYPD), Siber Suçlar Birimi ile bu alandaki öncü departmanlardan biri olarak karşımıza çıkmaktadır (NYPD, 2020).

6.2. ABD'nin Kolluk Teşkilatlarında Siber Güvenliğin Yeri ve Geliştirilen Stratejiler

ABD, dijital tehditlerin giderek artan karmaşıklığına karşı kolluk kuvvetlerinde siber güvenliğe büyük önem atfetmektedir. Bu bağlamda hem federal hem de eyalet düzeyindeki teşkilatlar, siber suçlarla mücadele için özel birimler ve stratejiler geliştirmiştir (FBI, 2021). ABD'de siber güvenlik stratejilerinin merkezinde FBI yer almaktadır. FBI, 2002 yılında Siber Birimi kurarak siber güvenlik alanında kapsamlı bir mücadele başlatmıştır. Bu birim, ABD'nin siber tehditlere karşı ulusal düzeyde savunmasında kilit bir rol oynamaktadır. Siber Birim, hem ulusal güvenliği tehdit eden siber saldırılara hem de bireylerin ve işletmelerin karşı karşıya olduğu siber suçlara odaklanmaktadır (FBI, 2021). Siber Birim'in temel görevlerinden biri, kritik altyapılara yönelik siber saldırıları önlemek ve bu tür saldırıların sonuçlarını en aza indirmektir. Özellikle enerji, sağlık ve finans sektörlerinde güvenlik açıklarının tespit edilmesi ve giderilmesi için kamu ve özel sektörle iş birliği yapmaktadır. Ayrıca, uluslararası tehditlerle mücadelede diğer ülkelerin kolluk kuvvetleriyle koordinasyonu sağlamaktadır (FBI, 2021). Birim, siber suçlara karşı mücadelede ileri teknoloji araçlarından ve uzman ekiplerden faydalanmaktadır. Fidyeye yazılımlar, kimlik hırsızlığı, veri ihlalleri ve ulus devlet destekli saldırılar gibi karmaşık tehditlerle başa çıkmak için yenilikçi yöntemler geliştirmektedir. Ayrıca, FBI'nın InfraGard programı aracılığıyla özel sektörle bilgi paylaşımı yaparak, tehditlere karşı erken uyarı sistemlerini güçlendirmektedir (FBI, 2020). FBI'nın Siber Birimi, yalnızca tehditleri engellemekle kalmaz, aynı zamanda kamu farkındalığını artırmak için eğitim ve bilinçlendirme kampanyaları düzenler. Örneğin, işletmelerin ve bireylerin siber güvenlik önlemleri almasını teşvik etmek amacıyla düzenli raporlar ve rehberler yayımlamaktadır (FBI, 2021). FBI, IC3 ve Siber Suç Birimi aracılığıyla bireyler ve kurumların karşılaştığı siber tehditleri incelemekte ve bu tehditlere karşı etkili çözümler üretmektedir (DOJ, 2020). Ayrıca, DHS'a bağlı CISA, kritik altyapıların korunmasında lider bir rol oynamaktadır. Bu ajans, kamu ve özel sektörle iş birliği yaparak siber saldırılara karşı ulusal savunma mekanizmaları geliştirmektedir (CISA, 2022).

ABD'de Birleşim Merkezleri (Fusion Centers), yerel, eyalet ve federal kolluk kuvvetleri ile özel sektör arasında bilgi paylaşımını ve iş birliğini artırmak amacıyla oluşturulmuş stratejik merkezlerdir. İlk olarak 2003 yılında kurulan bu merkezler, özellikle 11 Eylül 2001 terör saldırılarından sonra ulusal güvenliği artırmak ve tehditlere daha hızlı yanıt vermek için geliştirilen bir stratejinin parçasıdır (DHS, 2020). Birleşim merkezleri, sadece terörle mücadele değil, aynı zamanda siber tehditler, organize suçlar ve doğal afetler gibi geniş bir tehdit

yelpazesini ele almak için çalışmaktadır. Bu merkezlerin temel amacı, bilgi paylaşımını kolaylaştırarak tehditlerin erken tespit edilmesini ve koordineli bir yanıt verilmesini sağlamaktır. Özellikle siber güvenlik alanında, birleşim merkezleri kritik altyapıların korunması ve yerel düzeydeki güvenlik açıklarının kapatılması için önemli bir araçtır (NFCA, 2021). Birleşim merkezleri, federal kurumlarla koordinasyon sağlamakla birlikte, yerel topluluklarla da yakın bir iş birliği içerisinde. Örneğin, DHS'nin İç Güvenlik Bilgi Ağı (Homeland Security Information Network-HSIN) gibi araçları, birleşim merkezlerinin güvenilir bilgiye erişimini kolaylaştırmaktadır. Ayrıca, bu merkezler özel sektörle ortaklıklar kurarak, siber tehdit istihbaratını paylaşp, tehditlerin etkisini en aza indirmek için kolektif çözümler geliştirmektedir (DHS, 2020). Ancak birleşim merkezleri, veri gizliliği ve bireysel haklar konularında eleştirilere de maruz kalmaktadır. Özellikle, geniş çaplı veri toplama ve analiz süreçlerinin, vatandaşların mahremiyetini ihlal edebileceği endişeleri dile getirilmektedir. Bu nedenle, birleşim merkezleri hem güvenliği sağlamak hem de vatandaş haklarını korumak için dengeleyici bir yaklaşım benimsemeye çalışmaktadır (NFCA, 2021). Birleşim Merkezleri, ABD'de yerel düzeyde güvenlik yönetiminin ve siber tehditlerle mücadelenin temel taşlarından biri haline gelmiştir. Bilgi paylaşımını ve iş birliğini artıran bu merkezler, ulusal güvenliğin ve toplumsal dayanıklılığın güçlendirilmesinde kritik bir role sahiptir.

ABD, siber güvenlik stratejilerinde teknolojiye dayalı çözümleri ön planda tutmaktadır. Örneğin, Yapay Zekâ (AI) ve Büyük Veri (Big Data) analiz yöntemleri, olası tehditlerin tespit edilmesi ve önlenmesi için kullanılmaktadır (DHS, 2021). Ayrıca, federal düzeydeki kurumlar arasında veri paylaşımı ve koordinasyonun artırılması amacıyla "National Cyber Investigative Joint Task Force- Ulusal Siber Araştırma Ortak Görev Gücü" gibi yapılar oluşturulmuştur (FBI, 2021). Yerel düzeyde ise, büyük şehirlerdeki polis departmanlarının siber suçlarla mücadeleye yönelik özel birimleri bulunmaktadır. Örneğin, New York Polis Departmanı, teknolojik suçlara odaklanan birimlerini genişleterek siber güvenlik tehditlerine karşı etkin bir yapı oluşturmuştur (NYPD, 2020). Bu tür yerel inisiyatifler, federal ve eyalet düzeyindeki stratejilerle entegre bir şekilde çalışmaktadır.

Uluslararası iş birliği ABD'nin siber güvenlik stratejilerinde önemli bir yer tutmaktadır. INTERPOL, EUROPOL ve diğer uluslararası kuruluşlarla iş birliği içinde çalışan ABD, dünya çapında operasyonlar düzenlemektedir. Özellikle NATO bünyesindeki Siber Savunma Mükemmeliyet Merkezi (CCDCOE) ile ortak tatbikatlar yürütmektedir (NATO, 2020). Neticesinde ABD'nin kolluk teşkilatlarında siber güvenliğin önemi giderek artmakta ve bu

alandaki yenilikçi stratejiler geliştirilmektedir. Federal, eyalet ve yerel düzeydeki iş birliği mekanizmaları hem ulusal hem de uluslararası düzeyde siber suçlarla etkin bir mücadele sağlanmasına katkıda bulunmaktadır.

6.3. Uluslararası İş birliği Örnekleri ve Küresel Yönetişime Katkısı

ABD kolluk kuvvetleri, siber güvenlik tehditlerinin uluslararası bir boyut kazandığını göz önünde bulundurarak, diğer ülkelerin güvenlik birimleriyle iş birliğini artırmıştır. Bu kapsamda, FBI, Siber Eylem Timleri (Cyber Action Teams- CATs) gibi özel birimler aracılığıyla uluslararası siber suç operasyonlarında aktif rol almaktadır. Bu ekipler, fidye yazılım saldırıları, ulus-devlet destekli siber tehditler ve organize suç şebekeleri gibi küresel ölçekli sorunlarla mücadelede etkili olmaktadır (FBI, 2020).

Kolluk kuvvetleri ayrıca, küresel yönetim standartlarının belirlenmesine de katkıda bulunmaktadır. ABD, Budapeşte Siber Suç Sözleşmesi gibi uluslararası anlaşmalara taraf olarak, siber suçların sınır ötesi boyutlarıyla mücadelede diğer ülkelerle ortak politikalar geliştirmiştir (Council of Europe, 2001). Ayrıca FBI, INTERPOL ve EUROPOL gibi uluslararası kuruluşlarla yakın iş birliği yaparak bilgi paylaşımı ve ortak operasyonlar yürütmektedir (DHS, 2020). Kolluk kuvvetlerinin küresel siber güvenliğe katkısını artırmak için ABD, siber tehdit istihbaratının paylaşımına büyük önem vermektedir. Örneğin, CISA kamu ve özel sektör arasında bilgi akışını teşvik ederek küresel iş birliklerini güçlendirmiştir (Congress.gov, 2015). Bunun yanı sıra, FBI'nın InfraGard programı, özel sektör ortaklarıyla iş birliği yaparak küresel tehditlere karşı daha güçlü bir savunma mekanizması oluşturmuştur (FBI, 2021).

ABD ve AB arasında, siber güvenlik alanında stratejik bir ortaklık bulunmaktadır. "AB-ABD Siber Diyalog" çerçevesinde, taraflar arasında bilgi paylaşımı, tehdit analizi ve politika geliştirme süreçlerinde iş birliği sağlanmaktadır (European Council, 2020). Bu iş birliği, özellikle kritik altyapıların korunması ve fidye yazılım saldırılarına karşı alınan önlemler üzerinde yoğunlaşmıştır (U.S. Department of Homeland Security, 2021). ABD, EUROPOL ile siber suçlarla mücadelede güçlü bir ortaklık geliştirmiştir. ABD Adalet Bakanlığı ve FBI, EUROPOL bünyesindeki operasyonlara destek sağlayarak çok uluslu suç ağlarının çökertilmesinde önemli bir rol oynamaktadır (EUROPOL, 2021). Örneğin, "Operation Trojan Shield" isimli operasyonda, ABD ve EUROPOL iş birliği sayesinde yüzlerce suçlu tutuklanmış ve önemli miktarda yasa dışı malzeme ele geçirilmiştir (DOJ, 2021). ABD, INTERPOL ile siber suçların önlenmesi ve soruşturulması konularında aktif bir iş birliği yürütmektedir. INTERPOL

Siber Suç Merkezi'nin operasyonlarına teknik destek sağlayarak, dünya genelindeki suç ağlarının tespitine katkıda bulunmaktadır (INTERPOL, 2021). Örneğin, ABD'nin katkılarıyla gerçekleştirilen "Operation Infrared" kapsamında, küresel ölçekte çok sayıda suçlunun yakalanması sağlanmıştır (INTERPOL, 2022). ABD, NATO ve Birleşmiş Milletler gibi uluslararası kuruluşlar aracılığıyla küresel siber güvenlik politikalarının geliştirilmesine liderlik etmektedir. NATO'nun siber savunma politikasında etkin bir rol oynayan ABD, aynı zamanda Birleşmiş Milletler'in "Siber Suçlarla Mücadele Programı'nın finansal ve teknik destekçilerinden biridir (NATO, 2021; UN, 2021).

ABD kolluk kuvvetleri, siber tehditlere yönelik küresel iş birliğini güçlendirme çabalarının yanı sıra, diğer ülkelerin kapasitelerini artırmak için eğitim ve teknik destek sağlamaktadır. Bu çerçevede, uluslararası ortaklara yönelik eğitim programları ve bilgi teknolojisi altyapısının geliştirilmesine yönelik projeler uygulanmaktadır (Goodman, 2016). ABD'nin gelişen kapsamlı dijital altyapı projeleri, siber güvenlik eğitim programları ve teknoloji transfer çalışmaları, bir yandan bu ülkelerin dijital kapasitelerini artırmayı hedeflerken, diğer yandan siber sömürgeleştirme endişelerini gündeme getirmektedir. Kısaca siber sömürgeleştirme, dijital teknolojilerin güçlü devletler tarafından diğer ülkelerin aleyhine kullanılması anlamına gelmektedir. ABD'nin dijital ekonomideki baskın rolü ve Amerikan teknolojisinin dünya çapında yaygınlığı, gelişen ülkelerin dijital altyapılarının ABD merkezli platformlara ve hizmetlere bağımlı hale gelmelerine yol açmaktadır (Carr, 2016). Bu bağımlılık, veri kontrolünün ve bilginin ABD tarafından yönlendirilmesi gibi ciddi egemenlik sorunlarına neden olabilmektedir. ABD'nin teknoloji devleri, bulut hizmetleri, yapay zekâ altyapıları ve veri yönetim sistemleri ile kritik alanlarda dünya çapında bir hakimiyet sağlamış olduğu görülmektedir. Gelişmekte olan ülkelerde, veri sistemlerinin ortak kullanıma sunulması aynı zamanda bu ülkelerin, küresel dijital ekosisteme bağımlı hale gelmesine neden olabilmektedir (Chander, 2013). Bu durum, yalnızca ekonomik değil, aynı zamanda politik bir üstünlük yaratmaktadır.

Ayrıca ABD'nin ulusal güvenlik politikaları çerçevesinde uygulanan siber gözetim ve veri erişim yöntemleri, siber sömürgeleştirmenin daha görünür bir boyut haline gelmesine neden olmaktadır. Edward Snowden'ın çalışmaları, ABD'nin dünya çapındaki gözetim programlarını ve bu programların diğer ülkelerin dijital ülkelerini nasıl ihlal ettiğini gözlerin önünde sermiştir (Greenwald, 2014). Bu bağlamda, ABD'nin siber politikalarının, gelişmekte olan ülkelerin dijital egemenliklerinin üzerinde egemenlik ihlali yapma potansiyeli olduğu ifade edilebilmektedir. Bu tür politikalarının etik bir temelde geliştirilmesi gerekmektedir. Aksi

takdirde, ABD'nin küresel dijital gelişimi, gelişen ülkeler için fırsatlardan çok kısıtlamalar yaratabileceği değerlendirilmektedir. ABD'nin kolluk kuvvetleri, bu dijital üstünlüğü koruma ve genişletme çabalarında kritik bir rol oynamaktadır. Ulusal güvenlik politikaları ve kolluk kuvvetleri, bu yapının desteklenmesinde kritik öneme sahiptir. FBI, DHS ve NSA gibi kurumlar hem ulusal hem de uluslararası düzeyde siber güvenlik operasyonları yürütürken veri de toplamaktadır. Özellikle NSA, uluslararası gözetim faaliyetleri ve veri toplama kapasitesiyle dikkat çekmektedir. Edward Snowden'ın ifşaatları, NSA'nın yalnızca ABD vatandaşlarını değil, aynı zamanda diğer ülkelerin liderlerini ve vatandaşlarını da gözetlediğini ortaya koyarak, ABD'nin dijital hegemonya stratejisini gözler önüne sermektedir (Greenwald, 2014).

6.4. Küresel Siber Güvenlik Endeksinde ABD'nin Konumu ve Kolluk Kuvvetlerinin Etkisi

GCI'da ABD, sıralamalarında tarihsel olarak üst sıralarda yer almaktadır. 2014 yılında açıklanan endekste, ABD birinci sırada yer alarak siber güvenlik önlemlerinin en yüksek seviyede olduğu ülke olarak tanımlanmaktadır (Siber Bülten, 2014). Bu başarı, ABD'nin siber güvenlik alanındaki güçlü yasal düzenlemeleri, teknik kapasitesi ve uluslararası iş birlikleri sayesinde elde edilmiştir.

2024 yılına gelindiğinde, GCI raporunda sıralama yapısından seviyelendirme yapısına geçilmiş ve ülkeler "örnek alınan ülkeler" gibi kategorilerde değerlendirilmiştir. ABD'nin siber güvenlik alanındaki liderliği, internet teknolojilerinin ABD merkezli gelişmesiyle paralel değerlendirilebilir. Kapsamlı yasal çerçeveleri, gelişmiş teknik altyapısı ve uluslararası iş birlikleriyle desteklenmektedir. Özellikle FBI ve İç Güvenlik Bakanlığı gibi kurumlar, siber tehditlere karşı proaktif stratejiler geliştirerek ülkenin siber güvenlik kapasitesini artırmaktadır (FBI, 2021; DHS, 2020). Bu kurumlar ABD'nin diğer kolluk kuvvetleri ve diğer ülkelerin kolluk kuvvetleriyle iş birliklerine imza atarak küresel yönetim kavramı paralelinde hareket etmektedir.

ABD, GCI'da tarihsel süreçte üst sıralarda yer almış ve siber güvenlik alanında liderliğini sürdürmüştür. ABD'nin siber güvenlikteki güçlü duruşu ve sürekli gelişen stratejileri, küresel siber güvenlik ekosisteminde önemli bir rol oynamaya devam etmektedir.



7. SONUÇLAR VE ÖNERİLER

Siber alanda yaşanan gelişmeler küresel dünyanın köy olarak adlandırılmasının temel nedenlerinden biri olarak karşımıza çıkmaktadır. İnternet erişimi ile dijital dünyada sınırlar ortadan kalkmakta geleneksel güvenlik anlayışında dönüşümünü hızlandırmaktadır. Kopenhag Ekolü'nün tartıştığı yeni çerçevede güvenlik çok yönlü, çok çeşitli ve çok aktörlü bir yapıya doğru evrilmektedir. Siber alanda yaşanan gelişmeler, siber tehditleri ve siber suçları beraberinde getirmiş, devletler tek başına bu tehditlerle mücadele edemez hale gelmişti. Dijital kaleler kurmak, taş kaleler kurmaktan zor ve karmaşık bir hale gelmiştir. Bu siber tehditlere yönelik stratejiler, yalnızca ulusal düzeyde değil, bölgesel ve uluslararası düzeyde de uzun dönemde iş birliklerini elzem kılmaktadır.

Devletler iş birliği ve çok taraflı siber güvenlik anlaşmalarıyla siber tehditlerin yönetiminde temel bir rolde bulunmaktadır. Mahremiyet ve dijital hakların korunması, siber güvenliğin etik ve toplumsal boyutlarını ortaya çıkarmakta, devletlerin bu alandaki sorumluluklarını genişletmektedir. Geleneksel güvenlik politikalarının dönüşümü, devletlerin yalnızca askeri tehditlerle değil; ekonomik, teknolojik ve toplumsal tehditlerle de karşı karşıya olduğu gerçeğini ortaya koymaktadır. Kopenhag Ekolü'nün genişletilmiş güvenlik yaklaşımı çerçevesinde analiz edildiğinde, siber tehditlerin teknik boyutlarının ötesine geçilerek toplumsal ve politik yönlerinin önemi göze çarpmaktadır. Bu perspektife göre siber tehditler, yalnızca bireysel veya ulusal güvenlik sorunu teşkil etmemekte, uluslararası güvenlik çevresinin güç dinamiklerini etkileyen önemli bir unsur haline gelmektedir. Örneğin kritik altyapılara yapılan siber saldırılar ya da fidye yazılımı gibi tehditler, devletlerin iç istikrarını ve uluslararası düzeni doğrudan etkileyebilecek çok yönlü sorunlar olarak değerlendirilmektedir.

Dijital alanda gelişmeler dünyanın her noktasını etkilerken ülkelerin bu dijital gelişmeleri yakalamaları aynı seviyede gerçekleşmemektedir. Kimi ülkeler rol model olurken, kimi ülkeler gelişmemiş ya da gelişmekte olan kategorisinde kalmaktadır. Tez çerçevesinde incelen ülkelere bakıldığında ABD, internetin doğuşuna liderlik ederek altyapı sistemlerinin temelini oluşturmuştur. Fransa, Minitel gibi erken dönem teknolojilerle kullanıcı dostu çözümler sunmuş, ancak küresel internetin gerisinde kalmıştır. Türkiye de interneti ilk olarak akademik kullanımda ağırlıklı olarak benimsemiş, siber tehditlere karşı çalışmalarına 2000'lerin ilk çeyreğinde başlamıştır. Her üç ülke de internetin yaygınlaşmasıyla birlikte siber güvenlik stratejisi geliştirmiş ve siber tehditlerle mücadelede ulusal ve uluslararası iş birliklerine yönelmiştir. Yasal düzenlemelerin ulusal mevzuatlarda geliştirilmesi internetin tarihçesine paralel olarak gerçekleşmiş olup, internetin öncüsü ABD siber suçlarla en erken karşılaşan ülke

olmuş ve buna hızlı bir şekilde yasal düzenlemelerle yanıt vermiştir. Fransa, Minitel döneminde siber suç tehlikesini düşük düzeyde yaşamış ancak internetin yaygınlaşmasıyla bu tehditlerle karşı karşıya kalmıştır. Türkiye ise, internetin geç yaygınlaşması nedeniyle siber suçlarla daha geç tanışmış, buna rağmen hızlı bir şekilde yasal düzenlemeler ve ulusal stratejiler geliştirmiştir.

2024 yılında Türkiye, GCI'da tüm alanlarda tam puan alarak "örnek alınan ülkeler" arasında en üst seviyede yer almıştır. Bu başarı, Türkiye'nin siber güvenlik alanındaki kapsamlı çalışmalarının bir sonucudur. Ayrıca, "2024-2028 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" ile stratejik hedefler bütüncül bir yaklaşımla ele alınmaktadır. Fransa da GCI'da üst sıralarda yer alan ülkeler arasında yer almıştır. Güçlü yasal çerçevesi, teknik kapasitesi ve uluslararası iş birlikleri sayesinde siber güvenlik alanında yüksek bir performans sergilemektedir. Fransa'da ANSSI aracılığıyla yürütülen çalışmalar, ülkenin siber tehditlere karşı dayanıklılığını artırmaktadır. Ayrıca, AB'nin siber güvenlik politikalarıyla uyumlu stratejiler geliştirerek bölgesel güvenliğe katkı sağlamaktadır. ABD ise GCI'da genel itibarıyla lider konumda bulunmaktadır. Gelişmiş teknik altyapısı, kapsamlı yasal düzenlemeleri ve siber güvenlik alanındaki inovasyonlarıyla dikkat çekmektedir. NSA ve DHS gibi kurumlar, ülkenin siber güvenlik stratejilerinin uygulanmasında kritik rol oynamaktadır. Ayrıca, ABD'nin özel sektörü ve akademik kurumları, siber güvenlik araştırmaları ve çözümleri konusunda dünya çapında etkiye sahiptir.

Tezde incelenen üç örnek değerlendirildiğinde Türkiye, Fransa ve ABD, GCI'da üst sıralarda yer alarak siber güvenlik alanında güçlü performanslarıyla dikkat çekmektedirler. Her üç ülke de yasal düzenlemeleri, teknik kapasiteleri ve uluslararası iş birlikleri alanlarında önemli adımlar atarak siber güvenliğin küresel yönetişimine katkıda bulunmaktadır. Türkiye'nin son dönemde elde ettiği başarı, siber güvenlik alanındaki yatırımlarının ve stratejik planlamalarının etkinliğini göstermektedir. Fransa ve ABD ise mevcut güçlü altyapıları ve sürekli gelişim çabalarıyla siber tehditlere karşı küresel güvenliğe katkı sağlamaya devam etmektedirler. Bu üç ülkenin siber suçlarla mücadeledeki etkin çalışmaları, küresel ölçekte siber güvenliğin sağlanmasına büyük katkı sağlamaktadır. ABD'nin teknoloji ve kaynak üstünlüğü, Fransa'nın AB politikalarıyla uyumu ve Türkiye'nin bölgesel tehditlere karşı hızlı tepkisi, farklı seviyelerde siber güvenlik stratejilerinin başarıya ulaşmasını desteklemektedir. Uluslararası bilgi paylaşımı ve operasyonel iş birlikleri, siber tehditlere karşı küresel bir savunma mekanizması oluşturarak bireylerden devletlere kadar herkesin daha güvenli bir ortamda yaşamasını sağlamaktadır.

Kurumsal kolluk yapılanmaları incelendiğinde ABD'nin siber suçlarla mücadeledeki kurumsal yapısının oldukça geniş olduğu gözlemlenmektedir. Federal düzeyde birden fazla kurum siber güvenlikten sorumlu olup, yetki alanları net bir şekilde belirlenmiştir. ABD'de çok paydaşlı yönetim yaklaşımı çerçevesinde özel sektörle sıkı iş birlikleri yapılmakta ve şirketlerin siber güvenlik kapasitesini artırmaya yönelik politikalar geliştirmektedir. Türkiye'de ise ABD'ye nazaran daha merkezi bir yaklaşımla siber güvenlik yönetimi yürüten Türkiye'de siber suçlarla mücadele, kolluk kuvvetleri yönünden temel olarak Emniyet Genel Müdürlüğü ve Jandarma Genel Komutanlığı bünyesindeki yapılanmayla yürütülmektedir. Siber suçlarla mücadelede ağırlıklı olarak ceza hukuku odaklı bir yaklaşım benimsenmektedir. Türkiye'nin bu alandaki kurumsal yapısı, Fransa ile benzerlik gösterse de ABD'ye kıyasla daha az çeşitlilik göstermektedir. Fransa'da siber suçlarla mücadele hem kolluk kuvvetleri (Jandarma ve Polis) hem de ANSSI gibi uzmanlaşmış ajanslar tarafından yürütülmektedir. Fransa'nın yapısı, AB yasaları ve düzenlemeleri ile daha entegre bir şekilde çalışmaktadır.

Küresel yönetime katkıları bakımından incelendiğinde ABD, NATO gibi askeri ittifaklar çerçevesinde müttefikleriyle yoğun bilgi paylaşımı yapmaktadır. Ayrıca, fidye yazılım gruplarını hedef alan küresel operasyonlarda liderlik rolü üstlenmektedir. ABD'nin uluslararası iş birliklerindeki stratejisi genellikle teknoloji üstünlüğüne dayanmaktadır. Türkiye INTERPOL ve EUROPOL gibi kuruluşlarla iş birliği yaparken aynı zamanda NATO üyesi olması sebebiyle ittifak kapsamında birçok ortak projede de yer almaktadır. Fransa, AB'nin siber güvenlik politikalarının şekillenmesinde öncü bir rol oynamaktadır. AB içinde ortak bir dijital savunma stratejisinin oluşturulmasını savunan ve bölgesel operasyonlara yüksek katılım sağlayan Fransa, ABD ile kıyaslandığında küresel operasyonlara katılımında genellikle daha zayıf bir tutum sergilemektedir. Kolluk kuvvetleri, hızla gelişen siber suçlar karşısında güçlü bir mevzuat, güçlü bir alt yapı ve kaliteli eğitim programları kapsamında artan iş birlikleri yönünde evrilmektedir.

Uluslararası iş birliğinin önemi, teknolojik altyapının güçlendirilmesi, farkındalık ve eğitim programları yaygınlaştırılması konuları küresel siber güvenliğin sağlanmasında önemli alanlar olarak ortaya çıkmaktadır. Siber tehditlerin küresel doğası, uluslararası düzeyde iş birliğini zorunlu kılmaktadır. Türkiye'nin INTERPOL ve NATO ile daha yakın iş birliği geliştirmesi, Fransa'nın EUROPOL ile yürüttüğü ortak çalışmaları genişletmesi ve ABD'nin teknoloji odaklı uluslararası projelerde liderlik rolünü sürdürmesi gerekmektedir. Siber suçlarla etkili mücadele, ileri teknolojilerin kullanımı ile mümkündür. Türkiye'nin bu alanda yatırımlarını artırması, Fransa'nın uzmanlaşmış birimlerinin teknik kapasitesini genişletmesi ve ABD'nin

teknolojik liderliğini sürdürülebilir kılması önem taşımaktadır. Toplumun bilinçlendirilmesi, siber güvenliğin sürdürülebilirliği açısından kritik bir role sahiptir. Üç ülkenin de daha kapsayıcı ve yaygın farkındalık kampanyaları yürütmesi gerekmektedir.

Siber güvenlikte kolluk kuvvetlerinin etkinliği, teknik bilgi ve donanım düzeyine bağlı olarak değişmektedir. Ülkelerin, kolluk kuvvetlerinin hızlı bir şekilde ilerleyen, çeşitlenen dijital suçlarla mücadelede daha etkin hale gelmesi için eğitim programlarına ve altyapıya daha fazla yatırım yapmaları gerekmektedir. Siber güvenlik sınırlarını aşan bir politika çerçevesinde ele alınmalı ve bu doğrultuda uluslararası normların benimsenmesi teşvik edilmelidir. Devletler siber güvenlik politikalarını uluslararası hukuk çerçevesine uyumlaştırmalı ve bu normların uygulanabilirliğini sağlamalıdır. Devletlerin siber güvenlik politikalarını belirlerken, özel sektör, akademik kuruluşlar ve sivil toplum aktörlerinin katkılarına daha fazla yer vermesi gerekmektedir. Çok paydaşlı bir yönetim modeli kullanılarak siber tehditlere karşı daha esnek ve kapsamlı çözümler üretilmelidir. Siber güvenlik yalnızca teknik bir mesele olarak ele alınmayıp, aynı zamanda siber eğitim alanı ve toplumların dijital okuryazarlığıyla da doğrudan bağlantılı olarak değerlendirilmesine önem verilmesi gerekmektedir. Tüm ülkeler, dijital güvenlik bilincini artıracak kampanyalar düzenlemeli ve bu alanda eğitim programlarını yaygınlaştırmalıdır.

Sonuç olarak, küresel yönetim siber güvenliğin tesisi açısından önemli bir yaklaşımdır. Kolluk teşkilatlarının yerelde kamu-özel kurumlar, sivil toplum örgütleri arasında yönetimi tesis etmelerini müteakip uluslararası alanda da küresel yönetimin tesisi için gayretlerini arttırmaları gerektiği değerlendirilmektedir. Siber suçların asimetrik ve sınır aşan yapısı sebebiyle klasik suçlara nazaran küresel iş birlikleri, ortak kanun ve prosedürler oluşturulması bu suçların önlemesi açısından önemlidir. ABD ileri teknolojilerin öncüsü olması sebebiyle siber güvenlikte de öncü konumdadır. Fransa hem ulusal düzeyde yakaladığı gelişim hem de AB'nin kurucu üyesi olmasının getirdiği siber güvenlik alanındaki avantajlarla ileri bir seviyede olduğu görülmektedir. Türkiye ise jeopolitik konumu gereği geleneksel tehditlerle mücadele ederken gelişen ekonomisi, altyapı yatırımları, küreseli yakalayan inovasyon girişimleriyle siber güvenlikte hem bölgesel hem de küresel alanda etkinliğini arttırmaktadır.

Küresel siber güvenliğin yönetiminde bir aktör olarak kolluk kuvvetlerinin rolü giderek artmakta, küresel siber güvenliğin sağlanmasında kolluk güçlerinin başarısı ülkeler arası iş birliğine daha da bağılı hale gelmektedir. Siber suçların ağırlıklı olarak uluslararası boyut taşınması, kolluk kuvvetlerinin sınır ötesi koordine edilmesini ve bilgi paylaşımını zorunlu kılmaktadır. Bu doğrultuda bu üç ülkenin siber güvenlik yönetiminde artan bir öneme haiz olan kolluk kuvvetlerinin küresel siber güvenlik ekosisteminde daha etkin bir konuma geleceğini söylemek mümkündür.





KAYNAKLAR

- Abdulrauf, L. A., and Basu, S. (2022). Global Cybersecurity Index as a Tool for Capacity Building. *Journal of Cyber Policy*, 7(1), 56-72.
- Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). (2021). France cybersecurity strategy. <https://www.ssi.gouv.fr>, Erişim Tarihi: 12.12.2024.
- Agence nationale de la sécurité des systèmes d'information. (2025). Anational cybersecurity strategy." Retrieved from <https://www.ssi.gouv.fr>, Erişim Tarihi: 10.01.2025.
- Akgül, M. ve Kırılıdoğ, M. (2015). Türkiye'de internetin tarihi. *Bilgi Teknolojileri Dergisi*, 8(1), 1-15.
- Altıntaş, F. F. (2022). G7 Ülkelerinin Siber Güvenlik Performanslarının Analizi: Entropi Tabanlı Mabac Yöntemi İle Bir Uygulama. *Güvenlik Bilimleri Dergisi*, 11(1), 263-286. <https://doi.org/10.28956/gbd.11>.
- Anadolu Ajansı. (2022). Türkiye'den BM Destekli Siber Güvenlik Eğitimleri. <https://www.aa.com.tr>, Erişim Tarihi: 10.01.2025.
- Anadolu Ajansı. (2024). Türkiye siber güvenlikte dünyaya "rol model" olarak gösterildi. <https://www.aa.com.tr/tr/ekonomi/turkiye-siber-guvenlikte-dunyaya-rol-model-olarak-gosterildi/3382120>, Erişim Tarihi: 02.11.2024.
- Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.
- Ankara Üniversitesi Bilgi İşlem Daire Başkanlığı (BİDB). (2018). Bilgi Sistemlerinin Güvenliğine İlişkin OECD Rehber İlkeleri. <https://bid.ankara.edu.tr/wp-content/uploads/sites/139/2018/08/BİLGİ-SİSTEMLERİNİN-GÜVENLİĞİNE-İLİŞKİN-OECD-REHBER-İLKELERİ.pdf>, Erişim Tarihi: 02.11.2024.
- ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). (2013). <https://www.ssi.gouv.fr>. Erişim Tarihi: 10.12.2024.
- Bada, M., Sasse, M. A., and Nurse, J. R. (2019). "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?" *Cyber Security*, 5(1), 1-16.
- Başaran, İ. ve Şahin, O. (2020). Türkiye'nin Ulusal Siber Güvenlik Stratejisi ve Uygulamaları. *Siber Güvenlik Dergisi*.
- Bendell, B. (2020). Fransa'nın Siber Güvenlik Politikaları ve Küresel Katkıları. *Cyber Policy Review*.
- Berners-Lee, T. (2000). *Web'i Örmek: World Wide Web'in orijinal tasarımı ve nihai kaderi*. Harper San Francisco.
- Biermann, F., et al. (2009). *Global Environmental Governance: The Role of Non-State Actors*. MIT Press.

- Bilgi Teknolojileri ve İletişim Kurumu [BTK]. (2016). Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2016-2019). <https://www.btk.gov.tr>, Erişim Tarihi: 10.12.2024.
- Bilgi Teknolojileri ve İletişim Kurumu [BTK]. (2020). Ulusal Siber Olaylara Müdahale Merkezi (USOM). BTK Yayınları.
- Birleşmiş Milletler Genel Kurulu. (1998). Uluslararası güvenlik bağlamında bilgi ve telekomünikasyon alanında gelişmeler (A/RES/53/70).
- Birleşmiş Milletler Genel Kurulu. (2004). Uluslararası güvenlik bağlamında bilgi ve telekomünikasyon alanında gelişmeler (A/59/454).
- BM Türkiye. (2021). Türkiye'nin BM Siber Güvenlik Çalışmalarına Katkısı. <https://www.un.org>, Erişim Tarihi: 10.01.2025.
- Bojadžijev, M., and Fidler, D. P. (2018). Cybersecurity and the Role of Law Enforcement in a Digital Age. Cambridge University Press.
- Brown, A. (2021). Global governance and cyber security: The rise of digital colonialism. *International Security Journal*, 15(3), 45-62.
- Buzan, B. (2008). People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era. ECPR Press.
- Buzan, B., Waever, O., and de Wilde, J. (1998). Security: A New Framework for Analysis. Lynne Rienner Publishers.
- Choucri, N. (2012). Cyberpolitics in international relations. MIT Press.
- Congress.gov. (2015). Cybersecurity Information Sharing Act (CISA). Retrieved from <https://www.congress.gov>.
- Council of Europe, Budapest Convention on Cybercrime, 200 Altıntaş, F. F. (2022). G7 Ülkelerinin Siber Güvenlik Performanslarının Analizi: Entropi Tabanlı Mabac Yöntemi İle Bir Uygulama. *Güvenlik Bilimleri Dergisi*, 11(1), 263-286. <https://doi.org/10.28956/gbd.11097761>, <https://www.coe.int>, Erişim Tarihi: 10.01.2025.
- Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). Retrieved from <https://www.coe.int>.
- Darıcı, A. B. (2019). Türkiye'nin siber güvenlik politikalarının analizi; Türkiye'nin siber güvenlik modeli için öneriler. *Tesam Akademi Dergisi*, 6(2), 11-33. <http://dx.doi.org/10.30626/tesamakademi.613517>.
- Denning, D. (2017). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.
- Direction Centrale de la Police Judiciaire (DCPJ). (2022). Missions et organisation. <https://www.interieur.gouv.fr>.
- Erdoğan, H. (2022). Türkiye'de Siber Güvenlik ve Kolluk Kuvvetlerinin Yönetişim Rolü. *Güvenlik Bilimleri Dergisi*, 11(1), 23-45.

- European Commission (2016). General Data Protection Regulation (GDPR).
- European Commission (2020). Cybersecurity Strategy for the Digital Decade. European Union.
- European Commission. (2020). Cybersecurity Act: Strengthening Europe's cybersecurity. Retrieved from <https://ec.europa.eu>, Erişim Tarihi: 12.12.2024.
- European Commission. (2022). Horizon Europe Programme. Retrieved from <https://ec.europa.eu>, Erişim Tarihi: 12.12.2024.
- EUROPOL. (2021). International Ransomware Operation Results. <https://www.EUROPOL.europa.eu>, Erişim Tarihi: 12.12.2024.
- EUROPOL. (2021). Major ransomware operation dismantled in cooperation with C3N. <https://www.EUROPOL.europa.eu>, Erişim Tarihi: 12.12.2024.
- Federal Bureau of Investigation. (2020). InfraGard: Building a stronger cybersecurity partnership. Retrieved from <https://www.fbi.gov>
- National Fusion Center Association. (2021). Fusion centers: Enhancing public safety and national security. Retrieved from <https://www.nfcausa.org>.
- Federal Bureau of Investigation. (2021). Cyber Division: Tackling today's top cyber threats. Retrieved from <https://www.fbi.gov>, Erişim Tarihi: 01.01.2025.
- Federal Communications Commission. (2010). National broadband plan: Connecting America. Retrieved from <https://www.fcc.gov>, Erişim Tarihi: 01.01.2025.
- FIEP. (2023). FIEP'in görev ve çalışmaları. <https://www.fiep.org>, Erişim Tarihi: 01.01.2025.
- Fidler, D. P. (2018). Global Cybersecurity Governance and International Cooperation. Cambridge University Press.
- Finklea, K. (2018). Cybercrime: An Overview of the Federal Computer Crime Law and Its Enforcement. Congressional Research Service.
- Gazete İlk Sayfa. (2024). Türkiye siber güvenlikte dünya standartlarına yükseldi. <https://www.gazeteilksayfa.com/turkiye-siber-guvenlikte-dunya-standartlarina-yukseldi-258042h.htm>, Erişim Tarihi: 02.11.2024.
- Givens, B. (2011). The impact of the USA PATRIOT Act on privacy. *American Bar Association Journal*, 97(3), 45–49.
- Godfrain, Loi. (1988). Godfrain Yasası (5 Ocak 1988 tarihli 88-19 sayılı Bilgisayar Dolandırıcılığı Kanunu).
- Goodman, M. (2016). Future crimes: Everything is connected, everyone is vulnerable, and what we can do about it. Anchor Books.
- Gordon, L., Loeb, M., and Zhou, L. (2020). The Economics of Cybersecurity: Theory and Practice. Springer.

- Gorman, S., and Thomas, J. (2017). Cybersecurity in the Global Context. Harvard University Press.
- Greenwald, G. (2014). No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State. Picador.
- Gümüş, S. (2020). Emniyet Teşkilatının Siber Suçlarla Mücadeledeki Rolü: Türkiye Örneği. Polis Akademisi Yayınları.
- Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking. Wiley.
- Hansen, L., and Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly. <https://academic.oup.com/book/25111/chapter/192317023>, Erişim Tarihi: 10.01.2025.
- Hassan, A. (2019). Cybersecurity in the Age of Digital Transformation. Springer.
- Healey, J. (2011). The five futures of cyber conflict and cooperation. Strategic Studies Quarterly.
- Held, D., and McGrew, A. (2002). Governing Globalization: Power, Authority and Global Governance. Polity Press.
- <https://kvkkblog.com/kisisel-verilerin-korunmasi-tarihine-yolculuk/>, Erişim Tarihi: bu site açılmadı
- International Telecommunication Union (ITU) (2024), <https://www.itu.int/160/>, Erişim Tarihi: 25.12.2024.
- International Telecommunication Union (ITU). (2021). Global Cybersecurity Index (GCI) 2020. <https://www.itu.int>, Erişim Tarihi: 11.01.2025.
- International Telecommunication Union. (2024). Global Cybersecurity Index 2024. ITU Publications.
- INTERPOL. (2021). Cybercrime operations. <https://www.INTERPOL.int>.
- INTERPOL. (2023). Siber suçlarla uluslararası mücadele. <https://www.INTERPOL.int>.
- ISO/IEC 27001 (2013). Information Security Management Systems – Requirements. International Organization for Standardization.
- ITU and INTERPOL Collaboration. (2025). ITU and INTERPOL Partnership. Erişim: <https://www.itu.int/en/ITU-D/Partnerships/Pages/INTERPOL.aspx>.
- ITU GCA. (2025). Global Cybersecurity Agenda (GCA). <https://www.itu.int/itu-d/sites/cybersecurity/>, Erişim Tarihi: 03.01.2025.
- ITU GCI. (25 Aralık 2023). Global Cybersecurity Index (GCI). <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx>.
- ITU Trainings. (2024). ITU Academy Trainings. Erişim: <https://academy.itu.int>.

- ITU. (2021). Global Cybersecurity Index 2020: Enhancing cybersecurity for the digital future. International Telecommunication Union.
- Jandarma Genel Komutanlığı. (2023). Türkiye'nin FIEP kapsamındaki çalışmaları. <https://www.jandarma.gov.tr>.
- JORF. (2025). Code pénal, Article 323, <https://www.legifrance.gouv.fr>, Erişim Tarihi: 10.01.2025.
- Jøsang, A., et al. (2021). Handbook of Cybersecurity Risk: Management, Control, and Governance. Springer.
- Karns, M. P., and Mingst, K. A. (2010). International Organizations: The Politics and Processes of Global Governance. Lynne Rienner Publishers.
- Kaya, Y. (2021). Türkiye'de Jandarma ve Siber Güvenlik: Sorunlar ve Çözüm Önerileri. İstanbul: Beta Yayınları.
- Keohane, R. O. (2002). Power and Governance in a Partially Globalized World. Routledge.
- Kim, D., and Solomon, M. G. (2020). Fundamentals of Information Systems Security. Jones and Bartlett Learning.
- Kişisel Verileri Koruma Kurumu (KVKK). (2023). Kişisel verilerin korunması tarihine yolculuk. <https://kvkkblog.com/kisisel-verilerin-korunmasi-tarihine-yolculuk>.
- Kramer, F. D., Starr, S. H., and Wentz, L. K. (2010). Cyberpower and national security. National Defense University Press.
- Kshetri, N. (2021). Cybersecurity capacity building in developing economies: The role of the GCI. Palgrave Macmillan.
- Leiner, BM, Cerf, VG, Clark, DD, Kahn, RE, Kleinrock, L., Lynch, DC, Postel, J., Roberts, LG, and Wolff, S. (2009). İnternetin kısa bir tarihi. ACM SIGCOMM Bilgisayar İletişim İncelemesi, 39(5), 22–31. <https://doi.org/10.1145/1629607.1629613>.
- Lemoine, J., et al. (2019). Fransa'da Siber Güvenlik Stratejileri ve Kolluk Kuvvetlerinin Rolü. Cybersecurity Review.
- Lemos, R. (2019). Cybersecurity and International Law: An Analysis of the Role of the Police. Routledge.
- Lemos, R., et al. (2020). Cybersecurity and Global Policy. Wiley-Blackwell.
- Loi pour la Confiance dans l'Économie Numérique (LCEN), 2004, <https://www.legifrance.gouv.fr>.
- Mailland, J. ve Driscoll, K. (2017). Minitel: İnternete Hoş Geldiniz. MIT Press.
- Mann, M., and Memon, M. (2021). Global Cybersecurity Governance: From International Law to Norms. Routledge.
- McGuire, M. (2020). Cyber Crime and Its Regulation. Springer.

- Miller, B. (2019). *Cyber Security and International Cooperation: Challenges and Solutions*. Palgrave Macmillan.
- Miller, C., and Thompson, R. (2019). Data sovereignty and the ethics of big tech. *Journal of Cyber Ethics*, 12(2), 78-92.
- Ministère de l'Intérieur. (2022). La lutte contre la cybercriminalité en France. <https://www.interieur.gouv.fr>.
- Ministère de l'Intérieur. (2022). La lutte contre les crimes organisés et la cybercriminalité en France. <https://www.interieur.gouv.fr>.
- National Institute of Standards and Technology (NIST). (2021). Cybersecurity framework. <https://www.nist.gov>.
- National Security Agency. (n.d.). Cybersecurity Information. Retrieved from <https://www.nsa.gov/cybersecurity/>.
- NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology.
- Nissenbaum, H. (2019). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press.
- Nye, J. S. (2004). *Soft power: The means to success in world politics*. PublicAffairs.
- OECD. (1980). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.
- OECD. (2025). *Guidelines for the Security of Information Systems and Networks*. <https://legalinstruments.oecd.org/public/doc/116/116.en.pdf>.
- Olsson, T., and Seitz, G. (2020). *Artificial Intelligence in Cybersecurity: Trends, Challenges, and Solutions*. Wiley.
- Özer, M. A., and Yıldırım, S. (2024). Küreselleşme Sürecinde Ulus Devletin ve Kamu Yönetiminin Değişimine Dair Değerlendirmeler. *Uluslararası Yönetim Akademisi Dergisi*, 6(4), 966-985. <https://doi.org/10.33712/mana.1333416>.
- Öztürk, M. (2020). Türkiye'de Siber Suçlarla Mücadele: Kolluk Kuvvetlerinin Rolü. *Siber Güvenlik Dergisi*.
- Perrin, P., and Courtois, S. (2018). "France's Role in Global Cybersecurity." *International Journal of Cyber*.
- Rainer, L. (2019). *Emerging Technologies in Cybersecurity*. Springer.
- Règlement Général sur la Protection des Données (RGPD). (2018). <https://eur-lex.europa.eu>.
- Rid, T. (2013). *Cyber war will not take place*. Oxford University Press.
- Rid, T. (2020). *Cyber War Will Not Take Place*. Oxford University Press.

- Rosenau, J. N. (2000). The Governance of the Globalized World. Palgrave Macmillan.
- Rosenau, J. N., and Czempel, E. O. (1992). Governance Without Government: Order and Change in World Politics. Cambridge University Press.
- Safa, N. S. (2019). "Cybersecurity Awareness and Education: A Review of Literature". Computers and Security, 87, 101575.
- Sarı, M., and Güler, S. (2019). "Türkiye'nin Siber Güvenlik Stratejileri ve Küresel Yönetişimdeki Rolü." Journal of Global Security Studies, 5(4), 112-123.
- Savunma Sanayii Başkanlığı. (2017). Siber Güvenlik Kümelenmesi. Retrieved from <https://ssb.gov.tr>.
- Schafer, V. ve Thierry, B. (2012). Minitel'den İnternete: Fransız kiosk modeli ve İnternetin ortaya çıkışı.
- Schelling, T. C. (2007). Arms and Influence. Yale University Press.
- Schjolberg, S. (2017). Global Cybersecurity Governance: A Framework for International Collaboration. Journal of Cyber Security and Law, 1(2), 45-58.
- Siber Güvenlik Kümelenmesi. (2023). Hakkımızda. Retrieved from <https://siberkume.org.tr>.
- Singer, P. W., and Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.
- Singh, S., and Chakraborty, R. (2020). International norms and the Global Cybersecurity Index. Cybersecurity Review, 5(3), 45-62.
- Smith, J. (2021). The Role of Law Enforcement in Cybersecurity: A U.S. Perspective. Journal of Cybersecurity.
- Smith, J., and Jones, M. (2020). Asymmetric power dynamics in cyber security: Risks and solutions. Cyber Governance Review, 8(4), 102-118.
- Smith, R. (2017). Cybersecurity and International Cooperation: The Role of Global Institutions. Oxford University Press.
- SosyalUp. (2024). Birleşmiş Milletler dönüm noktası niteliğindeki siber suç anlaşmasını kabul etti. SosyalUp. <https://sosyalup.net/birlesmis-milletler-donum-noktasi-niteligindeki-siber-suc-anlasmasini-kabul-etti>, Erişim Tarihi: 12.12.2024.
- Taddeo, M., and Floridi, L. (2018). How AI can be a force for good. Science, 361(6404), 751-752.
- TRT Haber. (2022). BM ve Türkiye'nin Siber Güvenlik İş Birliği. <https://www.trthaber.com>, Erişim Tarihi: 11.01.2025.
- TÜBİTAK. (2019). Siber güvenlik raporu: Türkiye'nin 2019 değerlendirmesi. TÜBİTAK Yayınları.

- U.S. Department of Homeland Security. (n.d.). Cybersecurity. Retrieved from <https://www.dhs.gov/cybersecurity>.
- Ulaştırma ve Altyapı Bakanlığı. (2013). Ulusal siber güvenlik stratejisi ve 2013 eylem planı. <https://www.uab.gov.tr>.
- Ulaştırma ve Altyapı Bakanlığı. (2021). Türkiye'nin ulusal siber güvenlik stratejisi ve 2021–2023 eylem planı. Ulaştırma ve Altyapı Bakanlığı Yayınları.
- UN CTED. (2022). Countering the Financing of Terrorism in the Digital Age. <https://www.un.org/cted>, Erişim Tarihi: 12.01.2025.
- UN OEWG. (2021). Open-Ended Working Group on Cybersecurity. <https://www.un.org/disarmament>.
- United States Department of Justice. (2020). Computer Fraud and Abuse Act (CFAA). Retrieved from <https://www.justice.gov>.
- UNODC. (2022). Cybercrime Capacity-Building Programs. <https://www.unodc.org>.
- USGS. (2025). Ulusal Siber Güvenlik Stratejisi (2024-2028). <https://www.uab.gov.tr/uploads/pages/siber-guvenligin-yol-haritasi-yerli-ve-milli-tekho/ulusal-siber-guvenlik-stratejisi-2024-2028.pdf>, Erişim Tarihi: 02.01.2025.
- USGSEP. (2024). Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2024-2028). <https://cyberartspro.com/ulusal-siber-guvenlik-stratejisi-ve-2024-2028-eylem-planı/>, Erişim Tarihi: 02.11.2024.
- USOM. (2023). Ulusal Siber Olaylara Müdahale Merkezi. Retrieved from <https://usom.gov.tr>.
- Ünal, M. (2021). Siber Güvenlikte Kritik Altyapılar ve Ulusal Politikalar. Ankara: Seçkin Yayıncılık.
- Vacca, J. R. (2017). Computer and Information Security Handbook. Elsevier.
- Vermesan, O., and Friess, P. (2018). Cybersecurity: Challenges and Solutions in the Global Context. John Wiley & Sons.
- Waeber, O. (1995). "Securitization and Desecuritization." In On Security, edited by Ronnie Lipschutz, 46-86. New York: Columbia University Press.
- Wall, D. S. (2015). Cybercrime: The Transformation of Crime in the Information Age. Policing and Society, 25(3), 303-318.
- Whitman, M. E., and Mattord, H. J. (2020). Principles of Information Security. Cengage Learning.
- Wiener, N. (1948). Cybernetics: Or control and communication in the animal and the machine. MIT Press.

Yeni Şafak. (2024). Türkiye “rol model” oldu: Siber güvenlikte dünyada öncüyüz. <https://www.yenisafak.com/ekonomi/turkiye-rol-model-oldu-siber-guvenlikte-dunyada-oncuyuz-4654467>, Erişim Tarihi: 02.11.2024.

Zetter, K. (2020). Cybersecurity and Law Enforcement: A Global Perspective. Oxford University Press.





ÖZGEÇMİŞ

İlk öğrenimine Kırıkkale’de Zübeyde Hanım İlköğretim Okulunda başladı ve Ankara’da Dr. Ümit Yaşar Akyol İlköğretim Okulunda tamamladı. Orta öğrenimini Ankara’da Yenimahalle Mustafa Kemal Anadolu Lisesi’nde tamamladı. 2012 yılında girdiği Gazi Üniversitesi Uluslararası İlişkiler (%30 İng.) Bölümünden 2017 yılında mezun oldu. 2021 yılında başladığı Yalova Üniversitesi Lisansüstü Eğitim Enstitüsü’nden “Siber Güvenliğin Küresel Yönetişiminde Bir Aktör Olarak Kolluk Kuvvetleri: Türkiye, Fransa ve ABD Örnekleri” konulu tezi ile 2025 yılında mezun oldu. 2019 yılından itibaren İçişleri Bakanlığında görev yapmaktadır.

DİĞER YAYIN VE ESERLER

Ertürk, Ş. (2024) Küresel Siber Güvenliğin Sağlanmasında Kolluk Kuvvetlerinin Rolü. İyit, N., Hasani, E. *14thInternational Istanbul Scientific Research Congress Proceeding Book 2024*(1076-1077), BZT Turan PUBLISHING House. DOI: <https://doi.org/10.30546/19023.978-9952-8541-7-6.2024.6097>.